SEMESTA TEKNIKA
Vol. XXX No.XXX (XXX): xxx-xxx

PERANCANGANAN SISTEM REDUNDANSI *VIRTUAL PRIVATE NETWORK* MELALUI JARINGAN INTERNET DENGAN *DYNAMIC MULTI VIRTUAL PRIVATE NETWORK*

(Designing Virtual Private Network Redundancy Systems Through Internet Networks With Dynamic Multi Virtual Private Networks)

ANDRE KISRIYANTO, SLAMET RIYADI, S.T., M.SC., PH.D., RONALD ADRIAN, S.T., M.ENG.

ABSTRACT

The development of data communication embedded in the process of different secure location activities is a major requirement for a company today. VPN can connect between areas with certain encryption methods as a security medium [16]. A single VPN network infrastructure is not enough to provide redundancy for the failure of network connectivity that cannot be calculated. Some WAN infrastructure technology solutions and VPN protocols have not been able to revitalize the problem of a backup VPN without building new infrastructure [11] [17] with failover mechanisms [10]. Dynamic Multipoint Virtual Private Network technology with routing distribution mechanism can build redundancy in failover VPN multiples sites utilizing public WAN as a backup VPN, supported by a hub and spoke, integrating full mesh topology, and providing data encryption when passing through the Internet. The Network Development Life Cycle (NDLC) method includes requirements analysis, network topology design, simulation and prototyping, implementation, network observation, and network management [18], but this research focuses on Analysis, Design and Simulation prototyping as well as testing. The QoS (Quality of Services) parameter which consists of throughput, delay, jitter and packet loss gets very good values according to ITU-T G.114 [23]. However, the difference in QoS quality obtained by MPLS-L3VPN is better than DMVPN, due to IPSec which has not been implemented in MPLS-L3VPN while DMVPN is applied [8] [7]. The results of real-time failover connection simulation tests show the successful status of the MPLS VPN to the DMVPN scenario applied without building new infrastructure.

Keywords: Redundancy, VPN, Internet, DMVPN, NDLC

1. PENDAHULUAN

Perkembangan teknologi yang sangat pesat dengan beragamnya teknologi informasi yang disematkan sangat mempengaruhi pola bisnis dan strategi bisnis perusahaan terutama komunikasi data yang menjadi kebutuhan utama bagi sebuah perusahaan saat ini. Penggunaan akan komunikasi data tentu tidak hanya sebatas area lokal saja, namun perusahaan cenderung mempunyai banyak area-area kantor cabang yang tersebar di lokasi tertentu.

Virtual Private Network (VPN) merupakan suatu koneksi antar dua jaringan yang dibuat untuk mengoneksikan kantor pusat, kantor cabang dan lain-lain menggunakan infrastruktur telekomunikasi dan metode enkripsi [16]. Teknologi infrastuktur WAN

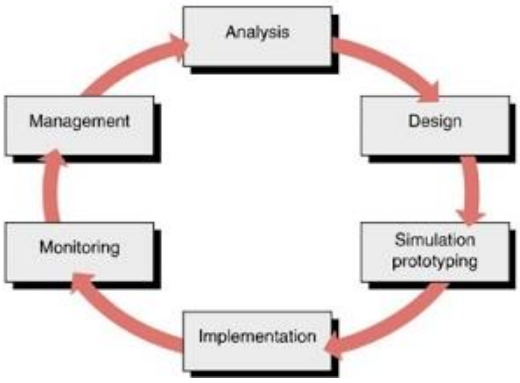
seperti X.25, ATM dan Frame Relay memberikan jalur transmisi antar berbagai lokasi. Meskipun ATM merupakan teknologi terbaru yang memberikan Throughput tinggi dan sedikit delay akan tetapi meminimalisirkan flow dan error controls-nya sehingga tidak sedikit terjadi overload. sedangkan flow dan error controls pada X.25 terdapat pada link-to-link berdampak overload yang tinggi dan Frame Relay terdapat pada end-to-end berdampak overload yang sedang. Jaringan ATM dan Frame relay lebih efisien daripada X.25 berdasarkan kehandalan, kualitas dan menyediakan multiprotocol [17]. Adapun kekurangan ketiga teknologi WAN tersebut yaitu tidak adanya suatu pengelolaan Quality of Service (QoS) dan saat ini digantikan sebagian besar oleh MPLS VPN dimana aplikasi seperti ERP, Citrix, RDP, VoIP dan video yang membutuhkan kualitas yang handal.

Dalam memenuhi kebutuhan komunikasi VPN yang menggunakan MPLS VPN sebagai media WAN tersebut, terkadang kegagalan sebuah konektifitas jaringan tidak dapat diperhitungkan waktu terjadinya ketika berhadapan dengan hardware jaringan dan kondisi alam. Redundansi pada VPN merupakan bentuk kesiagaan perusahaan dalam ketersediaan komunikasi antara area dengan mekanisme pergantian secara otomatis dari jalur utama ke jalur cadangan. Menurut [2], dalam memilih teknologi VPN secara site-to-site ada beberapa unsur penting yang disarankan untuk mendekati solusi kebutuhan perusahaan yaitu dengan mengetahui parameter-parameter sebagai berikut; QoS requirement, Topology requirement, Security requirement dan Protocol support requirement.

Berbagai solusi yang diperkenalkan dalam menyediakan VPN cadangan, antara lain teknologi infrastruktur WAN yaitu MPLS VPN dengan seluruh kelebihannya dan protokol VPN seperti PPTP, L2TP, OpenVPN, DMVPN dan GETVPN. Permasalahan dalam memilih teknologi VPN adalah bagaimana membangun redundansi dan tidak memerlukan penambahan infrastruktur baru, melainkan dapat memanfaatkan jalur Internet dengan mekanisme routing distribution agar dapat berpindah otomatis ke VPN cadangan. Berdasarkan relevansi masalah tersebut, MPLS VPN belum memberikan solusi dengan memanfaatkan infrastruktur WAN publik yang mana MPLS hanya menyediakan WAN tersendiri serta perusahaan juga memerlukan penambahan infrastruktur baru tanpa memanfaatkan sumber daya yang ada [11]. Sedangkan protokol VPN yang telah disebutkan, juga belum dapat mendukung mekanisme routing distribution agar dapat berpindah otomatis dari VPN utama. Berbeda dengan DMVPN dan GETVPN yang dapat mendukung kedua kekurangan tersebut, perbedaan dari teknologi ini adalah DMVPN dapat diimplementasikan pada WAN publik sedangkan GETVPN tidak dapat diimplementasikan [10]. DMVPN merupakan solusi yang dapat memberikan jawaban dari permasalahan dengan tunneling melalui internet menggunakan mGRE (Multipoint Generic Routing Encapsulation), performa komunikasi data pada QoS application yang handal, mendukung kecepatan pengiriman data yang aman dengan enkripsi IPSec yang lebih cepat dibandingkan menggunakan SSL, dan menyesuaikan protokol yang ada di perusahaan seperti routing protocol dan TCP/IP agar dapat melakukan perpindahan ke VPN cadangan secara otomatis [10]. Sehingga, dalam perancangan VPN cadangan dari studi kasus fail connection dan mendukung QoS application yang memanfaatkan infrastuktur Internet sebagai medianya adalah teknologi DMVPN.

Identifikasi permasalahan dalam penelitian ini adalah jaringan perusahaan yang memerlukan komunikasi data antara dua area di berbagai lokasi yang hanya memerlukan konektifitas VPN yang handal secara redudansi dari VPN utama tanpa membangun infrastruktur baru. Beberapa solusi teknologi infrastuktur WAN dan protokol VPN belum dapat merelevansikan permasalahan pada studi kasus tersebut. DMVPN dengan mekanisme routing distribution dapat membangun jaringan VPN multiples sites memanfaatkan WAN publik sebagai VPN cadangan, didukung dengan hub and spoke, menyematkan topologi full mesh, dan dapat memberikan enkripsi komunikasi data ketika melalui jalur Internet tersebut. Pada penelitian ini, juga melakukan pengamatan dari pengaruh pergantian *VPN* utama ke *VPN* cadangan, yang mana tujuannya melihat kualitas parameter *QoS* menurut standar internasional *ITU-T G.411*.

2. METODE PENELITIAN



Gambar 2.1. Network Development Life Cycle

Metode dalam perancangan yang akan dilakukan, peneliti menggunakan beberapa langkah yang ada di dalam metode *Network Development Life Cycle* (NDLC). Metode ini meliputi analisis kebutuhan pengguna, desain jaringan dengan topologi, simulasi dan prototipe, implementasi, pengamatan jaringan yang telah dibuat, serta manajemen jaringan [18] yang ditunjukkan pada gambar 3.1. Pada penelitian ini tahapan yang dilakukan hanya berfokus pada *Analysis*, *Design* dan *Simulation prototyping* beserta melakukan pengujian atau *Testing*.

2.1 Analisis Kebutuhan Pengguna

Merupakan tahap pengumpulan informasi yang diperlukan untuk perancangan desain jaringan yang akan dibangun. Informasi yang terdapat di studi literatur diperoleh dengan membaca literatur ataupun jurnal-jurnal yang berhubungan dengan *VPN*. Aspek dalam pemilihan redundansi *VPN* dibutuhkan infrastuktur baru yang mana sasaran bisnis optimal perlu dipertimbangkan sebaik-baiknya, ketika sebuah perusahaan menerapkan konsep *top down approach* yaitu mengedepankan kebutuhan perusahan sehingga teknologi dapat menyesuaikannya [9]. Dalam kasus permasalahan, perusahaan dapat mengintegrasikan *VPN over Internet* sebagai tujuan bisnis dalam meningkatkan tingkat ketersediaan ke kantor cabang tanpa membangun infrastruktur baru. Pemanfaatan jalur *internet* dengan solusi *VPN* menjadi sasaran bisnis optimal secara keseluruhan dengan perspektif masing-masing kebutuhan perusahaan termasuk penggunaan *real time application* yang sangat berpengaruh terhadap *QoS*. Hasil dari tahap ini, berupa spesifikasi rancangan simulasi jaringan dengan pendekatan pada dasar kebutuhan perusaahan yaitu pengguna yang ada di kantor pusat dan cabang dapat berkomunikasi melalui *VPN* dan pengguna dapat mengaplikasikan *real time* dalam komunikasi terebut.

2.2 Desain Jaringan denan Topologi

Merupakan perencanaan sistem yang didapat dari analisis yang akan diterapkan sesuai kebutuhan dan penemuan masalah yang terjadi dalam jaringan, termasuk persiapan kebutuhan alat dan bahan yang digunakan untuk menerapkan sistem tersebut. Dalam tahapan ini memperhatikan performa sistem, data pengujian dan perangkat dari penelitian sebelumnya digunakan, sehingga tidak mengganggu kinerja simulasi penelitian. Selanjutnya, merancang topologi logika dan fisik dirancang berdasarkan kebutuhan dan permasalahan yang telah diinterpretasi. Topologi logika adalah representasi dari jaringan tentang bagaimana *frame* dapat di *transfer* dari satu *node* ke *node* lainnya, sedangkan topologi fisik adalah *node* atau perangkat yang melakukan *transfer* koneksi tersebut sebagai medianya. Hal pertama yang dilakukan adalah merancang *IP Address* yang akan digunakan oleh *router* dan perangkat pengguna. Selanjutnya, menentukan topologi jaringan, posisi perangkat pengguna, dan *Server* dari kantor pusat dan kantor cabang. Perancangan terakhir adalah menentukan protokol Routing yang digunakan pada *IP Address* untuk *Peer-to-peer* dan dari *port router* ke perangkat pengguna, konfigurasi *MPLS-L3VPN* dan *DMVPN* termasuk dalam tahapan ini.

2.3 Simulasi dan Prototipe

Pada tahapan simulasi dan prototipe terhadap jaringan yang dirancangan, akan menggabungkan kedua *MPLS-L3VPN* dan *DMVPN* menjadi satu kesatuan topologi jaringan. Dari penggabungan didapatkan sebuah prioritas *route* yang terjadi pada jaringan yaitu *router* kantor pusat dan cabang, melalui kalkulasi otomatis dari *metric routing protocol*. Sehingga simulasi yang dibangun

menjadikan pengguna yang ada di kantor pusat dapat terhubung melalui *MPLS-L3VPN* ke pengguna yang ada di kantor cabang dan sebaliknya. Pada topologi tersebut dibuat simulasi yang mendekati realistis sedemikian rupa yang dirancang ke dalam software GNS3. Pada menerapkan real time application, peneliti akan menggunakan *RTMP* yang di instal menjadi *virtual server* sebagai *streaming server*. Tujuan *RTMP server* adalah untuk melihat kualitas *QoS* yang terjadi pada konektifitas simulasi jaringan *failover* tersebut.

2.4 Pengujian Topologi

Pada tahap pengujian, seluruh perangkat simulasi diintegrasikan dan diawasi serta melakukan verifikasi pengujian studi failover antar perangkat pengguna. Awal mula melakukan pengujian terhadap konektifitas, Host-1 yang berada di kantor pusat melakukan verifikasi ping ke Host-2 di kantor cabang melalui desain tersebut. Kemudian yang kedua, pengujian fail connection terhadap simulasi yang dibuat analisis pengukuran dari paramater meliputi delay, jitter, packet loss dan throughput menggunakan wireshark dengan pengambilan tiga skenario yang akan dilakukan. Pada skenario yang dimaksud adalah trafik MPLS-L3VPN, Failover Proccess dan DMVPN atau setelah pergantian rute VPN

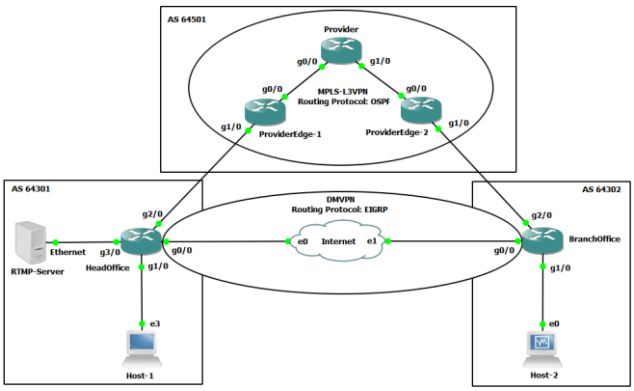
3. HASIL DAN PEMBAHASAN

3. 1 Topologi Sistem

Dalam penelitian ini, peneliti akan membuat dua model jaringan dalam pengujian skenario *failover VPN* dan menganalisis performa redundansi dari penggunaan masing-masing model teknologi *VPN*. Pada model jaringan pertama, yaitu *MPLS* berbasis *VPN service*. Desain lain yaitu *DMVPN* yang diasumsikan melalui *Internet*. Pada desain kantor pusat, *router* yang telah terhubung dengan *MPLS* sebagai media *VPN*. Di sisi kantor cabang, *router* digunakan hal yang sama dengan kantor pusat sehingga satu sama lain dapat berkomunikasi melalui *MPLS*. Pada topologi kedia, penambahan mitigasi pada *MPLS-L3VPN* sebagai media jalur utamanya adalah *DMVPN* yang diterhubung dengan *Internet* sebagai media jalur cadangannya. Dalam topologi simulasi penelitian, masing-masing yang telah diuraikan sebelumnya, bertujuan untuk mengatahui kondisi kualitas data VPN terhadap QoS dari model skema jaringan VPN. Untuk memperkuat data-data hasil pengukuran, pengujian yang diterapkan melakukan pengiriman paket TCP pada setiap skenario sebanyak 5 kali dengan setiap windows size adalah 2, 4, 8, 16 dan 32 bytes, sedangkan pengiriman UDP dalam aplikasi Video streaming sebanyak 5 kali dengan masing-masing dilakukan selama 60 detik komunikasi end-to-end.

Pengukuran paramater QoS dilakukan dengan mengatur Host-1 yang berada di kantor pusat melakukan pengiriman TCP ke Host-2 yang berada di kantor cabang. Setelah parameter diukur, kemudian melakukan pengukuran QoS Video streaming dengan menggunakan OBS Studio dalam mempublish video stream melalui URL RTMP yang telah dibuat pada server RTMP. Mekanisme pengukuran dilakukan dengan mengambil data UDP saat Host-2 sedang streaming video. Kedua pengaturan pengiriman TCP dan mekanisme UDP akan diukur dan dianalisis parameternya menggunakan wireshark pada Host-1. Metode pemutusan rute VPN di cloud MPLS dilakukan dengan perintah shutdown pada interface router PE-HeadOffice yang mengarah ke router CE-HeadOffice.

skema jaringan dapat ditunjukkan pada gambar 3.1.



Gambar 3.1 Topologi Simulasi *Failover*

Skenario simulasi yang dibangun akan dibuat secara realistis sedemikian rupa yang dirancang ke dalam software GNS3. Rancangan *MPLS-L3VPN* dibuat terpisah dengan rancangan *DMVPN*. Rancangan pertama dibangun dengan satu *router provider* dan dua *router edge provider*, sehingga dapat

mengimplementasi *MPLS-L3VPN*. Sedangkan rancangan *DMVPN* yang diasumsikan terhubung denga *internet* sehingga dibutuhkan satu *switch* sebagai media bridge antara dua *router customer edge* yang kedua *router* dibangun di dalam infrastuktur *customer*. Sistem akan dibuat dengan memiliki dua sisi, yaitu kantor pusat dan kantor cabang dengan masing-masing kantor dibangun satu *router* yang terhubung ke *MPLS* dan *DMVPN* serta perangkat host sebagai pengujian sistem.

Host atau *customer* akan digunakan sebagai pengujian konektifitas dari satu sisi ke sisi lain dan mengkalkulasikan waktu *route* yang terjadi ketika jalur *VPN* utama terputus berpindah ke *VPN* cadangan. Perhitungan diambil dari parameter yang terpantau oleh software Wireshark dan hasil nilai tersebut mereferensikan pada standar *ITU-T G.411*.

3. 2 Perancangan Sistem

Perancangan sistem merupakan tahap kedua dalam penerapan yang akan dirancang. *Routing* yang digunakan mereferensikan pada penelitian sebelumnya yang membahas terkait performa kualitas penggunaan protokol *routing*. Pada jaringan *MPLS*, *routing* yang digunakan adalah *OSPF* [16] dan jaringan *DMVPN* menggunakan *EIGRP* [14]. Selain itu, untuk menghubungkan *AS* dari *customer* dengan *provider* dalam suatu sistem jaringan *internet* diasumsikan menggunakan *eBGP* dengan *AS* 64501 untuk *provider*, *AS* 64301 untuk kantor pusat dan *AS* 64302 untuk kantor cabang.

Daftar *interface* serta *IP Address* yang akan diterapkan adalah sebagai berikut:

Tabel 4. 1 Konfigurasi *IP Address* dari masing-masing *interface router customer*

Device	Gi0/0	Gi1/0	Gi2/0	Gi3/0	*Tunnel*0
Head Office	172.16.90.1/24	192.168.1.1/24	10.0.0.6/30	192.168.43.1/24	10.10.10.1/24
Branch Office	172.16.90.2/24	192.168.2.1/24	10.0.0.22/30	-	10.10.10.2/24

Tabel 4. 2 Konfigurasi *IP Address* dari masing-masing *interface router provider*

Device	Loopback0	Gi0/0	Gi1/0
Provider	10.1.1.2/32	10.0.0.10/30	10.0.0.14/30
ProviderEdge-1	10.1.1.1/32	10.0.0.9/30	10.0.0.5/30
ProviderEdge-2	10.1.1.3/32	10.0.0.13/30	10.0.0.21/30

Tabel 4. 3 Konfigurasi *IP Address* dari masing-masing End device

Device	Interface	IP Address
Host-1	Ethernet3	192.168.1.10/24
Host-2	Ethernet0	192.168.2.10/24
RTMP-Server	Ethernet	192.168.43.10/24

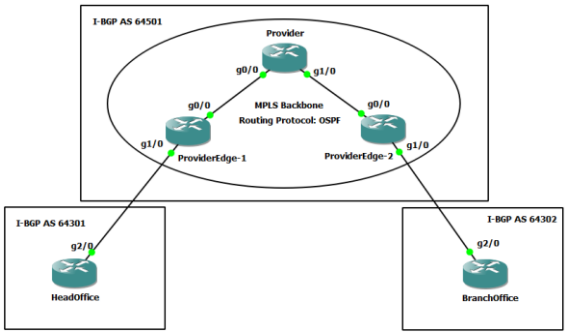
Langkah pertama implementasi jaringan yaitu memberikan *IP Address* pada *interface router* dan host. Setelah *IP Address* dikonfigurasikan pada masing-masing interface, maka langkah selanjutnya melakukan tes verifikasi ICMP pada koneksi *peer-to-peer* antara *router* Provider ke Provider Edge, *router* Provider ke Customer Edge (Headoffice dan BranchOffice), dan Customer Edge ke host (Host-1, Host-2 dan *RTMP Server*) serta koneksi antara *router* Customer Edge melalui *internet* sudah dapat terhubung.

Jaringan Provider yang menjembatani antara kedua jaringan *customer* tidak dapat melakukan *redistribute routing* dinamiknya jika tidak mengaktifkan *BGP connection* dari kedua *router* tersebut. Mengaktifkan *routing* dinamik untuk membuat *cloud MPLS*, semua *router* harus dapat men-forward *packet* agar *router* dapat established dengan jaringan luar dan dapat berkembang. Implementasi *BGP* pada simulasi ini mengadaptasikan eksternal *BGP*, karena *AS* yang digunakan berbeda antara Provider dan Customer.

3.2. 1 Jaringan MPLS-L3VPN

Model sistem pertama dibuat dengan memuat topologi sederhana *peer-to-peer*, dengan 3

router yang disimulasikan sebagai ISP seperti pada gambar 4.2. Pada jaringan ini, diasumsikan sebuah jaringan backbone dengan *routing* dinamik *OSPF* untuk *advertise* jaringannya. Selanjutnya mengimplementasikan *cloud MPLS* pada setiap *interface* yang mengarah ke *router provider* dan memanfaaatkan *routing* tabel *OSPF* sebagai informasi *routing*-nya.



Gambar 4. 1 Skema jaringan *MPLS-L3VPN*

Konfigurasi protokol *routing OSPF* dan *MPLS* pada *router* Provider sebagai *backbone* dari jaringan.

```
interface Loopback0
ip address 10.1.1.2 255.255.255.255
!
interface GigabitEthernet0/0
description Link to Provider Edge 1
ip address 10.0.0.10 255.255.255.252
mpls ip
!
interface GigabitEthernet1/0
description Link to Provider Edge 2
ip address 10.0.0.14 255.255.255.252
mpls ip
!
router ospf 1
network 10.0.0.8 0.0.0.3 area 0
network 10.0.0.12 0.0.0.3 area 0
network 10.1.1.2 0.0.0.0 area 0
!
```

Konfigurasi protokol *routing OSPF* dan *MPLS* pada *router* HeadOffice yang menghubungkan jaringan *customer* dengan jaringan *provider*.

```
interface Loopback0
ip address 10.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
description Link to Provider
ip address 10.0.0.9 255.255.255.252
mpls ip
!
router ospf 1
network 10.0.0.8 0.0.0.3 area 0
network 10.1.1.1 0.0.0.0 area 0
!
```

Konfigurasi protokol *routing OSPF* dan *MPLS* pada *router* BranchOffice yang menghubungkan jaringan *customer* dengan jaringan *provider*.

```
interface Loopback0
ip address 10.1.1.3 255.255.255.255
!
interface GigabitEthernet0/0
description Link to Provider
ip address 10.0.0.13 255.255.255.252
mpls ip
!
router ospf 1
network 10.0.0.12 0.0.0.3 area 0
network 10.1.1.3 0.0.0.0 area 0
!
```

Pada konfigurasi *OSPF* menunjukkan menggunakan *area* 0 sebagai *single area* dan pada skema topologi sederhana tidak memerlukan *multi-area* pada *routing* yang digunakan. Setelah konfigurasi *routing* dan *MPLS*, selanjutnya pengujian rancangan simulasi yang telah dibuat untuk memberikan verfikasi konektifitas antar *router* Provider sudah terhubung. Konfigurasi *routing* eksternal *BGP* agar dapat berkomunikasi dengan jaringan kantor cabang, pada *router* HeadOffice dilakukan konfigurasi sebagai berikut:

```
interface GigabitEthernet2/0
description Link to Provider Edge 1
ip address 10.0.0.6 255.255.255.252
negotiation auto
!
router bgp 64301
bgp log-neighbor-changes
network 192.168.1.0
timers bgp 10 30
neighbor 10.0.0.5 remote-as 64501
!
```

Kemudian menambahkan konfigurasi BGP *peer*-nya pada *router* ProviderEdge-1 sebagai berikut:

```
interface GigabitEthernet1/0
description Link to Customer Edge 1
```

```
ip vrf forwarding Customer
ip address 10.0.0.5 255.255.255.252
negotiation auto
!
ip vrf Customer
rd 64501:1
route-target export 64501:1
route-target import 64501:1
!
router bgp 64501
bgp log-neighbor-changes
neighbor 10.1.1.3 remote-as 64501
neighbor 10.1.1.3 update-source
Loopback0
!
address-family ipv4
neighbor 10.1.1.3 activate
neighbor 10.1.1.3 send-community
extended
exit-address-family
!
address-family vpnv4
neighbor 10.1.1.3 activate
neighbor 10.1.1.3 send-community
extended
exit-address-family
!
address-family ipv4 vrf Customer
neighbor 10.0.0.6 remote-as 64301
neighbor 10.0.0.6 activate
exit-address-family
!
```

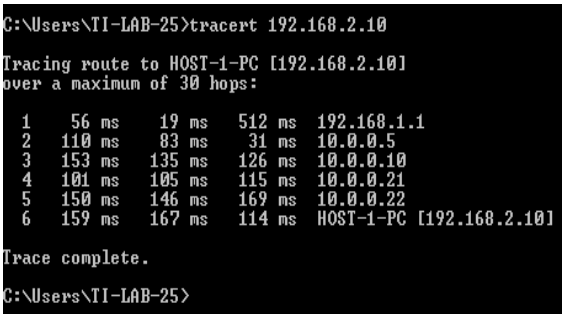
Pada jaringan kantor cabang dilakukan juga konfigurasi yang sama dengan *ASN* dan *IP Address* berbeda, pada konfigurasi *router* BranchOffice sebagai berikut:

```
interface GigabitEthernet2/0
description Link to Provider Edge 2
ip address 10.0.0.22 255.255.255.252
negotiation auto
!
router bgp 64302
bgp log-neighbor-changes
network 192.168.2.0
timers bgp 10 30
neighbor 10.0.0.21 remote-as 64501
!
```

Kemudian menambahkan konfigurasi *BGP peer*-nya pada *router* ProviderEdge-1 sebagai berikut:

```
interface GigabitEthernet1/0
description Link to Customer Edge 2
ip vrf forwarding Customer
ip address 10.0.0.21 255.255.255.252
negotiation auto
!
ip vrf Customer
rd 64501:1
route-target export 64501:1
route-target import 64501:1
!
router bgp 64501
bgp log-neighbor-changes
neighbor 10.1.1.1 remote-as 64501
neighbor 10.1.1.1 update-source
Loopback0
!
address-family vpnv4
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 send-community
extended
exit-address-family
!
address-family ipv4 vrf Customer
neighbor 10.0.0.22 remote-as 64302
neighbor 10.0.0.22 activate
exit-address-family
!
```

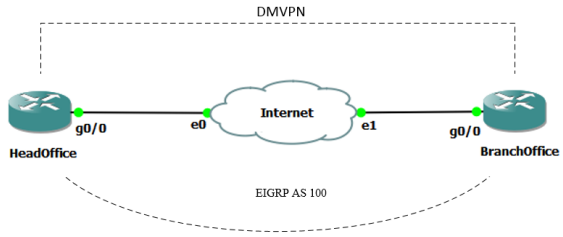
Setelah konfigurasi *MPLS-L3VPN*, selanjutnya pengujian rancangan simulasi yang telah dibuat untuk memberikan verfikasi konektifitas antara *router customer* sudah terhubung dengan baik. Berikut hasil pengecekan komunikasi tes ping dari HeadOffice ke *Customer* dengan menggunakan Host-1 ke jaringan lokal Branchoffice yaitu Host-2.



Gambar 4. 2 Hasil uji *tracert* Host-1 ke Host-2

Dari pengujian verifikasi koneksi data yang terlihat di atas bahwa, jaringan HeadOffice dan BranchOffice sudah aktif sebagai model jaringan *MPLS-L3VPN*.

3.2. 2 Jaringan DMVPN



Gambar 4. 3 Skema Jaringan *DMVPN*

Pada skema *DMVPN* yang merupakan solusi *VPN* dari Cisco melalui *internet* dengan menggabungkan *mGRE*, *NHRP* dan *IPSec* encryption, sehingga penerapan topologi sederhana dengan satu Branch dapat dilihat pada gambar 4.3. Pemodelan sistem ini diasumsikan dengan koneksi dengan *internet* menjadi simulasi menggunakan *switch* antara dua buah *router customer*. Protokol *routing* menggunakan *EIGRP* dalam implementasi *DMVPN* berdasarkan pada penelitian dari Ruta Jankuniene [14] yang menyatakan bahwa *EIGRP* merupakan *routing* yang paling efektif daripada *RIP* dan *OSPF* dalam kualitas layanan *real-time* terhadap *QoS*. Berikut konfigurasi protokol *routing EIGRP* pada *router* HeadOffice sebagai *Hub* dari jaringan *DMVPN*:

```
router eigrp 100
network 10.10.10.1 0.0.0.0
network 172.16.90.1 0.0.0.0
network 192.168.1.1 0.0.0.0
network 192.168.43.1 0.0.0.0
!
```

Konfigurasi protokol *routing EIGRP* pada *router* BranchOffice sebagai Spoke dari jaringan *DMVPN*:

```
router eigrp 100
network 10.10.10.2 0.0.0.0
network 172.17.90.2 0.0.0.0
network 192.168.2.1 0.0.0.0
!
```

Berikut implementasi *IPSec* menjadi ke dalam tiga bagian, yakni implementasi IKE Policies di *router customer*

```
crypto isakmp policy 1
encr aes
hash sha512
authentication pre-share
group 2
crypto isakmp key KEY-NETWORK address 0.0.0.0
!
```

Setelah melakukan konfigurasi *IKE Policies*, selanjutnya menerapkan *IPSec* dari setiap *peer* dengan mendefiniskan sebuah transform-set dan implementasi *IPSec tunnel mode*. Berikut transform-set dengan nama *Trans-IPSec* pada kedua *router customer*:

```
crypto ipsec transform-set Trans-IPSec esp-aes esp-sha512-hmac
mode tunnel
!
```

Pada konfigurasi transform-set dan *mode tunnel* yang terlah dilakukan, maka langkah terakhir adalah membuat sebauh profile dari *IPSec* yang akan digunakan ke dalam *interface router customer*. Berikut konfigurasi dari kedua *router customer*:

```
crypto ipsec profile MGRE-for-DMVPN
set security-association lifetime seconds 86400
set transform-set Trans-IPSec
!
```

Setelah diterapkan masing-masing langkah dari *IPSec* diatas, selanjutnya menerapkan *mGRE* dan *NHRP* ke dalam *interface Tunnel* yang akan diterapkan. Pertama adalah konfigurasi di *router* HeadOffice:

```
interface GigabitEthernet0/0
description Link to DMVPN Public
ip address 172.16.90.1 255.255.255.0
!
interface Tunnel0
description MULTI-POINT GRE TUNNEL for BRANCHE
ip address 10.10.10.1 255.255.255.0
no ip redirects
ip nhrp authentication Pa$$w0rd
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile MGRE-for-DMVPN
!
```

Kedua adalah konfigurasi di *router* BranchOffice:

```
interface GigabitEthernet0/0
description Link to DMVPN Public
ip address 172.16.90.2 255.255.255.0
!
interface Tunnel0
description MULTI-POINT GRE TUNNEL
for HO
ip address 10.10.10.2 255.255.255.0
no ip redirects
ip nhrp authentication Pa$$w0rd
ip nhrp map 10.10.10.1 172.16.90.1
ip nhrp map multicast 172.16.90.1
ip nhrp network-id 1
ip nhrp nhs 10.10.10.1
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile MGRE-for-
DMVPN
!
```

Sistem *DMVPN* yang mengintegrasikan *mGRE tunnelling*, *NHRP* dan *IPSec* dapat memberikan sebuah *tunnel* atau *link VPN* yang dienkripsikan oleh *IPSec*. Pada jaringan ini dapat di implementasikan pada sebuah jaringan *internet* yang memiliki protokol *routing*, namun pada penelitian ini menggunakan *EIGRP* sebagai protokol *routing*. Setelah konfigurasi *DMVPN*, selanjutnya pengujian rancangan simulasi yang telah dibuat untuk memberikan verfikasi konektifitas antara *router customer* sudah terhubung dengan baik. Berikut hasil pengecekan komunikasi tes ping dari HeadOffice ke *Customer* dengan menggunakan Host-1 ke jaringan lokal Branchoffice yaitu Host-2.

```
C:\Users\TI-LAB-25>tracert 192.168.2.10

Tracing route to HOST-1-PC [192.168.2.10]
over a maximum of 30 hops:

  1    15 ms    20 ms    20 ms  192.168.1.1
  2   148 ms    91 ms    85 ms  10.10.10.2
  3    63 ms    83 ms    81 ms  HOST-1-PC [192.168.2.10]

Trace complete.

C:\Users\TI-LAB-25>_
```

Gambar 4. 4 Hasil uji *tracert* Host-1 ke Host-2

Dari pengujian verifikasi koneksi data yang terlihat di atas bahwa, jaringan HeadOffice dan BranchOffice sudah aktif sebagai model jaringan *DMVPN*.

3. 3 Pengujian Sistem

Pengujian sistem pertama menggunakan tes ICMP tanpa menghidupkan aplikasi Video *streaming* terlebih dahulu, kemudian setelah data telah didapatkan maka ICMP perlu di matikan dan aplikasi Video *streaming* dapat mulai dihidupkan untuk dilakukan pengukuran skenario *failover VPN*. Pada gambar 4.15 menunjukkan bahwa informasi tabel *routing* sebelum *failover* dilakukan, *router* HeadOffice masih terhubung dengan *MPLS-L3VPN* dibuktikan pada kode B atau *BGP* dengan *IP Address 192.168.2.0/24 via 10.0.0.5*.

```
      10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C        10.0.0.4/30 is directly connected, GigabitEthernet2/0
L        10.0.0.6/32 is directly connected, GigabitEthernet2/0
C        10.10.10.0/24 is directly connected, Tunnel0
L        10.10.10.1/32 is directly connected, Tunnel0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.90.0/24 is directly connected, GigabitEthernet0/0
L        172.16.90.1/32 is directly connected, GigabitEthernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet1/0
L        192.168.1.1/32 is directly connected, GigabitEthernet1/0
B     192.168.2.0/24 [20/0] via 10.0.0.5, 00:01:02
      192.168.43.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.43.0/24 is directly connected, GigabitEthernet3/0
L        192.168.43.1/32 is directly connected, GigabitEthernet3/0
HeadOffice#
```

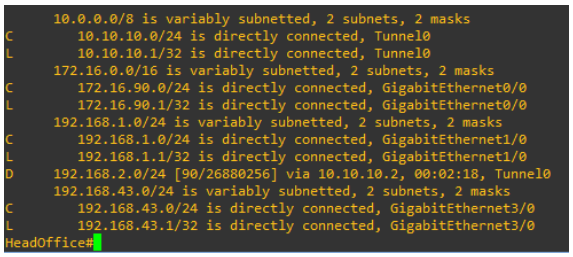
Gambar 4. 5 Informasi tabel *routing* sebelum *failover* dilakukan

Pada pengujian dilakukan memasukkan perintah *shutdown* pada *interface G2/0* yang menuju *MPLS-L3VPN*, sehingga *router* HeadOffice akan melakukan pembaharuan tabel *routing* yang secara otomatis akan melakukan *route distribution* ke *metric EIGRP*. Pada Gambar 4.16 informasi status jalur ke *VPN* utama telah di putuskan dan *BGP* melakukan *hello time* dan memberikan informasi bahwa routing *BGP* akan di *reset* dengan status *down* pada *neighbor* 10.0.0.5.

```
HeadOffice#
HeadOffice#
HeadOffice#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HeadOffice(config)#int g2/0
HeadOffice(config-if)#shutdown
HeadOffice(config-if)#
*Oct 23 19:46:10.355: %BGP-5-NBR_RESET: Neighbor 10.0.0.5 reset (Interface flap)
*Oct 23 19:46:10.379: %BGP-5-ADJCHANGE: neighbor 10.0.0.5 Down Interface flap
*Oct 23 19:46:10.379: %BGP_SESSION-5-ADJCHANGE: neighbor 10.0.0.5 IPv4 Unicast topology base removed from session  Interface flap
HeadOffice(config-if)#
*Oct 23 19:46:12.323: %LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to administratively down
*Oct 23 19:46:13.323: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to down
HeadOffice(config-if)#
```

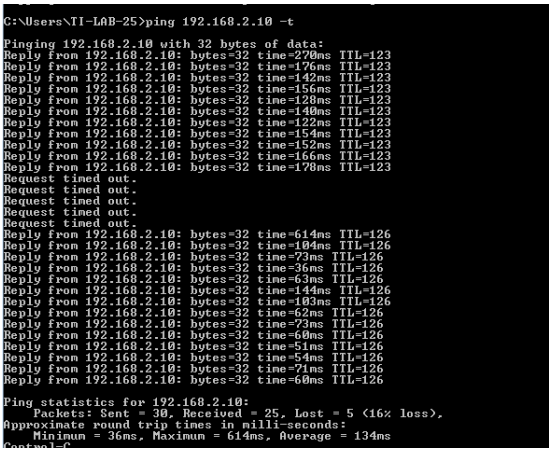
Gambar 4. 6 *Router* HeadOffice melakukan *route* ke *DMVPN*

Terlihat pada informasi tabel *routing*, *router* HeadOffice telah memperbaharui tabelnya dengan routing *EIGRP* seperti ditunjukkan pada gambar 4.17 yaitu kode D atau *EIGRP* terhubung dengan *IP Address 192.168.2.10/24 via 10.10.10.2*.



Gambar 4. 7 Informasi tabel *routing* setelah *failover* berhasil

Gambar 4.15 menunjukkan hasil validasi *Failover* melalui pengiriman ICMP dari saat proses pergantian rute jaringan *VPN* dengan pemutusan rute *cloud MPLS*. Pada pengiriman yang berhasil pertama, menunjukkan koneksi sedang melalui *MPLS-L3VPN* kemudian terputus dengan pesan Request Time out pada saat pengirmannya dan pengirman yang berhasil kedua menunjukkan koneksi telah kembali terhubung melalui *DMVPN*.



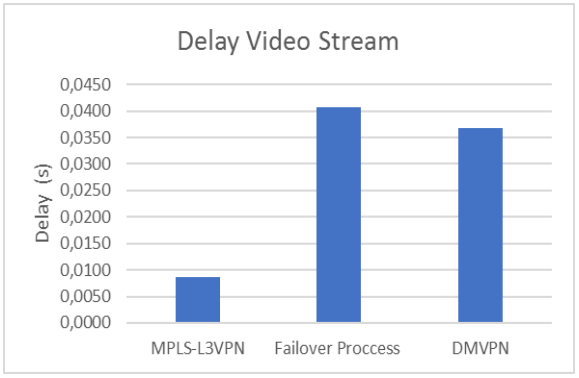
Gambar 4. 8 Hasil uji *ICMP* pada saat proses pemutusan

3. 4 Data Hasil Pengukuran

3.4. 1 Delay

Sejumlah paket yang dikirim salama komunikasi data di transmisikan dari sumber ke tujuan jaringan. Cara menghitung *delay* dengan persamaan dari setiap paket-paket yang ter-*capture* selama 60 detik dan kemudian mengambil rata-rata dari seluruh *delay* tersebut. Persamaan yang digunakan adalah selisih dari waktu penerimaan paket (T_r) dengan waktu pengirman paket (T_s).

$$Delay(s) = T_r - T_s \quad (1)$$

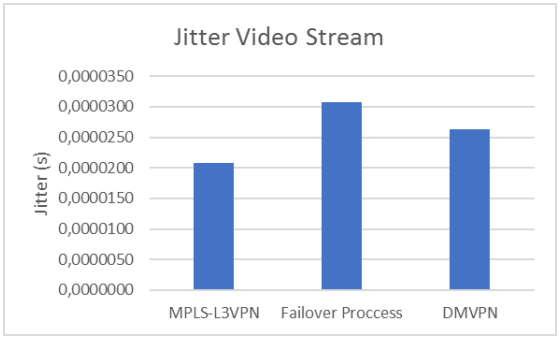


Gambar 4. 9 *Delay* rata-rata pada kondisi video *streaming*

3.4. 2 Jitter

Sebuah variasi dari seluruh transimisi *delay* yang terjadi ketika terdapat peningkatan trafik yang menimbulkan antrian paket. Perhitungan menggunakan hasil pengukuran *delay* sebelumnya, kalkulasi total variasi *delay* dengan melakukan *delay* kedua (T_{i+1}) dikurangi *delay* pertama (T_i) dan kemudian dibagi oleh total paket yang diterima (N) dalam satu transmisi selama 60 detik tersebut.

$$Jitter\,(s) = \frac{\sum(T_{i+1} - T_i)}{N} \quad (2)$$

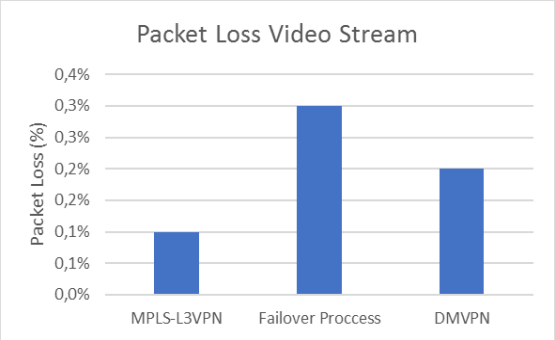


Gambar 4. 10 *Jitter* rata-rata pada kondisi video *streaming*

3.4. 3 Packet Loss

Sejumlah paket yang ter-*drop* selama transmisi dari satu sumber ke tujuan yang disebabkan oleh congestion ataupun collision. Perhitungan paramater ini menggunakan persamaan dari selisih total paket yang dikirim (P_s) dengan total paket yang diterima (P_r) dan kemudian dibagi oleh total paket yang dikirim (P_s) ke dalam satuan persentase pada masing-masing percobaan yang dilakukan.

$$Packet\ Loss(\%) = \left(\frac{P_s - P_r}{P_s}\right) \times 100\% \quad (3)$$

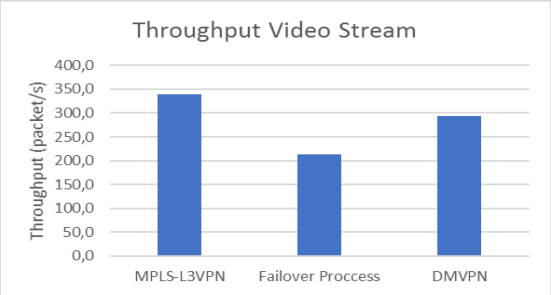


Gambar 4. 11 *Packet loss* rata-rata pada kondisi video *streaming*

3.4. 4 Throughput

Sebuah kecepatan transfer data yang efektif dalam satuan *bps* yang mana pengukuran pada jumlah total paket yang berhasil diterima oleh reciever selama waktu tertentu dan dibagi durasi waktu interval tersebut, sehingga persamaanya sebagai berikut.

$$Throughput\ (bps) = \frac{Jumlah\ paket\ yang\ diterima\ (bit)}{Lama\ pengamatan\ (s)} \quad (4)$$



Gambar 4. 12 *Throughput* rata-rata pada kondisi video *streaming*

KESIMPULAN

Berdasarkan hasil implementasi dan analisis pengujian yang dilakukan, sehingga dapat disimpulkan sebagai berikut:

1. Hasil Pengujian simulasi *failover connection* secara *real time* menunjukkan status berhasil dari skenario *MPLS VPN* menuju ke rute *DMVPN* yang diterapkan dalam membangun VPN cadangan tanpa membangun infrastruktur baru.
2. Pada Parameter QoS (*Quality of Services*) yang terdiri dari *throughput*, *delay*, *jitter* dan *packet loss* menurut ITU-T G.114:
   - *Delay* pada pengujian mimiliki nilai yang sangat baik di bawah standar yaitu 150 ms, selain itu skenario *Failover Proccess* mendapatkan kenaikan nilai *delay* sebesar 40,8 ms yang sebelumnya 8,7 ms pada skenario MPLS L3VPN sedangkan skenario DMVPN nilai yang didapatkan 36,9 ms.
   - *Jitter* pada pengujian memiliki nilai yang sangat baik juga yaitu di bawah 20 ms sesuai standar ITU, terlihat pada hasil yang didapatkan pada skenario MPLS L3VPN, *Failover Proccess* dan DMVPN yaitu 0,0208 ms, 0,0307 ms dan 0,0263 ms.
   - *Packet loss* pada pengujian memiliki nilai yang sangat baik dari maksimal yang direkomendasikan yaitu <0.5%, sedangkan nilai terbesar pada pengujian adalah pada skenario *Failover Proccess* sebesar 0,3% dan kedua skenario lainnya mendapatkan nilai sama sebesar 0,2%.
   - Parameter terakhir yaitu *Throughput* dengan total jumlah *bit* paket yang berhasil diterima, nilai terbesar pada hasil pengujian adalah skenario MPLS L3VPN sebesar 339 *bps*, skenario DMVPN sebesar 293,8 *bps* dan skenario *Failover Proccess* sebesar 212,5 *bps*.
3. Perbedaan kualitas QoS yang didapatkan oleh MPLS lebih baik daripada DMVPN, disebabkan IPSec yang belum diimplementasikan pada MPLS L3VPN sedangkan DMVPN diterapkan. Mereferensikan pada penelitian sebelumnya yaitu MPLS dengan mengimplementasikan IPSec akan menurunkan performa terhadap VoIP application [8], serta DMVPN dengan IPSec menyebabkan latensi dan penurunan kualitas VoIP application selama pembentukan *tunnel* DMVPN [7].

SARAN

Berdasarkan permasalahan dan pembangunan *failover VPN* peneliti memiliki beberapa saran untuk disampaikan antara lain:

1. Pada pengujian selanjutnya dalam menganalisis performa *DMVPN*, peneliti memberikan saran dalam menganalisis

QoS untuk VoIP dan aplikasi real-time lainnya

2. Diharapkan simulasi selanjutnya dilakukan terhadap perangkat nyata atau dapat di uji coba ke dalam jaringan WAN publik pada studi kasus ke perusahaan.
3. Peneliti merekomendasikan *pentesting* terhadap *IPSec DMVPN* terkait kriptograpi yang di integrasikannya, sehingga *administrator* dapat menentukan dan mengevaluasi konfigurasi enkripsi maupun menanggulangi resiko terjadi pencurian data.

DAFTAR PUSTAKA

[1] Agni, I. H. (2014, Desember 10). IMPLEMENTASI FAILOVER MENGGUNAKAN JARINGAN VPN DAN METRONET. *Penelitian*.

[2] Ahmed, A. J., Fathi, S. B., & Ashibani, M. (2017, May 06). Proper Virtual Private Network (VPN) Solution.

[3] Alam, H., Biddut, H., Shafin, U., & Shariar, I. (2016, March). Performance Analysis of Different Cryptography Algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering, 6*.

[4] Amankatiyar , Hemantjain , JayeshSurana, Soni, A., & Vishwakarma, A. (2017). Research on Tunneling Techniques in Virtual Private Networks. *International Journal of Scientific Research in Computer Science, 2*(5).

[5] Anwar, S., Ali, H., Al Mamun, A., & Sheltami, T. R. (2016, January). Performance evaluation of routing protocols for video conference over mpls vpn network. *Journal of Ubiquitous Computing and Intelligence, 7*, 01-06.

[6] Arini, Masruro, S. U., & Rizal, M. (2018, Januari). EVALUASI KINERJA JARINGAN DMVPN MENGGUNAKAN ROUTING PROTOCOL RIPv2, OSPF, EIGRP DENGAN BGP. *Jurnal Informatika Sunan Kalijaga, 2*(3).

[7] Bahnasse, A., & El Kamoun, N. (2017, July 18-20). Performance Evaluation of Web-based Applications and VOIP in Protected Dynamic and Multipoint VPN. *Computing Conference 2017*.

[8] Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017, March). Evaluation of tunnel layer impact on VOIP performances (IP – MPLS – MPLS VPN – MPLS VPN IPsec). *International Journal of Computer Science and Network Security, 17*(13).

[9] Cisco. (2015, November 15). *Network Design Requirements: Analysis and Design Principles*. Dipetik Oktober 25, 2019, dari https://community.cisco.com/legacyfs/online/ccde_9781587144615_chapter1.pdf

[10] Cisco. (2017, July 25). *Simple and Secure Branch-to-Branch Communications Data Sheet*. Dipetik July 2019, dari Products & Service: https://www.cisco.com/c/en/us/products/security/dynamic-multipoint-vpn-dmvpn/index.html

[11] Gupta, H., & Singh, K. K. (2016, March). A NEW APPROACH FOR THE SECURITYOF VPN. *Information Security and Cryptogrpahy*.

[12] JOKELA, P., MELEN, J., & MOSKOWITZ, R. (2015). Using the encapsulating security payload (ESP) transport format with the host identity protocol (HIP).

[13] Jyothi , K., & Reddy, D. (2018). Study on Virtual Private Network (VPN), VPN's Protocols And Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3*(3).

[14] Kakulapati, V., & Sandhya, K. (2018, August). Establishing Secured Enterprise Network. *International Journal of Computer Science and Information Security, 16*(8).

[15] Kakulapati, V., & Sandhya, K. (2018, August). Establishing Secured Enterprise Network. *International Journal of Computer Science and Information Security, 16*(8).

[16] Kevin, A. (2001). *Voice and Data Security*. USA: Sams Publishing.

[17] Mir, S. A., & Sharma, M. (2014, April). A Comparative study of X.25, Frame Relay and ATM in High Speed networks. *INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY, 2*(4).

[18] Moedjiono, S., Maulana, N., & Kusdaryono, A. (2017). Seamless Wireless Design With Single Service Set Identifier and Single Sign On Using Kerio

Control. *International Journal of Latest Research in Engineering and Technology, 03*(0), 27-34.

[19] Munadi, R., Purwanto, Y., & Shabirin, C. M. (2014). ANALISIS IMPLEMENTASI ROUTING PROTOCOL AUTHENTICATION PADA. *Tugas Akhir*.

[20] Munir. (2010). *Kontribusi Teknologi Informasi dan Komunikasi (TIK) dalam Pendidikan di Era Globalisasi Pendidikan Indonesia* (Vol. 2). Jurnal Pendidikan.

[21] Nurindra. (2017). *Standar Organisasi Dalam Bidang Komunikasi Data*. Dipetik Juli 2019, dari https://nurindra.com/standar-organisasi-dalam-bidang-komunikasi-data

[22] Osvari, A. (2006). *Membangun Jaringan Komunikasi Data Dengan Frame Relay*. Diambil kembali dari arsip: http://www.unsri.ac.id/upload/arsip

[23] *Quality of Service Regulation Manual*. (2017). Dipetik Agustus 2019, dari ITU Publications: http://handle.itu.int/11.1002/pub/8108e11f-en

[24] RAZA, S., DUQUENNOY, S., & SELANDER, G. (2013). Compression of ipsec ah and esp headers for constrained environments.

[25] Sukaridhoto, S. (2016). Komunikasi Data dan. Surabaya: Politeknik Negeri Surabaya.

[26] Sun, M.-S., & Wu, W.-H. (2012, November). Engineering analysis and research of MPLS VPN. *Strategic Technology (IFOST)*.

[27] Yudhi, T. (2016). *Simulasi Failover Link pada Routing Protocol OSPFv2*. Salatiga: Universitas Kristen Satya Wacana.