Virtual Private Network (Vpn) Network Design For Multiprotocol Label Switching (Mpls) Networks

Fathurrahmad, Salman Yusuf, Taufiq Iqbal, Abdus Salam

Abstract: MPLS is a packet delivery technology on high-speed backbone networks that connects several advantages of circuit-switched and packet-switched communication systems that produce better technology than existing. MPLS works on packages with MPLS headers, which contain one or more labels. The MPLS header consists of 32 data bits, including a 20-bit label, 2 test bits, and 1 stack collection bit, and 8 TTL bits. Labels on MPLS are used for process forwarding, including traffic engineering processes. It is hoped that with this MPLS path the network can be connected and connected easily and the access process is expected to be faster and better. This study aims to create a network model and implement a VPN network with routing protocols on the Multiprotocol Label Switching (MPLS) network at AMIK Indonesia. This research will use the method. This research will use the literature study method which is intended to obtain and study data contained in personal computers connected to the network in the AMIK Indonesia computer network laboratory. Data is collected according to the focus of research in the form of network topology used, IP addressing and MPLS techniques. The collection of data/information is simultaneously a simulation of researchers to imitate or represent the behavior of real systems. The conclusion obtained from this study is that this research has succeeded in building MPLS VPN networks and providing a stable network bandwidth efficiency and is used at AMIK Indonesia.

Keywords: Model, Implementation; VPN; Multi-Protocol Label Switching, Network, AMIK Indonesia, Indonesia.

1 INTRODUCTION

The development of the convergence of the internet and telecommunications, with applications in it that are increasingly dependent on the availability of large bandwidth, with its QoS settings requiring networks and elements therein that provide full support for data security and increased network performance [1]. So, we need data delivery technology that not only facilitates routing and discovery of the best trajectories but also can provide security in data communication. IETF standardizes the Multi-Protocol Label Switching (MPLS) solution as the development of Virtual Private Network (VPN) technology to improve forwarding performance [2] and traffic engineering intelligence on packet-based networks. This technology can simplify the routing process that is a burden on the router because it must analyze each incoming IP header, as well as optimize path selection through class of service and traffic engineering management capabilities. Virtual Private Network (VPN) allows communicating securely throughout a public network in such a way that the public network operates as one or several private communication links [3]. The development of MPLS in video streaming service networks can be improved to produce a better quality [4]. MPLS provides a solution to improve network performance, where MPLS makes the network simpler by adding headers or labels to packets as identification that will be used in the switching process [5]. MPLS VPN application is also able to improve the Quality of Service (QoS) OSPF routing protocol on VoIP networks, specifically on the parameters of throughput and jitter in service over Internet Protocol (VoIP) [6]. This research develops a network model and VPN network implementation with a routing protocol for the Multiprotocol Label Switching (MPLS) network implemented at the AMIK Indonesia College. After the model design is carried out, the network implementation is continued, so that the MPLS network performance will be tested and compared to the performance without MPLS using the model the research team planned.

2 LITERATURE REVIEW

2.1 Virtual Private Network (VPN)

Virtual Private Network (VPN) is a private network that connects one network node to another network node using a public network (internet). The data passed will be encapsulated and encrypted to ensure confidentiality. VPN networks are connected by communication service providers (Service Providers) through their routers to other routers using encrypted internet lines between two points. The security system on VPN uses several layers, i.e.

a. **Tunneling Method**
   Create virtual tunnels on public networks using protocols such as Point to Point Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Generic Routing Encapsulation (GRE) or IPSec. PPTP and L2TP are Layer 2 Tunneling Protocols, the function is to do payload wrapping on PPTP frames to be passed on the network. Whereas IPS stayed at layer 3, used packets, and would wrap IP headers before sending them to the network.

b. **Encryption Method**
   To wrap a data packet that passes in tunneling, the data passed on the packaging will be changed with certain cryptographic algorithms such as DES, 3DES, and AES.

- *Fathurrahmad is lecture at Department of Informatics AMIK Indonesia, Indonesia. E-mail: fathurrahmad@amikindonesia.ac.id*
- *Salman Yusuf is lecture at Department of Informatics AMIK Indonesia, Indonesia. E-mail: salmanyusuf@amikindonesia.ac.id*
- *Taufiq Iqbal is lecture at Department of Informatics AMIK Indonesia, Indonesia. E-mail: taufiqiqbal@amikindonesia.ac.id*
- *Abdussalam is lecture at Department of Informatics AMIK Indonesia, Indonesia. E-mail: abdussalam@amikindonesia.ac.id*

c. User authentication method

Because many users who will access usually use many user authentication methods such as Remote Access Dial-in user services (RADIUS) and Digital Certificates.

d. Data integrity

Data packets that are passed on public networks need to guarantee data integrity (integrity), whether changes occur or not. The VPN method uses HMA C-MD5 or HMA C-SHA1 so that the data packet does not change at the time of transmission [7].

2.2 Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a packet delivery technology on high-speed backbone networks that combines some of the advantages of circuit-switched and packet-switched communication systems that give birth to better technology than both [8]. MPLS is a network architecture defined by IETF to combine the label swapping mechanism at layer 2 with routing at layer 3 to speed up packet delivery [9]. Packets in MPLS are forwarded by routing protocols such as OSPF, BGP or EGP, routing protocols at layer 3 of the OSI system, while MPLS is located between layers 2 and 3 [10].

2.3 Routing

In a packet switching system, routing refers to the process of selecting a path for sending packets, and a router is a device that performs this task [11]. Routing in IP involves both existing gateways and hosts. When an application program in a host will communicate, the TCP / IP protocol will generate it in the form of many datagrams. The host must make a routing decision to choose the delivery path. A routing protocol is a protocol used by routers to exchange routing information [12]. Routers on TCP / IP networks form a routing table based on routing information that is exchanged at certain intervals. The routing protocol has the ability to dynamically build information in the routing table. If there is a change in the routing protocol network is able to update the routing information. Routing on TCP / IP networks is divided into 2 types :

a. Interior Gateway Protocol (IGP)

A routing protocol that handles routing in an autonomous system.

b. Exterior Gateway Protocol (EGP)

A routing protocol that handles routing between autonomous systems. An autonomous system is an internet network system that is under one administrative and technical control.

There are several types of routing protocols that are often used, including:

a. Routing Information Protocol (RIP)
b. Enhanced Interior Gateway Protocol (EIGRP)
c. Open Shortest Path First (OSPF)
d. Border Gateway Protocol (BGP)

Based on the main division, the routing protocols included in IGP are RIP, EIGRP, and OSPF, while those included in EGP are BGP. EGP has the ability to determine policy routing because some autonomous systems on the internet have policies in terms of routing [13]. For the implementation of routing in this IGP policy is not required [14].

2 RESEARCH METHOD

2.1 Method

This research will use the literature study method intended to obtain and study data contained in personal computers that are connected to the network in the AMIK Indonesia computer network laboratory. Data collected according to the focus of research in the form of network topology used, addressing IP addresses and MPLS techniques. The collection of data/information is at the same time researchers as simulations to imitate or represent the behavior of real systems.

2.2 Software used

In building a computer network simulator based on GUI (Graphical User Interface) in this study using simulators namely GNS3 and Visio 2016 as network architecture design.

2.3 System Requirements Analysis

This analysis was conducted to determine what operational needs are needed in making VPN computer network simulations with Routing Protocol on Multiprotocol Label Switching (MPLS) networks covering hardware, software and brainware requirements.

a. Hardware

- NoteBook with Intel Core i3 2.2 GHz Processor
- 4 Gb Random Access Memory (RAM) capacity
- Hard drive with a capacity of 1 TB
- VGA nVidia 820m.

b. (Software

- Microsoft Windows 8.1
- GNS3 network simulation
- Microsoft Visio Network Design 2016
- Virtual Machines (Virtual Box, Qemu Emulator)
- CISCO ISO Program

c. Brainware

Human Resources Needs are individuals who will be directly involved in making VPN network simulations with Routing Protocol on MPLS Networks. The needs are limited to users who can design and run this system later.

2.4 System Design

The design referred to here is the topology or physical form of the simulation to be made. Includes IP Addresses on each interface used. The network implementation that will be carried out in this study is made based on Figure 1. The network connectivity described occurs between 2 hosts through 3 connected routers. For addresses that are configured are IPv4 and IPv6 addresses. Where each host is configured with an IPv6 address. Whereas the three routers that are directly connected to the host are configured with IPv4 and IPv6 addresses. For the addressing table for each router and host can be seen in the table below.

TABLE 1.
Setting IP Address on each interface

Device	*Interface*	*IPv4 Address*	*IPv6 Address*
PC0	*Fa0/0*	*192.168.10.1/24*	*2001:db8:1:a::10/64*

PC1	*Fa0/0*	*192.168.10.2/24*	*2001:db8:1:a::11/64*
PC2	*Fa0/0*	*192.168.10.3/24*	*2001:db8:1:a::12/64*
RouterA	*Gig0/0*	*192.168.10.254/24*	*2001:db8:1:a::1/64*
	Se0/0/0	*10.2.2.1/24*	*2001:2:2:2:1::1/64*
PC3	*Fa0/0*	*192.168.20.1/24*	*2001:db8:1:b::10/64*
PC4	*Fa0/0*	*192.168.20.2/24*	*2001:db8:1:b::11/64*
PC5	*Fa0/0*	*192.168.20.3/24*	*2001:db8:1:b::12/64*
RouterB	*Gig0/0*	*192.168.20.254/24*	*2001:db8:1:b::1/64*
	Se0/0/0	*10.2.2.2/24*	*2001:2:2:2::2/64*
RouterC	*Gig0/0*	*192.168.30.254/24*	*2001:db8:1:b::2/64*
	Se0/0/0	*10.2.2.3/24*	*2001:2:2:2::3/64*

3 RESULTS

From this simulation several things have been done, viz:

a. Configure IPv4 on the host and router
b. Configuring IPv6 on Host and Router
c. dynamic routing configuration

The network framework is built as shown in Figure 1 below.

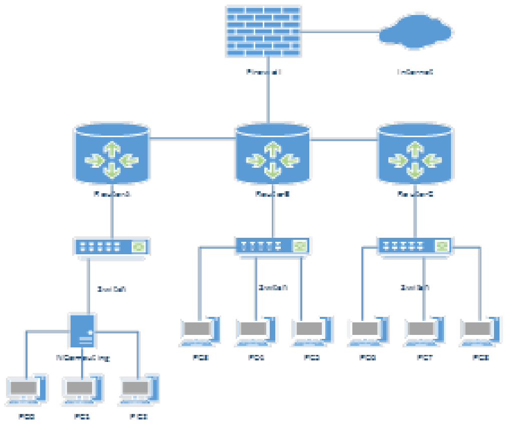


Fig. 1. *Network Framework that is built consists of 3 Routers, on Router A there are n-Computing servers, while Routers B and C are servers in different spaces and places.*

a. Configuring IPv6 on the RouterA

RouterA> enable
RouterA # configure terminal
RouterA (config) # ipv6 unicast-routing
RouterA (config) #int Gig0 / 0
RouterA (config-if) # ipv6 enable
RouterA (config-if) # ipv6 Address 2001: db8: 1: a :: 1/64
RouterA (config-if) #no shutdown.

Configuration on RouterA on WAN addresses (Se0 / 0/0)
RouterA (config) #int se0 / 0/0
RouterA (config-if) #interface serial0 / 0/0
RouterA (config-if) # ipv6 enable
RouterA (config-if) # ipv6 Address 2001: 2: 2: 2 :: 1/64
RouterA (config-if) #no sh

b. Configuring IPv6 on the RouterB

RouterB (config-if) # ipv6 unicast-routing
RouterB (config) #int Gig0 / 0
RouterB (config-if) # ipv6 enable
RouterB (config-if) # ipv6 Address 2001: db8: 1: b :: 1/64
RouterB (config-if) #no sh

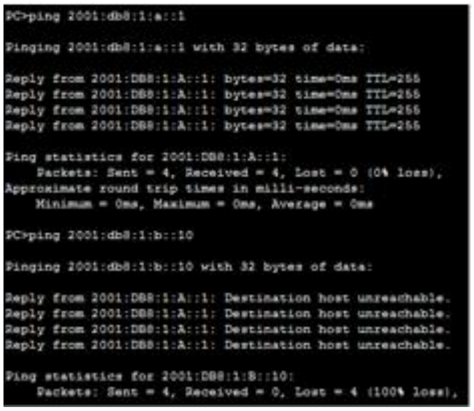
Configuration on RouterB at WAN address (Se0 / 0/0)
RouterB (config-if) #interface se0 / 0/0
RouterB (config-if) # ipv6 enable
RouterB (config-if) # ipv6 Address 2001: 2: 2: 2 :: 2/64
RouterB (config-if) #no sh

c. Configuring IPv6 on the RouterC

RouterB (config-if) # ipv6 unicast-routing
RouterB (config) #int Gig0 / 0
RouterB (config-if) # ipv6 enable
RouterB (config-if) # ipv6 Address 2001: db8: 1: c :: 1/64
RouterB (config-if) #no sh

Configuration on RouterC on WAN addresses (Se0 / 0/0)
RouterC (config-if) #interface se0 / 0/0
RouterC (config-if) # ipv6 enable
RouterC (config-if) # ipv6 Address 2001: 2: 2: 2 :: 3/64
RouterC (config-if) #no sh

Dynamic routing using RIP between routers results, All devices in this simulation already use dual-stack. From the test results on this simulation if a connection test (ping) is performed from PC0 (2001: db8: 1: a :: 10) to the Gateway (2001: db8: 1: a :: 1) the status is successful, but if pinged to PC3 on a different network cannot, because the routing process has not been done for IPv6 itself. Can be seen in the image below.



```
PC>ping 2001:db8:1:a::1

Pinging 2001:db8:1:a::1 with 32 bytes of data:

Reply from 2001:DB8:1:A::1: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:1:A::1: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:1:A::1: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:1:A::1: bytes=32 time=0ms TTL=255

Ping statistics for 2001:DB8:1:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 2001:db8:1:b::10

Pinging 2001:db8:1:b::10 with 32 bytes of data:

Reply from 2001:DB8:1:A::1: Destination host unreachable.
Reply from 2001:DB8:1:A::1: Destination host unreachable.
Reply from 2001:DB8:1:A::1: Destination host unreachable.
Reply from 2001:DB8:1:A::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:B::10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig. 2. *Error on PC0 to PC3, Test ping to PC3 on a different network, because the IPv6 routing process has not been set.*

To do routing so that it can be connected from one network to another, dynamic routing will be used using RIP Routing. The steps are as follows:

a. RIP Routing configuration on RouterA

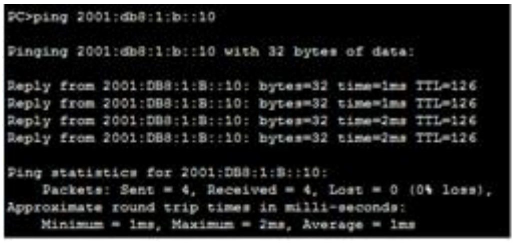
RouterA> en
RouterA # conf t
RouterA (config) # ipv6 router rip ciscorip
RouterA (config-rtr) #exit
RouterA (config) #int gig0 / 0
RouterA (config-if) # ipv6 rip ciscorip enable

```
RouterA (config-if) #ex
RouterA (config) #int se0 / 0/0
RouterA (config-if) # ipv6 rip ciscorip enable
RouterA (config-if) #exit
RouterA (config) #end
RouterA #
```

b. Configuring RIP Routing on RouterB

```
RouterB (config) # ipv6 router rip ciscorip
RouterB (config-rtr) #exit
RouterB (config) #interface gig0 / 0
RouterB (config-if) # ipv6 rip ciscorip enable
RouterB (config-if) #ex
RouterB (config) #int se0 / 0/0
RouterB (config-if) # ipv6 rip ciscorip enable
RouterB (config-if) #exit
RouterB (config) #end
RouterB #
```

The last step that has not been done is to test the connection from PC0 to PC3.



```
PC>ping 2001:db8:1:b::10

Pinging 2001:db8:1:b::10 with 32 bytes of data:

Reply from 2001:DB8:1:B::10: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:1:B::10: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:1:B::10: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:1:B::10: bytes=32 time=2ms TTL=126

Ping statistics for 2001:DB8:1:B::10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Fig. 3. *The connection result from PC0 to PC3 was successful.*

4 CONCLUSION

The conclusion obtained from this study is that MPLS VPN really provides bandwidth efficiency on the backbone, the application of MPLS VPN networks has been functionally functional according to the initial plan of this study and the author also managed to configure different networks and obtain a stable bandwidth capacity.

5 ACKNOWLEDGMENT

Thank you to the Directorate General of Research and Technology Strengthening and Development of the Ministry of Research, Technology and Higher Education (DITLITABMAS), as research funders for the 2019 Beginner Lecturer Research Grant (PDP). Furthermore, to the Chairperson of LPPM and staff and to the Team of Laboratory Research Supporters and also to Lecturers and AMIK Indonesia academics who always provide support to carry out this research in accordance with the expectations of the author.

6 REFERENCES

[1] Fathurrahmad, F. and Yusuf, S., 2019. Implementasi Jaringan VPN dengan Routing Protocol terhadap Jaringan Multiprotocol Label Switching (MPLS). Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi), 3(1), pp.29-33.

[2] Safitri, R., 2010. Implementasi dan Analisa Perbandingan QoS pada Jaringan VPN Berbasis MPLS menggunakan Routing Protocol RIPv2, EIGRP dan OSPF terhadap Tunneling IPsec untuk Layanan IP-Based Video Conference. Universitas Indonesia. Jakarta.

[3] Border, J., Dillon, D. and Pardee, P., Hughes Network Systems LLC, 2015. Method and system for communicating over a segmented Virtual Private Network (VPN). U.S. Patent 8,976,798.

[4] Fitri, F., Yamin, M. and Aksara, L.B., 2017. PERBANDINGAN METODE DIFFERENTIATED SERVICE DENGAN METODE INTEGRATED SERVICE UNTUK ANALISA QUALITY OF SERVICE (QOS VIDEO STREAMING) PADA JARINGAN MULTI PROTOCOL LABEL SWITCHING (MPLS). semanTIK, 3(1).

[5] Nurhasanah, N.A., Wahidah, I. and Cahyono, B., 2017. IMPLEMENTASI SEAMLESS MULTIPROTOCOL LABEL SWITCHING (MPLS) PADA JARINGAN MPLS. Prosiding SENIATI, 3(1), pp.45-1.

[6] Susanto, B.M. and Atmaji, E.S.J., 2017. Performa Protokol Routing OSPF dan BGP pada Jaringan VOIP MPLS dengan Tunelling L2TP/IPSec. Prosiding..

[7] Stiawan, D. and Rini, D.P., 2009. Optimalisasi Interkoneksi VPN Menggunakan Hardware Based dan Iix (Indonesia Internet Exchange) Sebagai Alternatif Jaringan Skala Luas (WAN). Jurnal Generic, 4(1), pp.57-68.

[8] Supriyadi, A. and Gartina, D., 2007. Memilih Topologi Jaringan Dan Hardware Dalam Desain Sebuah Jaringan Komputer. Informatika Pertanian, 16(2), pp.1037-1053

[9] Panhwar, M.A., Memon, K.A., Abro, A., Zhongliang, D., Khuhro, S.A. and Ali, Z., 2019, July. Efficient Approach for optimization in Traffic Engineering for Multiprotocol Label Switching. In 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC) (pp. 1-7). IEEE.

[10] Beyene, A.M. and Argaw, S.A., 2019, May. Improving Quality of Service of Border Gateway Protocol Multiprotocol Label Switching Virtual Private Network of EthioTelecom Service Level Agreements. In International Conference on Information and Communication Technology for Development for Africa (pp. 278-288). Springer, Cham.

[11] Meyer, H., Sancho, J.C., Mrdakovic, M., Miao, W. and Calabretta, N., 2018. Optical packet switching in HPC. An analysis of applications performance. Future Generation Computer Systems, 82, pp.606-616.

[12] Furukawa, H., Mendinueta, J.M.D., Wada, N. and Harai, H., 2017. Spatial and spectral super-channel optical packet switching system for multigranular SDM-WDM optical networks. Journal of Optical Communications and Networking, 9(1), pp.A77-A84.

[13] Sari, L.O., Safrianti, E. and Adhil, I.F., Analisa Perbandingan Pengaruh Routing Protocol Ipv4 Dengan Ipv6 Studi Kasus Jaringan Data PT. PERTAMINA RU II DUMAI. Skripsi. Universitas Indonesia.