Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

journal homepage: http://journal.lembagakita.org/index.php/jtik

Implementasi Jaringan VPN dengan *Routing Protocol* terhadap Jaringan *Multiprotocol Label Switching* (MPLS)

Fathurrahmad [1], Salman Yusuf [2]

[1,2] *AMIK Indonesia*

a r t i c l e i n f o

Article history:
Received 10 April 2019
Received in revised form
9 Mei 2019
Accepted 27 Juni 2019
Available on*line* Juni 2019

DOI:
https://doi.org/10.35870/jtik.v3i1.83

Keywords:
Implementation; VPN; Multi Protocol Label Switching.

Kata Kunci:
Implementasi; VPN; *Multi Protocol Label Switching.*

a b s t r a c t

The convergence of the internet and telecommunications is growing, with applications in it increasingly dependent on the availability of large bandwidth, with its QoS settings requiring networks and elements in them that provide full support for data security and increased network performance. The need for data transmission technology that not only facilitates routing and discovery of the best paths but can also provide security in data communication. This study discusses the implementation of VPN networks with routing protocols on the Multiprotocol Label Switching (MPLS) network. After implementation, MPLS network performance will be tested and compared to performance without MPLS using the model planned by the researcher. The specific purpose of this study is to show how routing protocols play an important role in strengthening data communication traffic management that supports MPLS capabilities of VPN networks and is applied to the AMIK Indonesia network architecture. This research will use the literature study method which is intended to obtain and study data contained in computers connected to networks in the AMIK Indonesia computer network laboratory. The conclusion obtained from this study is that MPLS VPN provides bandwidth efficiency in the backbone, MPLS VPN network applications have functioned functionally according to the initial plan of the study and the authors have also managed to configure different networks and obtain stable bandwidth.

a b s t r a k

Konvergensi internet dan telekomunikasi yang berkembang, dengan aplikasi di dalamnya yang semakin tergantung pada ketersediaan *bandwidth* besar, dengan pengaturan QoS-nya membutuhkan jaringan dan elemen di dalamnya yang memberikan dukungan penuh untuk keamanan data dan peningkatan kinerja jaringan. Kebutuhan teknologi pengiriman data yang tidak hanya memfasilitasi perutean dan penemuan lintasan terbaik tetapi juga dapat memberikan keamanan dalam komunikasi data. Penelitian ini membahas implementasi jaringan VPN dengan protokol *routing* pada jaringan *Multiprotocol Label Switching* (MPLS). Setelah implementasi, kinerja jaringan MPLS akan diuji dan dibandingkan dengan kinerja tanpa MPLS menggunakan model yang direncanakan peneliti. Tujuan khusus dari penelitian ini adalah untuk menunjukkan bagaimana protokol *routing* memainkan peran penting dalam memperkuat manajemen lalu lintas komunikasi data yang mendukung kemampuan MPLS dari jaringan VPN dan diterapkan pada arsitektur jaringan AMIK Indonesia. Penelitian ini akan menggunakan metode studi literatur yang dimaksudkan untuk memperoleh dan mempelajari data yang terkandung dalam komputer yang terhubung ke jaringan di laboratorium jaringan komputer AMIK Indonesia. Kesimpulan yang didapat dari penelitian ini adalah bahwa MPLS VPN memberikan efisiensi *bandwidth* pada *backbone*, aplikasi jaringan VPN MPLS telah berfungsi secara fungsional sesuai dengan rencana awal penelitian dan penulis juga berhasil mengkonfigurasi jaringan yang berbeda dan memperoleh *bandwidth* yang stabil.

*Corresponding author. Email: fathurrahmad@amikindonesia.ac.id[1]

1. Latar Belakang

Berkembangnya konvergensi *internet* dan telekomunikasi, dengan aplikasi didalamnya yang kian tergantung pada ketersediaan *bandwidth* yang besar, dengan pengaturan QoS-nya membutuhkan jaringan dan elemen didalamnya yang memberi dukungan penuh terhadap keamanan data dan peningkatan kinerja jaringan. Maka dibutuhkan teknologi pengiriman data yang tidak hanya memudahkan *routing* dan *discovery* lintasan terbaik, namun juga dapat memberikan keamanan dalam melakukan komunikasi data. IETF menstandarkan solusi *Multi Protocol Label Switching* (MPLS) sebagai pengembangan dari teknologi *Virtual Private Network* (VPN) untuk meningkatkan kinerja *forwarding* (Safitri, 2010) dan kecerdasan *traffic engineering* pada jaringan *packet-based*. Teknologi ini dapat menyederhanakan proses *routing* yang menjadi beban *router* karena harus menganalisa setiap *header* IP yang masuk, serta mengoptimalkan pemilihan path melalui kemampuan manajemen *class of service* dan *traffic engineering*. *Virtual Private Network* (VPN) memungkinkan berkomunikasi secara aman di seluruh jaringan publik dengan sedemikian rupa sehingga jaringan publik beroperasi sebagai satu atau beberapa tautan komunikasi pribadi (Border, Dillon, dan Pardee, 2015). Penelitian ini membahas mengenai implementasi jaringan VPN dengan *routing protocol* terhadap jaringan *Multiprotocol Label Switching* (MPLS). Setelah dilakukan implementasi, performansi jaringan MPLS tersebut akan diuji dan dibandingkan dengan performansi tanpa MPLS dengan menggunakan model yang peneliti rencanakan.

2. Tinjauan Pustaka

Virtual Private Network (VPN)

Virtual Private Network (VPN) merupakan sebuah jaringan *private* yang menghubungkan satu *node* jaringan ke *node* jaringan lainnya dengan menggunakan jaringan publik (*internet*). Data yang dilewatkan akan dibungkus (*encapsulation*) dan dienkripsi agar terjamin kerahasiaannya.

Jaringan VPN dikoneksikan oleh penyedia jasa komunikasi (*Service Provider*) melalui *router*nya ke *router-router* lain dengan menggunakan jalur *internet* yang telah dienkripsi diantara dua titik. Sistem keamanan di VPN menggunakan beberapa lapisan, yaitu :

a. Metode *tunneling* (terowongan)
   Membuat terowongan virtual di atas jaringan publik menggunakan protokol seperti *Point to Point Protocol* (PPTP), Layer 2 *Tunneling Protocol* (L2TP), Generic *Routing Encapsulation* (GRE) atau IPSec (Hikmaturokhman, Pamungkas, dan Berlianti, 2015). PPTP dan L2TP adalah Layer 2 *Tunneling Protocol*, keduanya melakukan pembungkusan payload pada frame PPTP untuk dilewatkan pada jaringan. Sedangkan IPSec berada di layer 3, menggunakan paket, dan akan melakukan pembungkusan IP *header* sebelum dikirim ke jaringan.
b. Metode enkripsi
   Untuk membungkus paket data yang lewat di dalam *tunneling*, data yang dilewatkan pada pembungkusan tersebut akan dirubah dengan algoritma kriptografi tertentu seperti DES, 3DES dan AES.
c. Metode autentikasi *user*
   Karena banyak *user* yang akan mengakses biasanya digunakan beberapa metode autentikasi *user* seperti *Remote Acces Dial* in *user Services* (RADIUS) dan *Digital Certificates*.
d. Integritas data
   Paket data yang dilewatkan pada jaringan publik perlu penjaminan integritas (keutuhan) data, apakah terjadi perubahan atau tidak. Metode VPN menggunakan HMA C-MD5 atau HMA C-SHA1 agar paket data tidak berubah pada saat pengiriman (Stiawan dan Rini, 2009)

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) adalah teknologi penyampaian paket pada jaringan *backbone* (jaringan utama) berkecepatan tinggi yang menggabungkan beberapa kelebihan dari sistem komunikasi *circuit-switched* dan *packet-switched* yang melahirkan teknologi yang lebih baik dari keduanya (Supriyadi dan Gartina, 2007). MPLS adalah arsitektur jaringan yang didefinisikan oleh IETF untuk memadukan mekanisme label swapping di layer 2 dengan *routing* di layer 3 untuk mempercepat pengiriman paket. Paket-paket pada MPLS diteruskan dengan protokol *routing* seperti OSPF, BGP atau EGP, Protokol *routing* pada layer 3 sistem OSI, sedangkan MPLS berada diantara layer 2 dan 3.

Routing

Dalam suatu sistem *packet switching*, *routing* mengacu

pada proses pemilihan jalur untuk pengiriman paket, dan *router* adalah perangkat yang melakukan tugas tersebut. Perutean dalam IP melibatkan baik *gateway* maupun *host* yang ada. Ketika suatu program aplikasi dalam suatu *host* akan berkomunikasi, protokol TCP/IP akan membangkitkannya dalam bentuk banyak datagram. *Host* harus membuat keputusan perutean untuk memilih jalur pengiriman. Protokol *routing* adalah protokol yang digunakan oleh *router-router* untuk saling bertukar informasi *routing*. *Router-router* pada jaringan TCP/IP membentuk tabel *routing* berdasarkan informasi *routing* yang dipertukarkan setiap selang waktu tertentu. Protokol *routing* mempunyai kemampuan untuk membangun informasi dalam tabel *routing* secara dinamik. Apabila terjadi perubahan jaringan protokol *routing* mampu memperbaharui informasi *routing* tersebut. *Routing* pada jaringan TCP/IP dibagi menjadi 2 macam :

a. Interior *Gateway* Protocol (IGP)
   Merupakan protokol *routing* yang menangani perutean dalam suatu *autonomous system*.
b. Exterior *Gateway* Protocol (EGP)
   Merupakan protokol *routing* yang menangani *routing* antar autonomous system. Autonomous system adalah suatu sistem jaringan *internet* yang berada dalam satu kendali administrasi dan teknis.

Ada beberapa macam protokol *routing* yang sering digunakan, diantaranya :

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

Berdasarkan pembagian utamanya maka protokol *routing* yang termasuk dalam IGP adalah RIP, EIGRP, dan OSPF, sedangkan yang termasuk dalam EGP adalah BGP. EGP memiliki kemampuan untuk menentukan policy *routing* karena sebagian autonomous system di *internet* mempunyai kebijakan dalam hal *routing*. Untuk pelaksanaan *routing* dalam IGP policy ini tidak diperlukan (Sari, Safrianti, dan Adhil. 2010).

3. Metode Penelitian

Penelitian ini akan menggunakan metode studi literatur dimaksudkan untuk memperoleh dan mempelajari data-data yang terdapat pada personal komputer yang terhubung ke jaringan di laboratorium jaringan komputer AMIK Indonesia. Data yang dihimpun sesuai fokus penelitian berupa topologi jaringan yang digunakan, pengalamatan IP *Address* serta teknik MPLS. Pengumpulan data/informasi ini peneliti sekaligus sebagai simulasi untuk menirukan atau merepresentasikan perilaku dari sistem nyata.

Perangkat Lunak yang digunakan

Dalam membangun simulator jaringan komputer berbasis GUI (*Graphical User Interface*) pada penelitian ini menggunakan simulator yaitu GNS3 dan Visio 2016 sebagai desain arsitektur jaringan.

Analisis Kebutuhan Sistem

Analisis ini dilakukan untuk mengetahui kebutuhan operasional apa saja yang dibutuhkan dalam pembuatan simulasi jaringan komputer VPN dengan *Routing Protocol* pada Jaringan *Multiprotocol Label Switching* (MPLS) yang meliputi kebutuhan *hardware*, *software* dan *brainware*.

a. Kebutuhan Perangkat Keras (*Hardware*)
   - Laptop dengan Prosesor Intel Core i3 2.2 GHz
   - Kapasitas Random Access Memory (RAM) 4 Gb
   - Hardisk dengan kapasitas 1 TB
   - VGA nVidia 820m.

b. Kebutuhan Perangkat Lunak (*Software*)
   - Microsoft Windows 8.1
   - Simulasi jaringan GNS3
   - Desain Jaringan Microsoft Visio 2016
   - Virtual Mesin (Virtual Box, Qemu Emulator)
   - Program iso CISCO

c. Kebutuhan *Brainware*
   Kebutuhan Sumber Daya Manusia merupakan individu yang akan terlibat langsung dalam pembuatan simulasi jaringan VPN dengan *Routing Protocol* pada Jaringan MPLS (Sismoro dan Artha, 2016). Kebutuhan yang dipakai sebatas pengguna yang dapat mendesain dan menjalankan sistem ini nantinya.

Desain Sistem

Perancangan desain yang dimaksud disini adalah topologi atau bentuk secara fisik dari simulasi yang

akan dibuat. Meliputi IP *Address* pada setiap *interface* yang digunakan. Dalam implementasi jaringan yang akan dilakukan dalam penelitian ini dibuat berdasarkan gambar 1. konektivitas jaringan yang digambarkan tersebut terjadi antara 2 *host* yang melalui 3 buah *router* terhubung.

Untuk pengalamatan yang dikonfigurasi adalah alamat IPv4 dan IPv6. Dimana masing-masing *host* dikonfigurasi dengan alamat IPv6. Sedangkan ketiga *router* yang terkoneksi langsung dengan *host* dikonfigurasi dengan alamat IPv4 dan IPv6. Untuk table pengalamatan masing-masing *router* dan *host* dapat dilihat pada tabel dibawah ini.

Tabel 1. Pengaturan IP *Address* di setiap *interface*

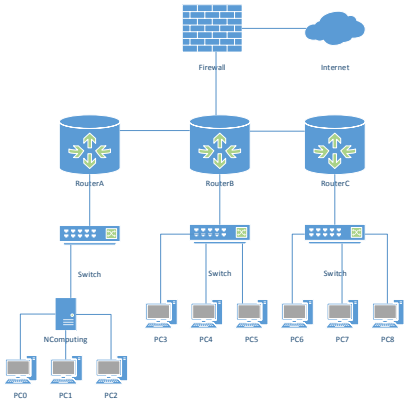
Device	*Interface*	IPv4 *Address*	IPv6 *Address*
PC0	Fa0/0	192.168.10.1/24	2001:db8:1:a::10/64
PC1	Fa0/0	192.168.10.2/24	2001:db8:1:a::11/64
PC2	Fa0/0	192.168.10.3/24	2001:db8:1:a::12/64
*Router*A	Gig0/0	192.168.10.254/24	2001:db8:1:a::1/64
	Se0/0/0	10.2.2.1/24	2001:2:2:2:1::1/64
PC3	Fa0/0	192.168.20.1/24	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
*Router*B	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
*Router*C	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

4. Hasil dan Implementasi

Dari simulasi ini telah dilakukan beberapa hal, yaitu:

b. Konfigurasi IPv4 di *host* dan *Router*
c. Konfigurasi IPv6 di *host* dan *Router*
d. konfigurasi *routing* dynamic

adapun kerangka jaringan yang dibangun seperti terlihat pada gambar 1 berikut.



Gambar 1. Kerangka Jaringan yang dibangun

a. Konfigurasi IPv6 pada *Router*A

```
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.
```

Konfigurasi pada *Router*A pada alamat WAN (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. Konfigurasi IPv6 pada *Router*B

```
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
```

Konfigurasi pada *Router*B pada alamat WAN (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. Konfigurasi IPv6 pada *Router*C

```
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
```

Konfigurasi pada *Router*C pada alamat WAN (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
```

Hasil Implementasi

Dari simulasi ini telah dilakukan beberapa hal, yaitu:

a. Konfigurasi IPv4 di *host* dan *Router*
b. Konfigurasi IPv6 di *host* dan *Router*
c. konfigurasi *routing* dynamic

5. Kesimpulan

Kesimpulan yang diperoleh dari penelitian ini bawwa MPLS VPN sangat memberikan efisiensi *badwith* pada *backbone*, penerapan jaringan MPLS VPN secara fungsional telah berjalan baik sesuai dengan rencana

awal penelitian ini dan penulis juga berhasil mengkofigurasi jaringan yang berbeda dan mendapatkan kapasitas *bandwith* yang stabil.

6. Ucapan Terima Kasih

Ucapan terima kasih sebesar-besarnya kepada Ditjen Penguatan Riset dan Pengembangan Kementerian Riset, Teknologi, dan Pendidikan Tinggi selaku penyandang dana penelitian pada hibah Penelitian Dosen Pemula (PDP) Tahun Anggaran 2019. Selanjutnya kepada Ketua LPPM dan jajaran staff dan kepada Tim pembantu peneliti laboratorium dan juga kepada Dosen dan pihak akademik AMIK Indonesia yang selalu memberikan dukungan agar terlaksananya penelitian ini sesuai dengan harapan penulis.

7. Daftar Pustaka

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.

Cisco Systems Learning. 2006. Implementing Secure Converged Wide Area Networks (Volume 1). San Jose : Cisco Systems Inc.

Hikmaturokhman, A., Pamungkas, W. and Berlianti, L., 2015. Analisa Model Propagasi Cost 231 Multiwall pada Perancangan Jaringan Indoor Femtocell HSDPA menggunakan Radiowave Propagation Simulator. Purwokerto: Sekolah Tinggi Teknologi Telematika Telkom.

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.

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.

Sismoro, H. and Artha, E.U., 2016. Perancangan Dan Implementasi Static Tunnel Sebagai Media Pembelajaran Jaringan Komputer Menggunakan Dual Stack. Data Manajemen dan Teknologi Informasi (DASI), 17(1), pp.27-32.

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.

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