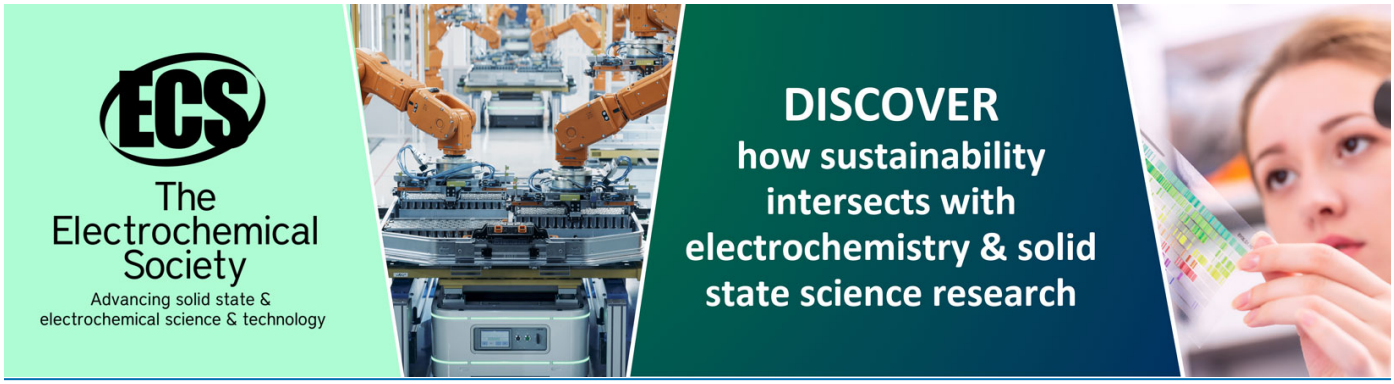
Building Dynamic Mesh VPN Network using MikroTik Router



Building Dynamic Mesh VPN Network using MikroTik Router

S H Kurniadi[1], E Utami[2] and F W Wibowo[3]

[1,2,3] Magister of Informatics Engineering, AMIKOM Yogyakarta University, Indonesia.

E-mail: sidikhadik@windowslive.com

Abstract. Dynamic Multipoint Virtual Private Network (DMVPN) is a VPN technology to form an automatic, fast, and dynamic logical mesh network. DMVPN is a proprietary technology from Cisco, so this technology is not available on MikroTik routers. Although not equipped with the DMVPN technology, MikroTik scripting and scheduler feature can help to make the network becomes a DMVPN network. This paper discusses the usage of OpenVPN and Open Shortest Path First (OSPF) to form a Dynamic Mesh VPN network using MikroTik routers inside the GNS3 simulation environment. The final part of this study proves that this solution can help the routers that do not equipped with the DMVPN technology to form a Dynamic Mesh VPN network

1. Introduction

Dynamic Multipoint Virtual Private Network (DMVPN) becomes a solution if not possible to create a full mesh topology using leased-line. DMVPN combines the following protocols [1]: (i) Multipoint Generic Routing Encapsulation (mGRE), a protocol to set up multiple VPN connections within a single tunnel interface; (ii) Next Hop Resolution Protocol (NHRP), a protocol that reads SPOKE as a neighbor for every other SPOKE; (iii) IP Security (IPSec), a protocol to maintains the data security; and an added dynamic routing protocols.

The primary requirements of dynamic tunnels on DMVPN are NHRP and mGRE [2]. MikroTik routers do not have the NHRP and mGRE protocol although both are standard protocols, so MikroTik router cannot form the dynamic mesh VPN network using both protocols. The solution to form a dynamic mesh VPN network is using the other protocols.

The purposes of this research are: (i) offer a solution to make the routers to adjust to the network changes, following the characteristics of DMVPN; (ii) offer a Dynamic Mesh VPN network solution using the open standard protocols. The scope of the problem: (i) the substitution technologies to form a DMVPN network are Open Shortest Path First (OSPF) and OpenVPN; (ii) the topology testing run single OSPF area using three MikroTik routers and one server inside the GNS3 network simulation environment; (iii) the server is running Apache,

PHP, and MySQL programs; (iv) each router will periodically update the data if these routers detect the network configuration changes or if these routers get a trigger to update the data.

The remainder of the paper is organized as follows. Section II presents the related works on comparing OSPF with Enhanced Interior Gateway Routing Protocol (EIGRP), the benefits of VPN, the usage of DMVPN, and the early research of DMVPN in MikroTik. Section III presents the basic knowledge of related technologies and how to set up a DMVPN network. Section IV presents the simulation on designing a Dynamic Mesh VPN network using MikroTik. Section V presents the results and discussion of the simulation. Section VI presents the conclusion of the paper.

2. Related Work

Based on the earlier research, OSPF and EIGRP is the best routing protocol. Jain et al. [3], prove that OSPF is faster than EIGRP in packet processing because the average delay and jitter on OSPF are smaller than EIGRP. Routing update characteristic of the routing protocol is affecting the delay and jitter. OSPF routing update is aperiodic while EIGRP routing update is periodic.

Hanif et al. [4] prove that EIGRP requires more CPU resources than OSPF. EIGRP routing update is periodic, so EIGRP requires a continuous routing update. OSPF uses the earlier routing information when doing routing update, so OSPF reduces the routing update process and more efficient.

Mohammed and Elrahim [5] prove that EIGRP has the fastest convergence time compared to the other routing protocols. Idrissi et al. [6] explain that it happens because all routers inside an area will update the topology by flooding the neighbor with the Link-State Advertisements (LSA). EIGRP is a proprietary routing protocol from Cisco. Overall EIGRP has the best value in all tests followed by OSPF, but OSPF is best in error handling.

Garg and Gupta [7] prove that backups in OSPF can decrease the delay time. Anjana et al. [8] explain that OSPF is the preferred and most used routing protocol. OSPF is the best routing protocol to use in this research because OSPF is an open standard protocol and has a performance that is almost equal to EIGRP.

Mukhtar et al. [9] apply VPN to address limited location coverage issues on Local Area Network (LAN) networks. This paper proves that VPN can join two or more networks as a single virtual LAN network over the internet. However, VPN requires a higher bandwidth than the physical LAN.

Salman [10] proves in GNS3 network simulation that VPN can secure the data transfer over public networks. Qehaja et al. [2] describe the benefits of DMVPN over conventional VPN. DMVPN creates a mesh network between secure sites over the public network.

Kamoun et al. [1] describe the scalability of DMVPN on the WiMAX network. DMVPN is suitable for a small network. Therefore, it is necessary to divide the network into several areas. McRoberts [11] shows early research that MikroTik router can use another technology to form a DMVPN network.

3. Basic Knowledge

A computer network consists of connected nodes and end stations that exchange network resources through specific media. A node is a device to connect two end stations or more [12, 13, 14, 15, 16]. Nodes can be routers that connect different computer networks and transfer packet data between them [16, 17, 18].

One of the router tasks is to find the best route to the destination network [19]. End stations can be computers, smartphones, and other devices used by end users. Metropolitan Area Network (MAN) and Wide Area Network (WAN) network is using the terms like nodes and end stations, whereas LAN network is using the terms like servers and hosts [16].

Computer networks consist of topologies, routing algorithms, and packet data control mechanisms [20]. The internet is the largest public computer network that built from many Internet Service Providers (ISP) [12, 21]. The internet can be used to create a WAN network [12] however, it is not secure and reliable enough [9, 12]. Leased-line is a solution from ISP to create a WAN network on top of their infrastructure. It is relatively more secure but more expensive than the internet [9].

The VPN is a secure connection used over the internet [9, 10, 22, 23, 24, 25, 26]. VPN becomes the solution for connecting different computer networks over public media such as the Internet [10, 22] and eliminating the need for leased-line networks [26, 27]. VPN uses security procedures and tunneling to send and receive data [22, 28, 29, 30].

Tunneling handles the IP packet encapsulation to secure the data transmissions [12, 25], while the encryption and authentication handle the data integrity and confidentiality within the VPN [10, 24]. Both tunnel endpoints must support the same tunneling protocol. Tunnels can run on layer 2, 3 or above on the Open System Interconnection (OSI) layer depending on the used tunneling protocol [10, 24]. Tunnel works using the CPU [26] therefore the speed provided by the VPN also becomes slower than the internet [26, 28].

VPNs will form a virtual point-to-point network [26] to build a flexible remote computer network [31]. Two types of VPN networks are [29, 30]: (i) Remote Access VPN, a condition where every user on the network connects to the VPN network and manages the VPN Client configuration. (ii) Site-to-site VPN, a condition where VPN connection construction is assigned to the router or server, each user does not need to configure the VPN Client.

DMVPN is an automatic site-to-site VPN technology that builds mesh network topologies where each node acts as a gateway VPN to improve redundancy [1, 2, 27]. A network topology is a relationship between nodes including the transmission medium [12, 16, 32] that affects the cost, efficiency, reliability, and network performance [32, 33, 34].

Latency is the time required by data to arrive at the destination [35]. Low latency shows that a computer network is in excellent condition. The way to reduce latency is through redundancy [35, 36]. Redundancy prevents the network problems and provides backups without knowing the cause of the problem [32, 35]. There are two considerations to create a redundant network: reducing the points of failure and reducing the number of hops [32, 34].

Mesh topology is used on large-scale networks [37]. Each node in the mesh topology is directly connected to each other [12, 13]. Mesh topologies are rapidly adapting to the changes within the network [37, 38]. The mesh network has a high redundancy because of backup links [12, 37, 38, 39]. However, mesh topology has a weakness that will be more difficult to configure. For each n location or node, (1) connections are required.

$$n (n - 1) / 2 \quad (1)$$

When the network consists of 4 nodes, it will take 6 connections [13], which means the cost of a physical network will be more expensive when the network becomes larger [32]. DMVPN has the advantage of the mesh network topology and overcoming its weakness [1, 2]. Network administrators do not need to change routing settings [1].

The DMVPN forming part consists of HUB and SPOKE. HUB is the server of DMVPN, while SPOKE is the client of DMVPN [1, 2]. At first step, each SPOKE informs its public IP address to the HUB then HUB creates an NHRP database that has the public interface address of each SPOKE. Every SPOKE becomes a neighbor to another SPOKE. Every SPOKE will set up a VPN connection with the neighbor it knows [2]. The HUB and SPOKE must be statically connected, whereas SPOKE-to-SPOKE connection would be created dynamically according to the network changes [1]. If the SPOKE did not connect to the HUB then, SPOKE-to-SPOKE connection will also be interrupted because the SPOKE cannot read the network changes.

OpenVPN is an open standard VPN solution that runs in the transport layer. OpenVPN is working using Secure Socket Layer (SSL) certificates that handle the data security [9, 25] and can bypass the ISP's firewall because it does not rely on specific ports.

OSPF is one of the many dynamic routing protocols. Routing is the primary key in Internet communication [4, 6, 7]. Routing is a way to forward packets of data from one computer network to another computer network and determining the optimal data path [6, 13, 18]. Without routing, network traffic will be limited to one physical network [6]. A routing protocol shows how a router communicates with other routers to determines the best packet data delivery path to the destination node [4, 6, 7]. The routing algorithm determines the choice of a particular route [7]. The router records every network element inside a routing table [18] and share it with other routers using the same routing protocol. The router uses the routing table to decide the destination path [21]. Dynamic routing can adapt to the network changes by reading the routing updates messages [8]. Network administrators only have to write the protocol with the required syntax. If the router detects the network changes, then the router will decide the best path to the destination [14, 23].

OSPF routing protocol is a link-state and intra-domain routing protocol [5, 6, 7, 8, 18]. OSPF uses the Dijkstra algorithm and the topology to figure the shortest path to the destination [4, 5, 6, 7, 18, 34, 40]. This routing protocol is used to build large-scale networks [8, 21, 41]. OSPF is part of the Interior Gateway Protocol (IGP) which serves to route packet data within a single routing domain [7, 8, 21]. OSPF builds a topology based on connection status information with the other routers [8]. The OSPF divides the network into routing areas [8]. Every router within an OSPF area store a topology database for their area. The router does not have complete information about topology outside its area, so that OSPF usage will reduce the database size and the network load [8, 42].

OSPF communicates using the LSA that store the information of all connected routers and networks [42] containing a network identifier, subnet mask, and a list of all routers in a single broadcast domain [21]. OSPF does not convey routing information via transport protocols such as User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). In contrast, OSPF uses a dedicated IP datagram [7]. OSPF is one of the many dynamic routing protocols preferred for having high performance [3, 5] because it has high speed to deals with weak links [43]. As an intra-domain routing protocol, OSPF has advantages in scalability and convergence [41, 42].

4. Simulation

The network simulated inside a GNS3 network simulation environment. It consists of four internet-connected nodes. These nodes consist of three MikroTik routers and one web server. These nodes communicate using a domain or public IP.

The virtual server functions as a HUB which handles storing data, updating data, assigning neighbors configuration to each router, and giving triggers to each neighbor. The router functions as a SPOKE which handles sending configuration data to the server using the scripting feature with the HTTP GET method.

Each network segment of each router consists of two hosts that are MikroTik router itself and a PC that is simulated using docker container. The physical topology of this network simulation can be seen in Figure 1.

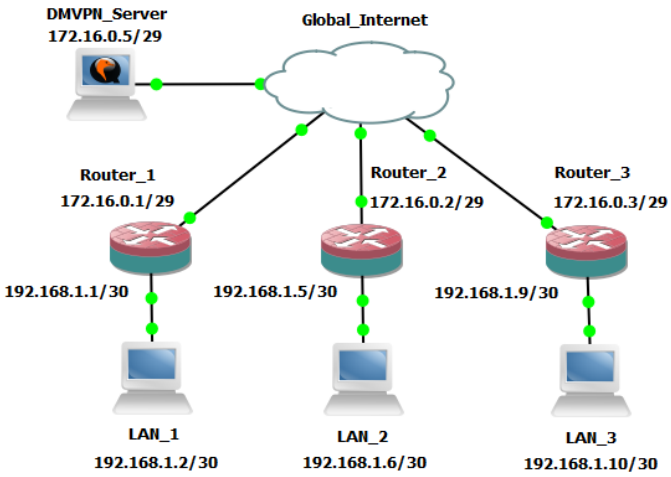


Figure 1. Simulated Physical Network Topology

The server is recording each router by its domain or public IP. This job is done using Apache, PHP, and MySQL. Each device is running inside a virtual machine using Vmware Player 14 software that loads the GNS3-VM operating system. Host PC specification can be seen in Table 1, while each network device specification in the simulation environment can be seen in Table 2.

Table 1. Host PC Specification

Device	Spesification
Processor	Intel Core i7-8550u
Memory	16GB DDR4
Harddisk speed	5400rpm
Operating System	Microsoft Windows 10
Virtualization Software	VMware Player 14

Table 2. Specification of Each Network Device in The Simulation Environment

	CPU	Memory (MB)	Guest OS	Device Count
DMVPN_Server	1	1024	Ubuntu 14.04 Server	1
Router	1	128	MikroTik CHR 6.41.4	3
Global Internet	1	128	MikroTik CHR 6.41.4	1
PC	Managed by Docker		Alpine Linux	3

The server inserts router data and router configuration data into the database when the data sent by the router is unavailable in the database or the server detects a new router. The server updates the router configuration data into the database when it finds the configuration data difference between the router and the database.

When the server receives an insert or update command, the server will provide the latest configuration data and neighbor configuration data to the sender router. The server finishes the process by giving a trigger to the neighbor of the sender router to do re-convergence.

Every neighbor will check the re-convergence trigger periodically following the time written in the scheduler. If the neighbor detects a re-convergence trigger, then each neighbor will run the Dynamic Mesh VPN script and repeat the convergence process. Graphical explanation of this process is shown in Figure 2.

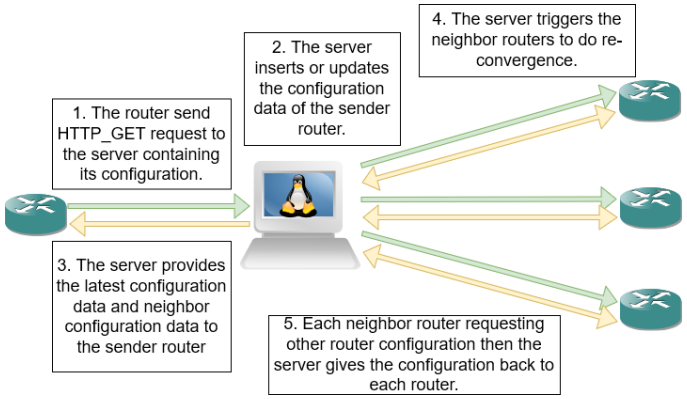


Figure 2. Network Convergence Process

5. Result and Discussion

This section presents the simulation results consisting of (i) proof of the formation of Dynamic Mesh VPN network; (ii) convergence speed, delay time, and resource usage of Dynamic Mesh VPN network.

5.1. Proof of the Formation of Dynamic Mesh VPN

This step is done by verifying the number of generated VPN connections on each router and verify that each network segment can connect to other network segments securely.

Generated VPN connections on each router can be seen in Figure 3, Figure 4, and Figure 5. These generated VPN connections simplified in Table III while the logical topology created by these generated VPN connections can be seen in Figure 6.

```
/interface ovpn-client
add comment=Mesh-VPN connect-to=172.16.0.2 mac-address=FE:C
B:D9:91 name=ovpn-client-172.16.0.2 \
    password=pass1 port=443 profile=default-encryption user
add comment=Mesh-VPN connect-to=172.16.0.3 mac-address=FE:B
6:BB:B4 name=ovpn-client-172.16.0.3 \
    password=pass1 port=443 profile=default-encryption user
[admin@MikroTik] > /ppp secret exp
/ppp secret
add comment=Mesh-VPN local-address=192.168.0.1 name=user3 p
d=pass3 profile=default-encryption \
    remote-address=192.168.0.2 service=ovpn
add comment=Mesh-VPN local-address=192.168.0.1 name=user2 p
d=pass2 profile=default-encryption \
    remote-address=192.168.0.3 service=ovpn
[admin@MikroTik] >
```

Figure 3. Generated VPN Connections on Router 1

```
/interface ovpn-client
add comment=Mesh-VPN connect-to=172.16.0.1 mac-address=FE:85:B6:C
3:34:CA name=ovpn-client-172.16.0.1 \
    password=pass2 port=443 profile=default-encryption user=user2
add comment=Mesh-VPN connect-to=172.16.0.3 mac-address=FE:E8:48:0
B:24:E4 name=ovpn-client-172.16.0.3 \
    password=pass2 port=443 profile=default-encryption user=user2
[admin@MikroTik] > /ppp secret exp
/ppp secret
add comment=Mesh-VPN local-address=192.168.0.3 name=user1 passwor
d=pass1 profile=default-encryption \
    remote-address=192.168.0.1 service=ovpn
add comment=Mesh-VPN local-address=192.168.0.3 name=user3 passwor
d=pass3 profile=default-encryption \
    remote-address=192.168.0.2 service=ovpn
[admin@MikroTik] >
```

Figure 4. Generated VPN Connections on Router 2

```
/interface ovpn-client
add comment=Mesh-VPN connect-to=172.16.0.1 mac-address=FE:AF:82:E
E:AC:A2 name=ovpn-client-172.16.0.1 \
    password=pass3 port=443 profile=default-encryption user=user3
add comment=Mesh-VPN connect-to=172.16.0.2 mac-address=FE:93:A6:D
4:2E:EF name=ovpn-client-172.16.0.2 \
    password=pass3 port=443 profile=default-encryption user=user3
[admin@MikroTik] > /ppp secret exp
/ppp secret
add comment=Mesh-VPN local-address=192.168.0.2 name=user1 passwor
d=pass1 profile=default-encryption \
    remote-address=192.168.0.1 service=ovpn
add comment=Mesh-VPN local-address=192.168.0.2 name=user2 passwor
d=pass2 profile=default-encryption \
    remote-address=192.168.0.3 service=ovpn
[admin@MikroTik] >
```

Figure 5. Generated VPN Connections on Router 3

Table 3. Generated VPN Connections

Router Name	IP Address	as OpenVPN Client	as OpenVPN Server	
		Connect to	Local address	Remote address
Router_1	172.16.0.1	172.16.0.2	192.168.0.1	192.168.0.2
		172.16.0.3	192.168.0.1	192.168.0.3
Router_2	172.16.0.2	172.16.0.1	192.168.0.2	192.168.0.1
		172.16.0.3	192.168.0.2	192.168.0.3
Router_3	172.16.0.3	172.16.0.1	192.168.0.3	192.168.0.1
		172.16.0.2	192.168.0.3	192.168.0.2

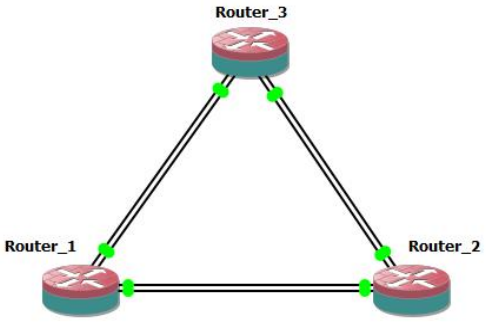


Figure 6. Logical Topology of Generated VPN Connections

Connection and security test are done by sending ping messages to another network segment. The monitored connections are from the router to the internet and from LAN to the gateway router. The monitoring result shows that ping messages are encapsulated when passing the internet as seen in Figure 7, while ping messages are readable by each network segment as seen in Figure 8.

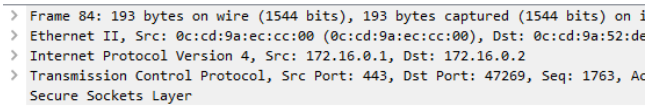


Figure 7. Encapsulated Ping Message in the Internet Side

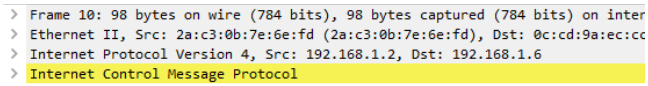


Figure 8. Decapsulated Ping Message in the LAN Side

From the number of generated VPN connections, the successful connection, and security test, it can be proven that the scripting, scheduler, OpenVPN, and OSPF combination can help the routers to form a Dynamic Mesh VPN network.

5.2. Convergence Speed, Delay Time, and Resource Usage of Dynamic Mesh VPN Network

The convergence speed test is done by changing a router local network address 25 times, while delay time test is done by disconnecting one of the VPN links 25 times. The result of the test can be seen in Table 4.

Table 4. Convergence and Delay Test Results

Convergence testing		Delay testing	
Testing phase	Convergence time (s)	Testing phase	Delay time (s)
1	79	1	7
2	78	2	7
3	62	3	4
4	69	4	4
5	76	5	4
6	60	6	4
7	62	7	5
8	73	8	6
9	62	9	7
10	65	10	7
11	62	11	5
12	70	12	5

13	69	13	7
14	79	14	4
15	64	15	6
16	61	16	7
17	62	17	7
18	62	18	5
19	73	19	4
20	77	20	5
21	80	21	7
22	68	22	7
23	67	23	4
24	66	24	5
25	65	25	6
Average	68	Average	5

The test result shows that the average time required to achieve convergence status is 68 seconds, while the average delay time is 5 seconds. This average speed is slower than Cisco's DMVPN average speed. Memory usage of the pre-configured router is 17.9 MB while the CPU resource usage is 0%. Resource usage checked every 30 seconds in 3 minutes. The result of the check can be seen in Table 5.

Table 5. Resource Usage monitoring

Memory usage (MB)	CPU usage (%)
22.2	1
22.4	2
22.4	0
22.4	1
22.4	1
22.4	1
Average: 22.367	Average: 1

The check result shows that the average memory used by the router is 22,367 MB and average CPU used by the router is 1%. This Dynamic Multipoint VPN does not take a lot of memory and CPU resource in the GNS3 network simulation environment.

6. Conclusion

The scripting, scheduler, OpenVPN, and OSPF combination can help the routers that are not equipped with the DMVPN technology to form a Dynamic Mesh VPN network. It can be proven by the number of generated VPN connections, the successful connection test, and the successful security test. Although the speed is slower than Cisco's DMVPN, this combination has overcome the problems on the routers that do not equipped with DMVPN technology. This method has a disadvantage that the network administrator needs to allocate unique networks addresses for the VPN networks as many as the required areas.

Acknowledgments
Many thanks to Welby McRoberts for his early research on the DMVPN-like network at MikroTik User Meeting 2016. AMIKOM University and all the lecturers who provide a lot of support and facilities

7. References

[1] N E Kamoun, A Bahnasse, and F Bensalah 2017 Evaluation of The Scalability of The Protected Multipoint Dynamic VPN by IPSec in A WiMAX Network *International Journal of Computer Science and Network Security (IJCSNS)* Vol 17 No 12 p 108–110
[2] B Qehaja, A Bajraliu, A Shabani, and E Hajrizi 2016 Enterprise Integration, Networking and Virtual Communications *International Federation of Automatic Control (IFAC)* Vol 49 Issue 29 p 144-147
[3] G Jain, T Hadpawat, and D Vaya 2017 Performance Evaluation of Authenticate (MD5, SHA) Routing Traffic over EIGRP and OSPF with IPv6 *International Journal of Computer Applications (IJCA)* Vol 176 p 26–29
[4] M K Hanif, R Talib, N Ayub, M U Sarwar, and S Ullah 2017 OSPF vs EIGRP: A Comparative Analysis of CPU Utilization Using OPNET *International Journal of Advanced Computer Science and Applications (IJACSA)* Vol 8 No 7 p 468–471
[5] Z K A Mohammed and A G A Elrahim 2016 Performance Evaluation Comparison of RIP, IGRP, EIGRP, and OSPF Routing Protocols in UMTS *Red sea university Journal of Basic and Applied Science* Vol 1 p 19–36
[6] D E Idrissi, N Elkamoun, F Lakrami, and R Hilal 2017 Performance Comparison of Protocols Combination Based on EIGRP and OSPF for Real-time Applications in Enterprise Networks *International Journal of Advanced Computer Science and Applications (IJACSA)* Vol 8 No 5 p145–150
[7] P Garg and A K Gupta 2017 Extensive Reviews of OSPF for Reducing the Convergence Time *International Journal of Advanced Research in Computer Science (IJARCS)* Vol 8 No 9 p 425–428
[8] K Anjana, A Singh, and G S M Krishnan 2017 Comparative Analysis of Dynamic Routing Protocols *International Journal of Engineering Research & Technology (IJERT)* Vol 6 p 346–353
[9] H Mukhtar, A Hafid, and F A Wenando 2017 Local Network Communication Based on Virtual Private Network (VPN) at Universitas Muhammadiyah Riau *International Conference of Applied Science on Engineering, Business, Linguistics and Information Technology* 13-15 October 2017 (Padang, Indonesia)
[10] F A Salman 2017 Implementation of IPSec-VPN Tunneling using GNS3 *Indonesian Journal of Electrical Engineering and Computer Science* Vol 7 No 3 p 855–860
[11] W McRoberts 2016 *Dynamic VPNS How to Make A Poor Mans DMVPN Type System with RouterOS* Available Online: https://mum.mikrotik.com/presentations/UK16/presentation_3868_1479205573.pdf (Last accessed: 12 July 2018)
[12] B Shi 2017 *A Practical Introduction to Enterprise Network and Security Management* (NW: CRC Press)
[13] T Lammle 2015 *CompTIA Network+ TM Deluxe Study Guide, 3rd edition* (Indiana: John Wiley & Sons)
[14] T Lammle and J Swartz 2013 *CCNA ® Data Center Introducing Cisco Data Center Networking Study Guide* (Indiana: John Wiley & Sons)
[15] G A Donahue 2011 *Network Warrior, 2nd edition* (CA: O'Reilly Media)
[16] M M D Silva 2016 *Cable and Wireless Networks Theory and Practice (*NW: CRC Press)
[17] P R Tadimety 2015 *OSPF: A Network Routing Protocol* (Apress)
[18] R Srivastava and A Singh 2017 Route Redistribution Between EIGRP and OSPF Routing Protocol Using GNS3 Software *International Journal for Research in Applied Science & Engineering Technology* Vol 5 p 1232–1237
[19] T Lammle 2016 *CCNA Routing and Switching Complete Study Guide, 2nd edition* (Indiana: John Wiley & Sons)

[20] A Punhani, P Kumar, and N Nitin 2017 Three-dimensional Topology Based on Modified Diagonal Mesh Interconnection Network *Journal of Telecommunication, Electronic and Computer Engineering* Vol 9 p 1–6
[21] S Voigt, C Howard, D Philp, and C Penny 2017 Representing and Reasoning about Logical Network Topologies *Graph Structures for Knowledge Representation and Reasoning* 21 August 2017 (Melbourne,Australia)
[22] S Andreevski, A Bozhinovski, and B Stojchevska 2017 Vpn Server Versus Proxy Server Privacy *The 14th International Conference for Informatics and Information Technology* (Mavrovo, Macedonia)
[23] S Rahimi and M Zargham 2017 Quantitative Evaluation of Virtual Private Networks and Its Implications for Communication Security in Industrial Protocols *International Journal of Computational Intelligence Theory and Practice* Vol 3 No 1 p 51–61
[24] M J Bellar 2015 Cloud Computing Security with VPN *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)* Vol 4 p 100–103
[25] P Likhar, R S Yadav, and M K Rao 2011 Securing IEEE 802.11g WLAN using OpenVPN and Its Impact Analysis *International Journal of Network Security & Its Applications (IJNSA)* Vol 3 No 6 p 97–113
[26] A Singh, and A Mallick 2017 A Survey on Virtual Private Network *National Conference On Contemporary Research and Innovations in Computer Science (NCCRICS)* 16 December 2017 (Bangalore, India)
[27] Y Matsuhashi, T Shinagawa, Y Ishii, N Hirooka, and K Kato 2012 Transparent VPN Failure Recovery with Virtualization *Future Generation Computer Systems* Vol 28 p 78–84
[28] S Aswad and M Qasim 2013 A Solution to Enhance VPN Effect on Wireless Network Performance *College of Engineering Journal (NUCEJ)* Vol 16 No 1 (Nahrain University) p 102–110
[29] R Kajal, D Saini, and K Grewa 2012 Virtual Private Network International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Vol 2 p 428-432
[30] H Bourdoucen, A A Naamany, and A A Kalbani 2009 Impact of Implementing VPN to Secure Wireless LAN *World Academy of Science, Engineering and Technology* 27 p 625–630,
[31] N E Rikli and S Almogari 2013 Efficient Priority Schemes for The Provision of End-to-end Quality of Service for Multimedia Traffic over MPLS VPN Networks *Journal of King Saud University – Computer and Information Sciences* Vol 25 p 89-98
[32] H Qi 2017 Model of Computer Network Topology Optimization Based on Pattern Recognition Technology *3rd International Conference on Social Science, Management and Economics*
[33] C Wang, N Huang, S Zhang, Y Zhang, and W Wu 2016 A Hierarchical Network Model for Network Topology Design using Genetic Algorithm *MATEC Web Conf* Vol 119, 28 October – 01 November 2016 (Taichung, Taiwan)
[34] V Chellappan, K M Sivalingam, and K Krithivasan 2016 A Centrality Entropy Maximization Problem in Shortest Path Routing Networks *Computer Networks* Vol 104 p 1–15
[35] A Vulimiri, O Michel, P B Godfrey, and S Shenker 2012 More is Less: Reducing Latency Via Redundancy *11th ACM Workshop on Hot Topics in Networks* 29 – 30 October 2012 (Redmond, Washington)
[36] G Joshi, E Soljanin, G Wornell 2017 Efficient Redundancy Techniques for Latency Reduction in Cloud Systems *ACM Transactions on Modeling and Performance Evaluation of Computing Systems* Vol 2 p 1–30
[37] J Chen, G Wang, C Lin, T Wang, and G Wang 2007 Probabilistic Analysis on Mesh Network Fault Tolerance *Journal of Parallel and Distributed Computing* Vol 67 p 100–110
[38] S Srinivasa and M Haenggi 2014 Combining Stochastic Geometry and Statistical Mechanics for The Analysis and Design of Mesh Networks *Ad Hoc Networks* Vol 13 p 110–122
[39] S Shah-Heydari and O Yang 2009 Heuristic algorithms for designing self-repairing protection trees in mesh networks *Computer Networks* Vol 53 p 2537–2551

[40] A Castelucio, A T A Gomes, A Ziviani, R M Salles 2012 Intra-domain IP Traceback Using OSPF *Computer Communications* Vol 35 p 554–564
[41] A Jaron, A Mihailovic, and A H Aghvami 2016 Qos-aware Multi-plane Routing Method for OSPF-based IP Access Networks *Computer Networks* Vol 99 p 1–14
[42] Y Nozaki, P Bakshi, H Tuncer, and N Shenoy 2014 Evaluation of Tiered Routing Protocol in Floating Cloud Tiered Internet Architecture *Computer Networks* Vol 63 p 33–47
[43] L Wenxing, W U Muqing, Z Min, and L I Peizhe 2017 The Impacts of Weak Links on Routing Process in Large Scale Multi-hop Networks *IEEE Access* Vol 5 p 12125-12134