UNIVERSITAS
MERCU BUANA

KONFIGURASI DMVPN MENGGUNAKAN *IPSEC* DAN *ROUTING* EIGRP PADA PT. CAHAYA KREATIF DIGITAL

TUGAS AKHIR

Zainul Zufar
41516210033

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA 2020

KONFIGURASI DMVPN MENGGUNAKAN *IPSEC* DAN *ROUTING* EIGRP PADA PT. CAHAYA KREATIF DIGITAL

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
Zainul Zufar
41516210033

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA 2020

LEMBAR PERNYATAAN ORISINALITAS

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	41516210033
Nama	: Zainul Zufar
Judul Tugas Akhir	: KONFIGURASI DMVPN MENGGUNAKAN IPSEC DAN ROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 30 Agustus 2020

Zainul Zufar

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Zainul Zufar
NIM	:	41516210033
Judul Tugas Akhir	:	KONFIGURASI DMVPN MENGGUNAKAN IPSEC DAN ROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 30 Agustus 2020

Zainul Zufar

SURAT PERNYATAAN LUARAN TUGAS AKHIR

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Zainul Zufar
NIM	:	41516210033
Judul Tugas Akhir	:	KONFIGURASI DMVPN MENGGUNAKAN IPSEC DAN ROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL

Menyatakan bahwa Luaran Tugas Akhir saya adalah sebagai berikut:

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	
		Jurnal Nasional Terakreditasi			
		Jurnal International Tidak Bereputasi		Diterima	
		Jurnal International Bereputasi			
	Disubmit/dipublikasikan di :	Nama Jurnal	:		
		ISSN	:		
2	Kertas Kerja, Merupakan material haasil penelitian sebagai kelengkapan Artikel Jurnal. Terdiri dari (minimal 4)	Literatur Review			[ ]
		Hasil analisa & perancangan aplikasi			[ ]
		Source code			[ ]
		Data set			[ ]
		Tahapan eksperimen			[ ]
		Hasil eksperimen seluruhnya			[ ]
		....			
3	HAKI Disubmit / Terdaftar	HKI		Diajukan	
		Paten		Tercatat	
		No & Tanggal Permohonan	:		
		No & Tanggal Pencatatan	:		

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 30 Agustus 2020

METERAI TEMPEL 6000 ENAM RIBU RUPIAH

Zainul Zufar

iv

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516210033
Nama	:	Zainul Zufar
Judul Tugas Akhir	:	KONFIGURASI DMVPN MENGGUNAKAN IPSEC DANROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada ProgramStudi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 7 September 2020

(Dr. Ida Nurhaida)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516210033
Nama	:	Zainul Zufar
Judul Tugas Akhir	:	KONFIGURASI DMVPN MENGGUNAKAN IPSEC DANROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada ProgramStudi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 7 September 2020

(Desi Ramayanti, S.Kom., MT)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516210033
Nama	:	Zainul Zufar
Judul Tugas Akhir	:	KONFIGURASI DMVPN MENGGUNAKAN IPSEC DANROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada ProgramStudi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 7 September 2020

(Diky Firdaus, S.Kom, MM)

LEMBAR PENGESAHAN

NIM	:	41516210033
Nama	:	Zainul Zufar
Judul Tugas Akhir	:	KONFIGURASI DMVPN MENGGUNAKAN IPSEC DAN ROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, September 2020

Menyetujui,

(Sri Dianing Asri, ST, M.Kom) Dosen Pembimbing

Mengetahui,

(Diky Firdaus, S.Kom, MM) Koord. Tugas Akhir Teknik Informatika	(Desi Ramayanti, S.Kom, MT) Ka. Prodi Teknik Informatika

ABSTRAK

Nama	:	Zainul Zufar
NIM	:	41516210033
Pembimbing TA	:	Sri Dianing Asri, ST, M.Kom
Judul	:	KONFIGURASI DMVPN MENGGUNAKAN IPSEC DAN ROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL

Dengan semakin berkembangnya teknologi maka semakin berkembang pula sistem keamanannya. Bagi perusahaan, mereka membutuhkan penghubung yang dapat menghubungkan kantor cabang mereka dengan kantor pusat, begitu juga sebaliknya. Saat data di enkripsi melalui internet, lalu-lintas data mereka melindunginya. Atas dasar tersebut diperlukan sebuah sistem konfigurasi jaringan yang melindungi transaksi data yang membuat jalur terowongan dan data dibungkus dengan kata sandi menjadikan data itu terenkripsi saat dikirimkan dan terdekripsi saat diterima. *DMVPN (Dynamic Multipoint Virtual Private Network*) adalah sebuah metode *VPN* yang menghubungkan banyak titik secara dinamis dengan tujuan mengefisienkan proses pengiriman data. *IPsec* (singkatan dari IP *Security*) adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. IPsec mendefiniskan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (internetwork layer). *EIGRP (Enhanced Interior Gateway Routing Protocol)* adalah *routing protocol* yang hanya di adopsi oleh router cisco atau sering disebut sebagai *proprietary protocol* pada *cisco*. Dimana EIGRP ini hanya bisa digunakan sesama *router cisco* saja.
Tujuannya akhir konfigurasi ini adalah setiap *router* dan *Peer Tunnel* yang merupakan IP *Private* yang nantinya *IP Private* setiap *router* tersebut akan menanyakan *IP Public*-nya kepada HUB sebagai *core*.

Kata kunci:
DMVPN, IPSec, EIGRP, Cisco routing, GNS3

ABSTRACT

Name	:	Zainul Zufar
Student Number	:	41516210033
Counsellor	:	Sri Dianing Asri, ST, M.Kom
Title	:	KONFIGURASI DMVPN MENGGUNAKAN IPSEC DAN ROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL

With the development of technology, the security system is also developing. For companies, they need a liaison that can connect their branch offices with the head office, and vice versa. When data is encrypted over the internet, their data traffic protects it. On this basis, we need a network configuration system that protects data transactions that make tunnel paths and data wrapped with a password making the data encrypted when sent and decrypted when received. DMVPN (Dynamic Multipoint Virtual Private Network) is a method VPN dynamically connecting many points in order to streamline the data transmission process. IPsec (stands for IP Security) is a protocol used to secure datagram transmission in a TCP / IP-based internetwork. IPsec defines several standards for dataencryption and data integrity at the second layer in the DARPA Reference Model (internetwork layer). EIGRP (Enhanced Interior Gateway Routing Protocol) is routing protocol which only adopted by Cisco routers or often referred to as proprietary protocol on cisco. Where EIGRP can only be used by others cisco router only. The final goal of this configuration is every router and Peer Tunnel which is IP Private which later IP Private every router it will ask IP Public- her to HUB as core.

Key words:
DMVPN, IPSec, EIGRP, Cisco routing, GNS3

KATA PENGANTAR

Puji syukur kita panjatkan kehadirat Allah SWT yang telah melimpahkan nikmat, taufik serta hidayah-Nya yang sangat besar sehingga pada akhirnya penulis dapat menyelesaikan Tugas Akhir dengan judul "Konfigurasi DMVPN Menggunakan *IPSec* dan *Routing EIGRP* pada PT. Cahaya KreatifDigital".

Penulis menyadari bahwa mengerjakan Tugas Akhir sampai penyusunan laporan akhir ini dapat terlaksana dengan lancar berkat kerjasama, bantuan, pengarahan, serta dukunngan dari berbagai pihak, baik secara langsung maupun tidak langsung. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Ibunda dan Ayahanda penulis yang memberikan doa secara terus menerus untuk anaknya. Sehingga, penulis dapat menyelesaikan penulisan ini dengan sebaik-baiknya.
2. Ibu Sri Dianing Asri, ST, M.Kom selaku Dosen Pembimbing dan Sekprodi Informatika Universitas Mercu Buana Kranggan.
3. Ibu Desi Ramayanti, S.Kom, MT, selaku Ketua Program Studi Informatika Universitas Mercu Buana Jakarta.
4. Bapak Diky Firdaus, S.Kom, M.M, selaku koordinator Tugas Akhir.
5. Kakak, adik, kakak ipar dan keponakan penulis yang menjadi *moodbooster* dikala penulis jenuh dengan pekerjaan, skripsi dan hal lainnya.
6. Nadya Laras Aprilia, kekasih penulis yang men-*support* 110% penulisan ini, menjadi auditor, pembimbing, *moodbooster,* tempat berkeluh kesah penulis sehingga penulis dapat menyelesaikan laporan ini.
7. BNI Sekuritas, Sukor Sekuritas, Cuan Troppers yang membuat penulis tetap bahagia saat trading dan investing di bursa saham. #InFundamentalWeTrust.
8. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu yang telah terlibat membantu sehingga tugas akhir ini dapat terselesaikan.

Akhir kata, penulis berharap semoga Allah SWT senantiasa melimpahkankarunia-Nya dan membalas segala amal budi serta kebaikan pihak-pihak yang telah membantu penulis dalam penyusunan laporan ini dan semoga tulisan ini dapat memberikan manfaat bagi pihak-pihak yang membutuhkan.

Jakarta, 30 Agustus 2020

Zainul Zufar

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

NASKAH JURNAL

KONFIGURASI DMVPN MENGGUNAKAN IPSEC DAN ROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL

Sri Dianing Asri
Fakultas Ilmu Komputer, Program Studi Teknik Informatika Universitas Mercu Buana
Email: sri.dianing@mercubuana.ac.id

Zainul Zufar
Fakultas Ilmu Komputer, Program Studi Teknik Informatika Universitas Mercu Buana
Email: 41516210033@student.mercubuana.ac.id

ABSTRAK

Dengan semakin berkembangnya teknologi maka semakin berkembang pula sistem keamanannya. Bagi perusahaan, mereka membutuhkan penghubung yang dapat menghubungkan kantor cabang mereka dengan kantor pusat, begitu juga sebaliknya. Saat data di enkripsi melalui internet, lalu-lintas data mereka melindunginya. Atas dasar tersebut diperlukan sebuah sistem konfigurasi jaringan yang melindungi transaksi data yang membuat jalur terowongan dan data dibungkus dengan kata sandi menjadikan data itu terenkripsi saat dikirimkan dan terdekripsi saat diterima. *DMVPN (Dynamic Multipoint Virtual Private Network*) adalah sebuah metode *VPN* yang menghubungkan banyak titik secara dinamis dengan tujuan mengefisienkan proses pengiriman data. *IPsec* (singkatan dari IP *Security*) adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. IPsec mendefiniskan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (internetwork layer). *EIGRP (Enhanced Interior Gateway Routing Protocol)* adalah *routing protocol* yang hanya di adopsi oleh router cisco atau sering disebut sebagai *proprietary protocol* pada *cisco*.

Kata kunci: *DMVPN, IPSec, EIGRP, Cisco routing,* GNS3

ABSTRACT

With the development of technology, the security system is also developing. For companies, they need a liaison that can connect their branch offices with the head office, and vice versa. When data is encrypted over the internet, their data traffic protects it. On this basis, we need a network configuration system that protects data transactions that make tunnel paths and data wrapped with a password making the data encrypted when sent and decrypted when received. DMVPN (Dynamic Multipoint Virtual Private Network) is a method VPN dynamically connecting many points in order to streamline the data transmission process. IPsec (stands for IP Security) is a protocol used to secure datagram transmission in a TCP / IP-based internetwork. IPsec defines several standards for dataencryption and data integrity at the second layer in the DARPA Reference Model (internetwork layer). EIGRP (Enhanced Interior Gateway Routing Protocol) is routing protocol which only adopted by Cisco routers or often referred to as proprietary protocol on cisco. Where EIGRP can only be used by others cisco router only.

Keywords*:DMVPN, IPSec, EIGRP, Cisco routing, GNS3.*

1. PENDAHULUAN

Dengan semakin berkembangnya teknologi maka semakin berkembang pula sistem keamanannya. Bagi perusahaan besar mereka membutuhkan penghubung yang dapat menghubungkan kantor cabang mereka dengan kantor pusat, begitu juga sebaliknya, saat data di enkripsi melalui Internet lalu-lintas data mereka melindunginya. Sebagai contoh, sebuah toko retail harus terhubung dengan kantor pusatnya untuk mengetahui persediaan barang dan pemesanan, toko cabang tersebut dapat juga terhubung dengan sesama toko cabang lainnya untuk mengetahui sisa produk yang tersedia. Dahulu, satu-satunya cara untuk menghubungkan cabang dengan pusat ialah dengan menggunakan *Layer-2* seperti ISDN atau *frame relay* untuk saling berkomunikasi. Dengan menggunakan ISDN atau *frame relay* akan memakan banyak waktu dan biaya yang cukup mahal. Jika semua kantor cabang (termasuk kantor pusat) sudah memiliki akses internet yang relatif murah, maka akses internet ini juga dapat digunakan untuk komunikasi IP internal antara cabang dan kantor pusat dengan menggunakan *IPsec tunnels* untuk memastikan privasi dan integritas data.

DMVPN adalah teknologi yang di perkenalkan Cisco untuk mempermudah koneksi antara kantor cabang dengan kantor pusat dan sebaliknya. *DMVPN* merupakan fitur yang ditawarkan oleh Cisco yang dapat memungkinkan pertukaran data melalui internet secara aman, seolah- olah data tersebut dikirimkan melalui perantara kabel. *DMVPN* memiliki banyak fitur dan teknologi seperti *IPSec (IP Security), mGRE (multipoint GRE), NHRP (Next Hope Resolution Protocol)*. Fitur *IPSec* membuat data yang di kirimkan ter-enkripsi dan ter-dekripsi. *IPSec* diibaratkan sebagai
Tunnel (terowongan) untuk jalur lalu-lintas data.

DMVPN memiliki keunggulan dibandingkan *VPN* biasa, karena *VPN* biasa memiliki konfigurasi yang cukup rumit dan kompleks dalam hal ini pada *VPN* biasa seorang administrator harus memasukkan konfigurasi satu persatu atau *site-to-site*, apabila *site* di tambah maka konfigurasi ditambahkan juga. Berbeda dengan *DMVPN*, apabila ada *site* yang ditambahkan *DMVPN* secara default akan menambahkan *site*tersebut.

Cisco *DMVPN* memungkinkan lokasi cabang untuk berkomunikasi secara langsung satu sama lain melalui WAN publik atau internet, seperti ketika menggunakan *voice over IP (VOIP)* antara dua kantor cabang, tetapi tidak memerlukan koneksi *VPN* permanen antara situs. Hal ini memungkinkan penyebaran zero-touch dari *IPsec VPN* dan meningkatkan kinerja jaringan dengan mengurangi *latency* (jumlah waktu yang dibutuhkan paket data untuk berpindah di seluruh koneksi jaringan) dan jitter (variasi dari delay atau selisih antara *delay* pertama dengan *delay* selanjutnya), sekaligus mengoptimalkan pemanfaatan *bandwidth* kantor pusat.

Sudah selayaknya bagi perusahaan-perusahaan besar untuk membagun koneksi *IPSec* secara besar untuk menghubungkan cabang mereka melalui jaringan internet. *IPSec* mengenkripsi *traffic* antara dua titik (*peer to peer*) dan pengenkripsian tersebut dilalukan kedua titik menggunakan kata kunci yang rahasia. Karena kata kunci rahasia ini hanya terdapat antara kedua titik tersebut, jaringan terenkripsi secara erat antara kedua *peer.* Oleh karena itu, *IPSec* secara interinsik adalah penghubung antara titik *tunnel* dalam jaringan. Metode ini layak di implementasikan untuk jaringan berskala besar dan memiliki titik cabang yang banyak dan untuk mengatur kedalam *hub* dan *spoke* atau secara penuh menggunakan *mesh network.* Dalam sebagian besar jaringan, *traffic* IP antara *spokes* dan *hub* cukup mendominasi dan antar *spoke* sangat kecil, jadi desain *hub* dan *spoke* sering menjadi pilihan utama. Desain ini juga cocok untuk jaringan *Frame Relay* versi lama, maka dari itu biaya yang dikeluarkan juga menjadi cukup mahal.

2. METODELOGI PENELITIAN

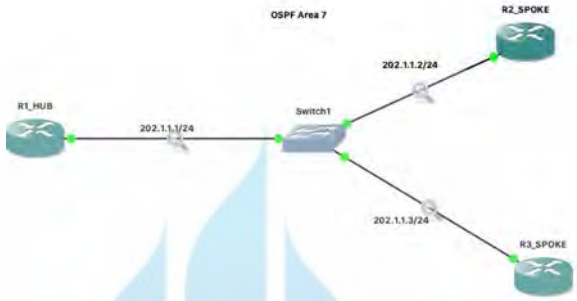
Studi kepustakaan, dilakukannya pengumpulan referensi mengenai hal-hal yang berhubungan dengan sistem *networking* dengan mengunakan *DMVPN* dan routing EIGRP dan literatur-literatur yang terkait.

Jenis penelitian, penelitian ini akan menggunakan metode *Forward Engineering*

Research, dilakukan mulai dari identifikasi masalah, pengumpulan data, penyusunan model, pengujian model, pembangunan, evaluasi, dan validasi. Penelitian dilakukan mulai dari abstraksi yang lebih tinggi menuju ke setingkat atau beberapa tingkat lebih rendah, sehingga dapat digunakan untuk menguji teori/ model/ *formula* (*confirmatory research*).

1.1. Analisis

Peneliti melakukan survei dan observasi secara langsung untuk melakukan pengamatan terhadap topologi jaringan yang sudah ada (*existing*) agar mendapatkan gambaran topologi jaringan seutuhnya sebelum masuk ke tahap *design*. Berikut adalah gambaran topologi yang sudah ada yang dapat dilihat pada gambar 1



1.2. Design

Setelah mendapatkan topologi beserta konfigurasi saat ini. Peneliti tidak mengubah topologi, tetapi mengubah konfigurasi seperti gambar dibawah ini.

1.3. Simulasi *Prototyping*

Pada tahap ini menggunakan GNS3 dan *cisco packet tracer* untuk *trial and error* dalam konfigurasi sebelum diimplementasikan pada router dan jaringan sesungguhnya.

3. HASIL DAN PEMBAHASAN

a. Analisa Software

i. ***GNS3* versi terbaru**.

GNS3 adalah aplikasi simulator jaringan (*Graphic Simulator Network*) berbasis GUI yang di rilis pada tahun 2008. Dengan GNS3 kita bisa mensimulasikan perangkat asli baik dengan bantuan emulator ataupun teknologi virtualisasi. Salah satu teknologi *emulator* yaitu dynamips, yang digunakan untuk mensimulasikan Cisco IOS.

ii. Wireshark.

Wireshark adalah program *Network Protocol Analyzer* alias penganalisa protokol jaringan yang lengkap. Program ini dapat merakam semua paket yang

lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin

iii. ***Image IOS Cisco 7200***.

b. Analisa Hardware

Perangkat keras (*hardware*) yang akan digunakan dalam penelitian ini adalah sebagai berikut;

Laptop *MacBook Pro (2018)*

- *Operating system mac OS Catalina v 10.15.4.*
- *Monitor 16 inch.*
- *Processor Intel Core i7.*
- *Memory 16 GB 2400 MHz DDR4.Graphics Radeon Pro 555X 4 GB dan Intel UHD Graphics 630 1536 MB.*
- *SSD 256 GB.*

Perangkat dan bahan yang dibutuhkan *(optional)*

- *Router Cisco series 7200 (4 unit).*
- Kabel UTP RJ45 3 buah.

c. Perbedaan DMVPN Phase

Phase 1	Phase 2	Phase 3
Hub menggunakan *mGRE tunnel*	*Hub* menggunakan *mGRE tunnel*	*Hub* menggunakan *mGRE tunnel* dan menambahkan konfigurasi *ip NHRP redirect*
Spoke menggunakan *GRE tunnel*	*Spoke* menggunakan *GRE tunnel*	*Spoke* menggunakan *GRE tunnel* dan menambahkan konfigurasi *ip nhrp shortcut*
Antar *spoke* dapat berkomunikasi hanya jika melalui *Hub*	Spoke dapat berkomunikasi tanpa melalui *Hub*	Spoke dapat berkomunikasi tanpa melalui *Hub*

d. Verifikasi Router

Berikut ini adalah hasil verifikasi router dari R1_HUB, R2_SPOKE dan R3_SPOKE. Verifikasi DMVPN ini digunakan untuk melihat status konfigurasi pada *tunnel*

```
R1_HUB#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel0, Type:Hub, NHRP Peers:2,
 # Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1       202.1.1.6      10.10.10.2    UP   never D
     1      202.1.1.10      10.10.10.3    UP   never D
```

```
R2_SPOKE#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel0, Type:Spoke, NHRP Peers:1,
 # Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1       202.1.1.1      10.10.10.1    UP 00:03:11 S
```

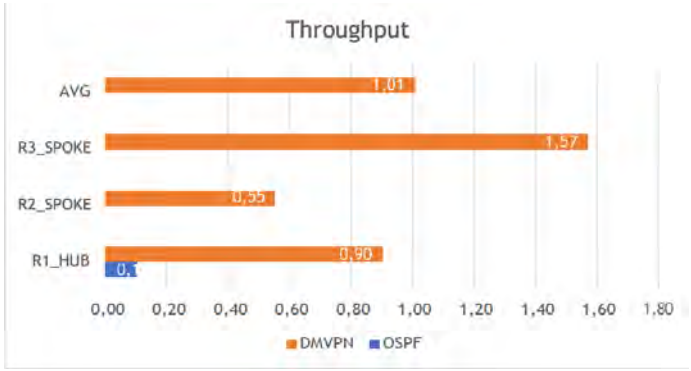
```
R3_SPOKE#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel0, Type:Spoke, NHRP Peers:1,
 # Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1       202.1.1.1      10.10.10.1    UP 00:03:41 S
```

e. Hasil Test Throughput

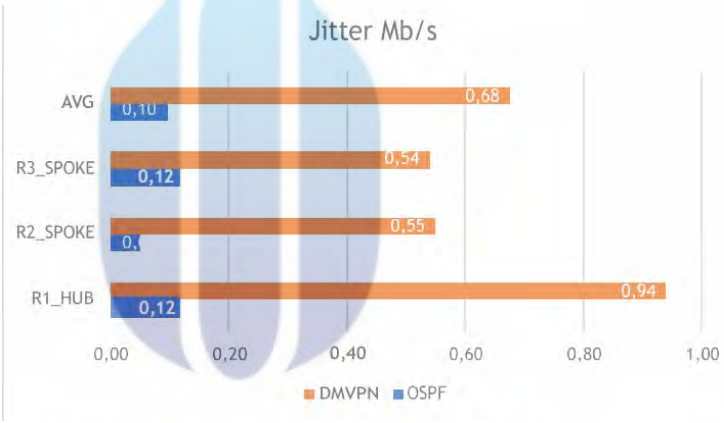
Throughput adalah bandwidth aktual. Jika bandwidth adalah batas maksimum,

throughput adalah sesuai dengan data aktual yang mengalir pada media transmisi.



f. Hasil Test Jitter

Hasil test jitter untuk menghitung kecepatan *request and receive data (ping)* dan dalam variasi *response time.* Pada data dibawah *jitter* pada DMVPN lebih besar dibanding OSPF dengan perbedaan rata-rata 0,68Mbps.



4. KESIMPULAN

DMVPN merupakan sebuah solusi untuk perusahaanbesar yang memiliki kantor cabang yang cukup banyak dan terlebih terletak di luar kota, pulau atau benua. *DMVPN* memiliki keunggulan dibanding *VPN* biasa yaitu dari fitur dimana *DMVPN* lebih mudah dalam mengkonfigurasi dan apabila ada *site* tambahan maka tidak perlu di konfigurasi dari ulang sehingga dapat mengefisiensikan waktu dan tenaga.

Singkatnya, Konfigurasi *DMVPN* Menggunakan *IPSec* dan *Routing EIGRP* pada PT. Cahaya Kreatif Digital membuat kinerja *network engineer* menjadi lebih efisien. Dengan investasi dibidang keamanan jaringan, PT. Cahaya Kreatif Digital dapat menekan *cost* kemungkinan kerugian atas hilangnya data maupun kerugian waktu karena *network engineer* harus men-*troubleshoot* jaringan dengan *effort* lebih.

DAFTAR PUSTAKA

[1] M. T. Kurniawan, *Buku Jaringan Komputer I.* .

[2] S. Jose, “Dynamic Multipoint VPN Configuration Guide , Cisco IOS XE Release 3S,” no. 6387, 2014.

[3] Cisco, “Cisco Express Forwarding,” *Architecture*, pp. 1–8, 2002, [Online]. Available:

http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c/xcfcef.ht ml.

[4] R. Arlan, R. Munadi, and N. Andini, “Implementasi Dan Analisis Sistem Keamanan Ip Security (Ipsec) Di Dalam Multi Protocol Label Switching-Virtual Private Network (Mpls- Vpn) Pada Layanan Berbasis Ip Multimedia Subsystem (Ims),” *J. Chem. Inf. Model.*, vol. 3, no. 9, p. 4630, 2016, doi: 10.1017/CBO9781107415324.004.

[5] P.-C. Cheng, J. A. Garay, A. Herzberg, and H. Krawczyk, “Security architecture for the internet protocol,” *Comput. Stand. Interfaces*, vol. 20, no. 6–7, p. 409, 1999, doi: 10.1016/s0920-5489(99)90778-x.

[6] S. M. Janosik, “IP Authentication Header,” *NASPA J.*, vol. 42, no. 4, p. 1, 2005, doi: 10.1017/CBO9781107415324.004.

[7] F. F. Information, “Encrypted Preshared Key Restrictions for Encrypted Preshared Key Information About Encrypted Preshared Key Using the Encrypted Preshared Key Feature to Securely Store Passwords,” vol. 6, pp. 1–15,2011.

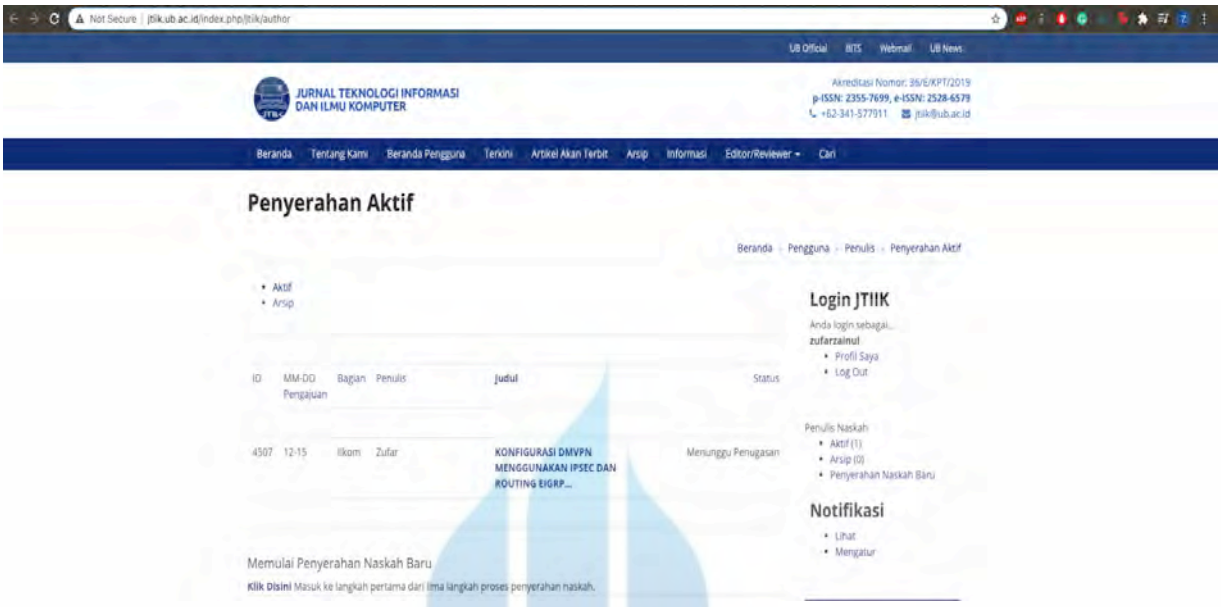
[8] I. Warman and A. Hanafi, “Analisa Perbandingan Kinerja Generic Routing Encapsulation (GRE) Tunnel Dengan Point to Point Protocol over Ethernet (PPPoE) Tunnel Mikrotik Routeros,” *Teknoif*, vol. 7, no. 1, pp. 58–66,2019.

[9] S. M. Janosik, “Generic Routing Encapsulation (GRE),” *NASPA J.*, vol. 42, no. 4, p. 1, 2005, doi: 10.1017/CBO9781107415324.004.

[10] A. Headquarters, “Segment Routing Configuration Guide , Cisco IOS XE Gibraltar 16 . 11 . x,” no. 63

LAMPIRAN KORESPONDENSI

1. Bukti Submit Jurnal



2. Email Korespondensi ACC Sidang

KERTAS KERJA

Ringkasan

Kertas kerja ini merupakan material kelengkapan artikel jurnal dengan judul KONFIGURASI DMVPN MENGGUNAKAN IPSEC DANROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL. Kertas kerja ini berisi semua material hasil penelitan Tugas Akhir yang tidak dimuat atau disertakan di artikel jurnal. Di dalam kertas kerja ini disajikan: literature review, analisis data, dan hasil eksperimen secara keseluruhan. Di dalam kertas kerja ini menjelaskan mengenai perbedaan antara setiap *phase* dalam *DMVPN.*

KONFIGURASI DMVPN MENGGUNAKAN IPSEC DANROUTING EIGRP PADA PT. CAHAYA KREATIF DIGITAL ini menggunakan *routing EIGRP* dan *tunneling DMVPN* di setiap router.

BAGIAN 1 PENDAHULUAN

1.1.Latar Belakang

Dengan semakin berkembangnya teknologi maka semakin berkembang pula sistem keamanannya. Bagi perusahaan besar mereka membutuhkan penghubung yang dapat menghubungkan kantor cabang mereka dengan kantor pusat, begitu juga sebaliknya, saat data di enkripsi melalui Internet lalu-lintas data mereka melindunginya. Sebagai contoh, sebuah toko retail harus terhubung dengan kantor pusatnya untuk mengetahui persediaan barang dan pemesanan, toko cabang tersebut dapat juga terhubung dengan sesama toko cabang lainnya untuk mengetahui sisa produk yang tersedia. Dahulu, satu-satunya cara untuk menghubungkan cabang dengan pusat ialah dengan menggunakan *Layer-2* seperti ISDN atau *frame relay* untuk saling berkomunikasi. Dengan menggunakan ISDN atau *frame relay* akan memakan banyak waktu dan biaya yang cukup mahal. Jika semua kantor cabang (termasuk kantor pusat) sudah memiliki akses internet yang relatif murah, maka akses internet ini juga dapat digunakan untuk komunikasi IP internal antara cabang dan kantor pusat dengan menggunakan *IPsec tunnels* untuk memastikan privasi dan integritas data.

DMVPN adalah teknologi yang di perkenalkan Cisco untuk mempermudah koneksi antara kantor cabang dengan kantor pusat dan sebaliknya. *DMVPN* merupakan fitur yang ditawarkan oleh Cisco yang dapat memungkinkan pertukaran data melalui internet secara aman, seolah- olah data tersebut dikirimkan melalui perantara kabel. *DMVPN* memiliki banyak fitur dan teknologi seperti *IPSec (IP Security), mGRE (multipoint GRE), NHRP (Next Hope Resolution Protocol)*. Fitur *IPSec* membuat data yang di kirimkan ter-enkripsi dan ter-dekripsi. *IPSec* diibaratkan sebagai *Tunnel* (terowongan) untuk jalur lalu-lintas data.

DMVPN memiliki keunggulan dibandingkan *VPN* biasa, karena *VPN* biasa memiliki konfigurasi yang cukup rumit dan kompleks dalam hal ini pada *VPN* biasa seorang administrator harus memasukkan konfigurasi satu persatu atau *site-to-site*, apabila *site* di tambah maka konfigurasi ditambahkan juga. Berbeda dengan *DMVPN*, apabila ada *site* yang ditambahkan *DMVPN* secara default akan menambahkan *site* tersebut.

Cisco *DMVPN* memungkinkan lokasi cabang untuk berkomunikasi secara langsung satu sama lain melalui WAN publik atau internet, seperti ketika menggunakan *voice over IP (VOIP)* antara dua kantor cabang, tetapi tidak memerlukan koneksi *VPN* permanen antara situs. Hal ini memungkinkan penyebaran zero-touch dari *IPsec VPN* dan meningkatkan kinerja jaringan dengan mengurangi *latency* (jumlah waktu yang dibutuhkan paket data untuk berpindah di seluruh koneksi jaringan) dan jitter (variasi dari delay atau selisih antara *delay* pertama dengan *delay* selanjutnya), sekaligus mengoptimalkan pemanfaatan *bandwidth* kantor pusat.

Sudah selayaknya bagi perusahaan-perusahaan besar untuk membagun koneksi *IPSec* secara besar untuk menghubungkan cabang mereka melalui jaringan internet. *IPSec* mengenkripsi *traffic* antara dua titik (*peer to peer*) dan pengenkripsian tersebut dilalukan kedua titik menggunakan kata kunci yang rahasia. Karena kata kunci rahasia ini hanya terdapat antara kedua titik tersebut, jaringan terenkripsi secara erat antara kedua *peer.* Oleh karena itu, *IPSec* secara interinsik adalah penghubung antara titik *tunnel* dalam jaringan. Metode ini layak di implementasikan untuk jaringan berskala besar dan memiliki titik cabang yang banyak dan untuk mengatur kedalam *hub* dan *spoke* atau secara penuh menggunakan *mesh network.* Dalam sebagian besar jaringan, *traffic* IP antara *spokes* dan *hub* cukup mendominasi dan antar *spoke* sangat kecil, jadi desain *hub* dan *spoke* sering menjadi pilihan utama. Desain ini juga cocok untuk jaringan *Frame Relay* versi lama, maka dari itu biaya yang dikeluarkan juga menjadi cukup mahal.

Ketika menggunakan internet sebagai penghubung antara *hub* dan *spoke*, *spoke* juga memiliki akses langsung ke *spoke* lainnya tanpa adanya biaya tambahan, tetapi cara ini cukup sulit, namun bukan hal yang mustahil untuk mengelola secara penuh maupun sebagian jaringan *mesh* ini. Menghubungkan jaringan secara penuh atau sebagian adalah cara paling menguntungkan karena dapat menghemat biaya jika *spoke* dapat berhubungan langsung dengan *spoke* lainnya tanpa adanya perantara *hub.* Jika lalu lintas antar *spoke* melalui *hub*, maka *hub* akan menggunakan sumberdayanya dan berdampak kepada delay-nya paket data yang dikirim karena hub akan meng-enkripsi *IPSec* dan men-dekripsi paket

data yang datang dari *spoke* pengirim dan di enkripsi kembali sebelum dikirimkan kepada *spoke* penerima. Sebagai contoh lainnya saat *spoke* dan *spoke* terhubung langsung akan sangat berfungsi ketika kedua *spoke* berada di kota yang sama sedangkan *hub* berada di negara atau kota berbeda, maka akan terjadi efisiensi dalam mengelola waktu dan biaya. Judul penelitian "**Konfigurasi *DMVPN* Menggunakan *IPSec* dan *Routing EIGRP* pada PT. Cahaya Kreatif Digital**"

1.2. Perumusan Masalah

Berdasarkan latar belakang diatas, maka permasalah yang akan dikaji pada penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana *DMVPN* dapat membuat *transfer* data menjadi efisien?
2. Bagaimana *IPSec* men-*encrypt* data?
3. Apa kelebihan *DMVPN* dibanding *VPN* biasa?

1.3. Tujuan dan Manfaat Penelitian

- Adapun tujuan penulisan tugas akhir ini antara lain:
  - 1.1.1. Menjadikan *DMVPN* dengan *routing EIGRP* sebagai *routing* utama dari perusahaan.
  - 1.1.2. Mengetahui kelebihan dari *IPSec* dibandingkan teknik enkripsi lainnya.
  - 1.1.3. Memahami kelebihan *DMVPN*.
- Manfaat yang diharapkan dari penelitian tugas akhir ini adalah sebagai berikut:
  1. Efisiensi dalam *transfer* data secara *reliable*.
  2. Investasi terhadap *infrastructure*.

1.4. Batasan Masalah

Dalam konfigurasi *DMVPN* menggunakan *IPSec* dan *router EIGRP* ini terdapat beberapa batasan masalah yang ada, yaitu:

1.1.4. Pada laporan ini hanya menampilkan pengiriman data antar *router*.
1.1.5. *Routing* menggunakan *EIGRP*.
1.1.6. *DMVPN* versi ketiga.

1.1.7. Menggunakan *GNS 3* sebagai *software* uji coba.

1.1.8. Menggunakan *Router* Cisco.

1.5. Metode Penelitian

Pada metodologi penelitian ini penulis menjabarkan beberapa hal tentang bagaimana penelitian yang dilaksanakan, antara lain:

1.1.9. Studi Kepustakaan

Dilakukannya pengumpulan referensi mengenai hal-hal yang berhubungan dengan sistem *networking* dengan mengunakan *DMVPN* dan routing EIGRP dan literatur-literatur yang terkait.

1.1.10. Jenis Penelitian

Penelitian ini akan menggunakan metode *Forward Engineering Research*, dilakukan mulai dari identifikasi masalah, pengumpulan data, penyusunan model, pengujian model, pembangunan, evaluasi, dan validasi. Penelitian dilakukan mulai dari abstraksi yang lebih tinggi menuju ke setingkat atau beberapa tingkat lebih rendah, sehingga dapat digunakan untuk menguji teori/ model/ *formula* (*confirmatory research*).

1.1.11. Metode Pengumpulan Data

Data yang akan digunakan dalam penelitian ini merupakan data primer yaitu data yang didapatkan dari PT. Cahaya Kreatif Digital lalu akan di tambah dengan beberapa studi pustaka yang menjadi data sekunder.

1.6. Sistematika Penulisan

Untuk memahami lebih jelas laporan ini, maka materi-materi yang tertera pada laporan skripsi ini dikelompokkan menjadi beberapa sub bab dengan sistematika penyampaian sebagai berikut:

BAB I PENDAHULUAN

Bab yang membahas tentang gambaran penelitian dan dasar masalah yang di lakukan oleh peneliti, yang mencakup latar belakang, identifikasi masalah, batasan masalah, tujuan dan manfaat penelitian serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab yang memaparkan teori – teori yang diperoleh dari sumber-sumber yang relevan untuk digunakan sebagai panduan dalam penelitian serta penyusunan tugas akhir.

BAB III ANALISIS SISTEM

Bab yang menjelaskan tentang gambaran sistem serta deskripsi dari hasil analisis sistem yang akan dijadikan sebagai petunjuk untuk perancangan pada tahapan berikutnya.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab yang menjelaskan mengenai kebutuhan *hardware*, *software* serta mengenai arsitektur dan proses konfigurasi *router* dan melakukan pengujian *ping, next-hop* dan hasil konfigurasi *DMVPN* itu sendiri.

BAB V KESIMPULAN DAN SARAN

Mengemukakan kesimpulan yang diambil dari hasil penelitian dan penulisan tugas akhir ini, serta saran-saran untuk pengembangan selanjutnya, agar dapat dilakukan perbaikan-perbaikan di masa yang akan datang.

DAFTAR PUSTAKA

LAMPIRAN

BAGIAN 2 LANDASAN TEORI

2.1. Jaringan Komputer

Konsep dasar tentang sistem pertama kali dikemukan oleh Bertanffy dan Ashby (1940). Konsep ini pada awalnya dikaji berdasarkan filosofi ilmu pengetahuan yang meliputi ilmu teknik, fisika, biologi, geografi, sosiologi, teori organisasi, manajemen, dan ekonomi. Saat ini, kajian tersebut disebut juga sebagai teori sistem.

2.1.1. Pengertian Jaringan Komputer

Menurut Kristanto (2000), jaringan komputer ialah sekelompok komputer otonom yang saling terhubung satu sama lain, dengan memakai satu *protocol* komunikasi sehingga semua komputer yang saling terhubung tersebut bisa berbagi informasi, program, sumber daya dan juga bisa saling memakai perangkat keras lainnya secara bersamaan, seperti *printer*, *harddisk* dan lain sebagainya. Sedangkan menurut Budhi Irawan (2005:5), jaringan Komputer ialah suatu *system* yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja bersama- sama untuk mencapai suatu tujuan yang sama.

Dari beberapa definisi mengenai jaringan komputer, dapat diambil kesimpulan bahwa jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung. Informasi dan data bergerak melalui kabel- kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan *data*, mencetak pada *printer* yang sama dan bersama sama menggunakan *hardware* atau *software* yang terhubung dengan jaringan. Tiap komputer, *printer* atau *peripheral* yang terhubung dengan jaringan disebut *node*. Setiap jaringan komputer terdiri dari minimal 2 buah *node*.

2.1.2. Jenis-jenis Jaringan Komputer

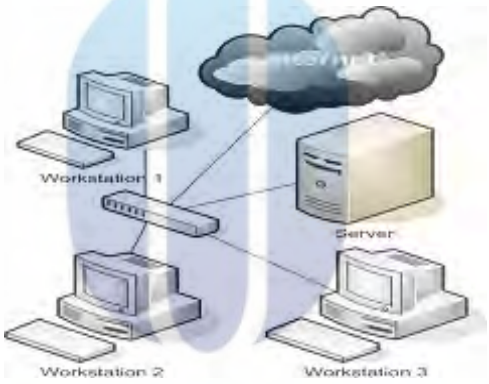
Pada dasarnya jaringan komputer terbagi menjadi beberapa jenis berdasarkan area, media penghantar dan fungsi. Berikut ini adalah pemaparan dari beberapa jenis jaringan komputer, yaitu:

1. Berdasarkan Area

   Yang dimaksud dari berdasarkan area adalah jangkauan area yang dapat dicangkup oleh jaringan komputer dan berikut adalah jenis jaringan komputer berdasarkan area:

- *LAN* (*Local Area Network*)

  LAN adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 km persegi.

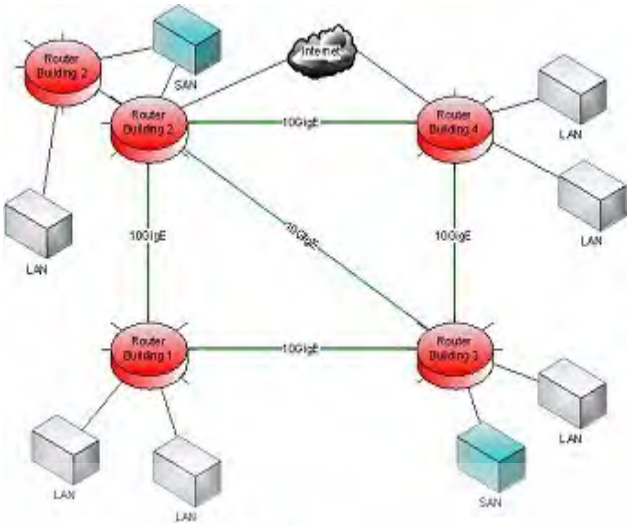


Gambar 1. Jaringan LAN yang langsung terhubung ke internet

- *MAN* (*Metropolitan Area Network*)

  MAN meliputi area yang lebih besar dari *LAN*, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar,

  contohnya jaringan Bank dimana beberapa kantor cabang sebuah Bank di dalam sebuah kota besar dihubungkan satu sama lain.



Gambar 2. **Jaringan MAN**

- *WAN* (*Wide Area Network*)

  WAN adalah jaringan yang lingkupnya besar biasanya sudah menggunakan sarana Satelit ataupun kabel bawah laut sebagai contoh keseluruhan jaringan Bank BNI yang ada di Indonesia ataupun yang ada di Negara-negara lain.

Gambar 3. Jaringan WAN

2. Berdasarkan Media Penghantar

Pada jaringan komputer, terdapat pembagian jenis jaringan komputer, salah satunya berdasarkan dari jenis media penghantar yang digunakan. Berikut adalah jenis-jenis jaringan komputer berdasarkan dari mediapenghantarnya:

- *Wired Network*

  Wired network adalah jaringan komputer yang menggunakan kabel sebagai media penghantar. Kabel yang umum digunakan pada jaringan komputer biasanya menggunakan bahan dasar tembaga. Ada pula jenis kabel lain yang menggunakan bahan serat optik.

- *Wireless Network*

  Wireless network adalah jaringan tanpa kabel yang menggunakan media penghantar gelombang radio atau cahaya *infrared*. Dewasa ini sudah semakin banyak lokasi-lokasi yang menyediakan layanan *wireless network*. Layanan ini membuat pengguna dengan mudah melakukan akses internet tanpa kabel.

3. Berdasarkan Fungsi

Selain terbagi berdasarkan area dan media penghantar, jenis jaringan komputer juga ada yang terbagi berdasarkan dari fungsi jaringan tersebut sendiri. Berikut adalah jenis-jenis jaringan komputer berdasarkan dari fungsinya:

- *Peer to Peer*

  Peer to peer adalah jaringan komputer dimana setiap komputer bisa menjadi *server* sekaligus *client*. Setiap komputer dapat menerima dan memberikan akses dari atau ke komputer lain. *Peer to peer* banyak diimplementasikan pada LAN walau dapat juga di implementasikan pada MAN, WAN, atau Internet.

- *Client Server*

  Client Server adalah jaringan komputer yang salah satu (boleh lebih) komputer difungsikan sebagai *server* atau induk bagi komputer lain. Dalam model ini *server* menjadi pusat komunikasi bagi client tersebut dan akan

menjadi media perantara dalam proses tukar menukar data. *Client* melakukan *request* kepada *server* yang akan menjalankan penuh *request* tersebut. Dalam suatu jaringan, sistem ini efisien karena dapat berkomunikasi dengan *client* lain di tempat yang berbeda. *Server* akan memiliki fungsi dapat mengatur efisiensi kerja dari jaringan yang berada dalam lingkupnya.

2.2. Protokol Jaringan

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras.[1]

2.2.1. Macam - macam Protokol Jaringan

1. *TCP/IP (Transmission Control Protocol/Internet Protocol*)

   TCP/IP adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (*software*) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah *TCP/IP stack*. Pada *TCP/IP* terdapat beberapa *subprotocol* yang menangani masalah komunikasi antar komputer. *TCP/IP*

   mengimplemenasikan arsitektur berlapis yang terdiri atas empat lapisan, diantaranya adalah:

   - Protokol lapisan aplikasi.
   - Protokol lapisan antar *host.*
   - Protokol lapisan *internetwork.*
   - Protokol lapisan antarmuka jaringan.

2. *UDP (User Datagram Protokol)*

   UDP adalah salah satu protokol lapisan *transport TCP/IP* yangmendukung komunikasi yang tidak andal (*unreliable*), tanpa koneksi (*connectionless*) antara *host-host* dalam jaringan yang menggunakan *TCP/IP*.

3. *PPP (Point-to-Point Protocol)*

   PPP adalah sebuah protokol enkapsulasi paket jaringan yang banyak digunakan pada *WAN*. Protokol ini merupakan standar industri yang berjalan pada lapisan *data-link* dan dikembangkan pada awal tahun 1990-an sebagai respon terhadap masalah-masalah yang terjadi pada protokol *Serial Line Internet Protocol (SLIP),* yang hanya mendukung pengalamatan *IP* statis kepada para *clien*nya.

4. *ICMP (Internet Control Message Protocol)*

   ICMP tidak digunakan secara langsung oleh aplikasi jaringan milik pengguna. Salah satu pengecualian adalah aplikasi *ping* yang mengirim pesan *ICMP Echo Request* (dan menerima *Echo Reply*) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan. Protokol *ICMP* utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan.

5. *DNS (Domain Name System)*

   DNS adalah *distribute database system* yang digunakan untuk pencarian nama komputer (*name resolution*) di jaringan yang mengunakan *TCP/IP*. *DNS* biasa digunakan pada aplikasi yang terhubung ke Internet seperti web browser atau email, dimana *DNS* membantu memetakan *hostname* sebuah komputer ke *IP address*. Selain digunakan di Internet, *DNS* juga dapat diimplementasikan ke *private network* atau intranet.

6. *SSH (Secure Shell)*

   SSH adalah protokol jaringan yang memungkinkan pertukaran data secara

aman antara dua komputer. *SSH* dapat digunakan untuk mengendalikan komputer dari jarak jauh mengirim *file*, membuat *tunnel* yang terenkripsi dan lain-lain. Protokol ini mempunyai kelebihan dibanding protokol yang sejenis seperti *Telnet* dan *FTP*, karena *SSH* memiliki sistem autentikasi, autorisasi, dan ekripsinya sendiri. Dengan begitu keamanan sebuah sesi komunikasi melalui bantuan *SSH* ini menjadi lebih terjamin.

7. *FTP (File Transfer Protocol)*

   FTP adalah sebuah protokol internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas (*file*) komputer dalam sebuah *internetwork*. *FTP* atau protokol *Transmission Control Protocol (TCP)* untuk komunikasi data antara klien dan *server*, sehingga diantara kedua komponen tersebut akan dibuatlah sebuah sesi komunikasi sebelum transfer data dimulai.

8. *SSL (Secure Socket Layer)*

   SSL adalah *arguably* internet yang paling banyak digunakan untuk enkripsi. Ditambah lagi, *SSL* digunakan tidak hanya keamanan koneksi web, tetapi untuk berbagai aplikasi yang memerlukan enkripsi jaringan *end-to-end*. *SSL* merupakan sistem yang digunakan untuk mengenkripsi pengiriman informasi pada internet, sehingga data dapat dikirim dengan aman. Protokol *SSL* mengatur keamanan dan integritas menggunakan enkripsi, autentikasi, dan kode autentikasi pesan.

2.3. DMVPN (Dynamic Multipoint VPN)

Dynamic Multipoint VPN (DMVPN) adalah jawaban Cisco atas meningkatnya permintaan perusahaan enterprise untuk dapat menghubungkan kantor cabang dengan kantor pusat dan antara satu sama lain dengan tetap menekan biaya, meminimalkan kompleksitas konfigurasi, dan meningkatkan fleksibilitas. Dengan DMVPN, satu *router* pusat, biasanya ditempatkan di kantor pusat, menjalankan peran *Hub* sedangkan semua *router* cabang lainnya adalah Juru-juru yang terhubung ke *router Hub* sehingga kantor cabang dapat mengakses sumber daya perusahaan. DMVPN terdiri dari dua desain penerapan utama:

- *DMVPN Hub & Spoke*, digunakan untuk melakukan interkoneksi dari kantor pusat ke cabang.
- *DMVPN Spoke-to-Spoke*, digunakan untuk melakukan interkoneksi cabang-ke-cabang.[2]

2.3.1. Latar Belakang *DMVPN*

Dengan semakin berkembangnya teknologi maka semakin berkembang pula sistem keamanannya. Bagi perusahaan besar mereka membutuhkan penghubung yang dapat menghubungkan kantor cabang mereka dengan kantor pusat, begitu juga sebaliknya, saat data di enkripsi melalui Internet lalu-lintas data mereka melindunginya. Sebagai contoh, sebuah toko retail harus terhubung dengan kantor pusatnya untuk mengetahui persediaan barang dan pemesanan, toko cabang tersebut dapat juga terhubung dengan sesama toko cabang lainnya untuk mengtahui sisa produk yang tersedia.

Dahulu, satu-satunya cara untuk menghubungkan cabang dangan pusat ialah dengan menggunakan *Layer-2* seperti *ISDN* atau *Frame Relay* untuk saling berkomunikasi. Dengan menggunakan *ISDN* atau *Frame Relay* akan memakan banyak waktu dan biaya yang cukup mahal. Jika semua kantor cabang (termasuk kantor pusat) sudah memiliki akses internet yang relatif murah, maka akses internet ini juga dapat digunakan untuk komunikasi *IP internal* antara cabang dan kantor pusat dengan menggunakan *IPsec tunnels* untuk memastikan privasi dan integritas data.

DMVPN adalah teknologi yang di perkenalkan Cisco untuk mempermudah koneksi antara kantor cabang dengan kantor pusat dan sebaliknya. *DMVPN* merupakan fitur yang ditawarkan oleh Cisco yang dapat memungkinkan pertukaran data melaui internet secara aman, seolah-olah data tersebut dikirimkan melalui perantara kabel. *DMVPN* memiliki banyak fitur dan teknologi seperti *IPSec (IP Security), mGRE (multipoint GRE), NHRP (Next Hope Resolution Protocol)*. Fitur *IPSec* membuat data yang di kirimkan ter-enkripsi dan ter-dekripsi. *IPSec* diibaratkan sebagai *Tunnel* (terowongan) untuk jalur lalu-lintas data.

DMVPN memiliki keunggulan dibandingkan *VPN* biasa, karena *VPN* biasa memiliki konfigurasi yang cukup rumit dan kompleks dalam hal ini pada *VPN* biasa seorang administrator harus memasukkan konfigurasi satu persatu atau *site-to-site*, apabila *site* di tambah maka konfigurasi ditambahkan juga. Berbeda dengan *DMVPN*, apabila ada *site* yang ditambahkan *DMVPN* secara *default* akan menambahkan *site* tersebut.

Cisco *DMVPN* memungkinkan lokasi cabang untuk berkomunikasi secara langsung satu sama lain melalui *WAN* publik atau internet, seperti ketika menggunakan *voice over IP (VOIP)* antara dua kantor cabang, tetapi tidak memerlukan koneksi *VPN* permanen antara situs. Hal ini memungkinkan penyebaran *zero-touch* dari *IPsec VPN* dan meningkatkan kinerja jaringan dengan mengurangi *latency* (jumlah waktu yang dibutuhkan paket data untuk berpindah di seluruh koneksi jaringan) dan *jitter* (variasi dari *delay* atau selisih antara *delay* pertama dengan *delay* selanjutnya), sekaligus mengoptimalkan pemanfaatan *bandwidth* kantor pusat.

Sudah selayaknya bagi perusahaan-perusahaan besar untuk membangun koneksi *IPSec* secara besar untuk menghubungkan cabang mereka melalui jaringan internet. *IPSec* mengenkripsi *traffic* antara dua titik (*peer to peer*) dan pengenkripsian tersebut dilalukan kedua titik menggunakan kata kunci yang rahasia. Karena kata kunci rahasia ini hanya terdapat antara kedua titik tersebut, jaringan terenkripsi secara erat antara kedua *peer.* Oleh karena itu, *IPSec* secara interinsik adalah penghubung antara titik tunnel dalam jaringan. Metode ini layak di implementasikan untuk jaringan berskala besar dan memiliki titik cabang yang banyak dan untuk mengatur kedalam *hub* dan *spoke* atau secara penuh menggunakan *mesh network.*

Dalam sebagian besar jaringan, *traffic IP* antara *spokes* dan *hub* cukup mendominasi dan antar *spoke* sangat kecil, jadi desain *hub* dan *spoke* sering menjadi pilihan utama. Desain ini juga cocok untuk jaringan *Frame Relay* versi lama, maka dari itu biaya yang dikeluarkan juga menjadi cukup mahal.

Ketika menggunakan internet sebagai penghubung antara *hub* dan *spoke*, *spoke* juga memiliki akses langsung ke *spoke* lainnya tanpa adanya biaya tambahan, tetapi cara ini cukup sulit, namun bukan hal yang mustahil untuk mengelola secara penuh maupun sebagian jaringan *mesh* ini. Menghubungkan jaringan secara penuh atau sebagian adalah cara paling menguntungkan karena dapat menghemat biaya jika *spoke* dapat berhubungan langsung dengan *spoke* lainnya tanpa adanya perantara *hub.*

Jika lalu lintas antar *spoke* melalui *hub*, maka *hub* akan menggunakan sumber dayanya dan berdampak kepada *delay*-nya paket data yang dikirim karena *hub* akan mengenkripsi *IPSec* dan mendekripsi paket data yang datang dari *spoke* pengirim dan di enkripsi kembali sebelum dikirimkan kepada *spoke* penerima. Sebagai contoh lainnya saat *spoke* dan *spoke* terhubung langsung akan sangat berfungsi ketika kedua *spoke* berada di kota yang sama sedangkan *hub* berada di negara atau kota berbeda, maka akan terjadi efisiensi dalam mengelola waktu dan biaya.

2.3.2. Fitur *Dynamic Multipoint VPN (DMVPN)*

Fitur *Dynamic Multipoint VPN (DMVPN)* memungkinkan pengguna untuk meningkatkan skala yang lebih baik pada *Virtual Private Network (VPN) IP Security (IPsec)* besar dan kecil dengan menggabungkan *tunnel Generic Routing Encapsulation (GRE)*, enkripsi IPsec, dan *Next Hop Resolution Protocol (NHRP)*.

Fitur *Dynamic Multipoint VPN (DMVPN)* menggabungkan *tunnel Generic Routing Encapsulation (GRE)*, enkripsi IPsec, dan *router* NHRP untuk memberi pengguna kemudahan konfigurasi melalui profil kripto yang menggantikan persyaratan untuk menentukan peta kripto statis dan penemuan dinamis titik akhir terowongan. Fitur ini mengandalkan dua teknologi standar Cisco yang disempurnakan berikut ini:

2.3.2.1. *NHRP* - Protokol klien dan server di mana *hub* adalah *server* dan jari-jarinya adalah klien. *Hub* memelihara *database NHRP* dari alamat antarmuka publik dari setiap *spoke*. Setiap *spoke* mendaftarkan alamat

aslinya ketika *boot* dan menanyakan *database NHRP* untuk alamat sebenarnya dari jari-jari tujuan untuk membangun *tunnel* langsung.

2.3.2.2. Antarmuka Terowongan *mGRE* - Memungkinkan satu antarmuka *GRE* untuk mendukung beberapa terowongan *IPsec* dan menyederhanakan ukuran dan kompleksitas konfigurasi.

2.3.2.3. Setiap ruji memiliki terowongan *IPsec* permanen ke *hub*, bukan ke jari-jari lain di dalam jaringan. Setiap berbicara terdaftar sebagai klien dari *server NHRP*.

2.3.2.4. Ketika *spoke* perlu mengirim paket ke subnet tujuan *(private)* di *spoke* lain, ia menanyakan *server NHRP* untuk alamat sebenarnya (di luar) dari tujuan (target) berbicara.

2.3.2.5. Setelah ruji asal "mempelajari" alamat *peer* dari ruji target, ia dapat memulai terowongan *IPsec* dinamis ke ruji target.

2.3.2.6. Terowongan *spoke-to-spoke* dibangun di atas antarmuka *GRE multipoint*.

2.3.2.7. Sambungan *spoke-to-spoke* dibuat sesuai permintaan setiap kali ada lalu lintas di antara jari-jari. Setelah itu, paket dapat melewati hub dan menggunakan tunnel *spoke-to-spoke*.[2]

2.3.3. *Dynamic Routing Protocol*

Routing dinamis adalah proses *router* yang me-rutekan jalur yang dibentuk secara otomatis oleh *router* itu sendiri sesuai dengan konfigurasi yang dibuat. Jika ada perubahan topologi antar jaringan, *router* otomatis akan membuat *routing* yang baru. *Routing* dinamis merupakan routing protocol digunakan untuk menemukan network serta untuk melakukan *update routing table* pada *router*. *Routing* dinamis ini lebih mudah dari pada menggunakan *routing* statis dan *default*, akan tetapi ada perbedaan dalam proses-proses di *CPU router* dan penggunaan *bandwidth* dari *link* jaringan.

Dynamic router mempelajari sendiri rute yang terbaik yang akan ditempuhnya untuk meneruskan paket dari sebuah *network* ke *network* lainnya. Administrator tidak menentukan rute yang harus ditempuh oleh paket-paket tersebut. Administrator hanya menentukan bagaimana cara router mempelajari paket, dan kemudian *router* mempelajarinya sendiri. Rute pada *dynamic* routing berubah, sesuai dengan pelajaran yang didapatkan oleh *router*, sebuah *router* yang

memiliki dan membuat tabel *routing* secara otomatis, dengan mendengarkan lalu lintas jaringan dan juga dengan saling berhubungan antara *router* lainnya.

Protokol routing mengatur *router-router* sehingga dapat berkomunikasi satu dengan yang lain dan saling memberikan informasi satu dengan yang lain dan saling memberikan informasi *routing* yang dapat mengubah isi *forwarding table,* tergantung keadaan jaringannya. Dengan cara ini, *router-router* mengetahui keadaan jaringan yang terakhir dan mampu meneruskan data ke arah yang benar.

Dengan kata lain, *routing* dinamik adalah proses pengisian data *routing* di *table routing* secara otomatis. Apabila jaringan memiliki lebih dari satu kemungkinan rute untuk tujuan yang sama maka perlu digunakan *dynamic routing.* Sebuah *dynamic routing* dibangun berdasarkan informasi yang dikumpulkan oleh protokol *routing*. Protokol ini didesain untuk mendistribusikan informasi yang secara dinamis mengikuti perubahan kondisi jaringan. Protokol *routing* mengatasi situasi *routing* yang kompleks secara cepat dan akurat. Protokol r*outing* didesain tidak hanya untuk mengubah ke rute *backup* bila rute utama tidak berhasil, namun juga didesain untuk menentukan rute mana yang terbaik untuk mencapai tujuan tersebut. Pengisian dan pemeliharaan tabel *routing* tidak dilakukan secara manual oleh admin. *Router* saling bertukar informasi *routing* agar dapat mengetahui alamat tujuan dan menerima tabel *routing*. Pemeliharaan jalur dilakukan berdasarkan pada jarak terpendek antara *device* pengirim dan *device* tujuan.

Keuntungan	**Kerugian**
Hanya mengenalkan alamat yang terhubung langsung dengan *router*nya (kaki-kakinya)	Beban kerja *router* lebih berat karena selalu memperbarui *ip table* pada setiap waktu tertentu.

Tidak perlu mengetahui semua alamat *network* yang ada.	Kecepatan pengenalan dan kelengkapan ip *table* terbilang lama karena *router* mem*broadcast* ke semua *router* sampai ada yang cocok. Sehingga setelah konfigurasi harus menunggu beberapa saat agar setiap *router* mendapat semua alamat *IP* yang ada.
Bila terjadi penambahan suatu *network* baru tidak perlu semua	Sulit melacak permasalahan pada suatu topologi jaringan lingkup besar.
router mengkonfigurasi, hanya *router-router* yang berkaitan	
Mudah dalam konfigurasi	

Tabel 1. Keuntungan dan Kerugian Menggunakan Dynamic Routing.

2.3.4. *DMVPN Phase*

DMVPN Phase memiliki beberapa phase yaitu *DMPVN Phase* 1, 2, 3. Dibawah ini adalah ciri-ciri phase yang dalam *DMVPN*:

Phase 1	Phase 2	Phase 3
Hub menggunakan *mGRE Tunnel*	*Hub* menggunakan *mGRE tunnel*	*Hub* menggunakan *mGRE tunnel* dan menambahkan konfigurasi *ip NHRP redirect*
Spoke menggunakan *GRE Tunnel*	*Spoke* menggunakan *GRE tunnel*	*Spoke* menggunakan *GRE tunnel* dan menambahkan konfigurasi *ip nhrp*

		shortcut
Antar *spoke* dapat berkomunikasi hanya jika melalui *Hub*	Spoke dapat berkomunikasi tanpa melalui *Hub*	Spoke dapat berkomunikasi tanpa melalui *Hub*

Tabel 2. Perbedaan Phase DMVPN

2.3.4.1.DMVPN Phase 1

Phase 1 DMVPN adalah *fase* dimana awal pembentukan *tunnel* antara *hub* dan *spoke-spokenya* menggunakan *dynamic IP address, hub* harus memiliki *static IP. Hub* menjadi unsur utama pertukaran data antara *spoke*, setiap *spoke* yang ingin mengirimkan data ke s*poke* lainnya harus melalui *hub.* Hal-hal yang perlu diketahui untuk membangun *DMVPN phase 1* adalah : *IP address*, *tunnel source*, dan *tunnel destination*.

Di dalam *DMVPN*, ketika kita belum mengetahui *IP Address* publik pada *spoke* akan terjadi koneksi sementara, *hub* tidak harus memiliki konfigurasi destinasi *tunnel.* Untuk mengatasi masalah itu kita harus ubah *tunnel mode* menjadi *Multipoint (tunnel mode gre multipoint*) pada konfigurasi *hub*. Setelah di ubah, *tunnel* tersebut akan *up* dan terkoneksi. Pada *DMVPN* ada sebuah mekanisme untuk membuat jalur *logical tunnel IP* pada *spoke* menuju *public IP*nya, mekanisme ini disebut juga *NHRP (Next Hop Resolution Protocol).*

Cara kerjanya adalah *spoke* mencoba untuk berhubungan dengan *hub* dan meregistrasikan *NHRP* databasenya. Paket pertama yang di kirim selalu diamankan oleh *IPSec* (paket ini yang membangun *IPSec tunnel* antara *Hub* dan *Spoke* pertama kali). Kita harus membuat *NHRP Network-ID* dan Authentikasi *NHRP* secara optional untuk me-r*egister spoke* kedalam *Hub. Spoke* memiliki jalur *NHRP static* untuk ke *hub*, dan *hub* menetapkan entri secara dinamis untuk setiap *spoke.*

Saat *spoke* pertama terhubung ke *hub, spoke* tersebut dengan sendirinya mengirimkan informasi routing yang ia miliki kepada *hub* melalui *tunnel.* Ada beberapa peringatan tergantung pada *routing protocol* yang digunakan. Sebagai contoh, *EIRGP* menggunakan aturan *Split Horizon* untuk menjadikan topologi yang bebas dari *looping*, aturan ini tidak memungkinkan informasi *routing* untuk mengirim kembali *link* yang telah mereka kirim. Kita harus men-*disable*-nya sehingga dapat mem-*forward* informasi *routing* dari *spoke* ke *spoke* lainnya.

2.3.4.2.DMVPN Phase 2

Dynamic Konsep dan konfigurasi *DMVPN Phase 2* memiliki hubungan dengan *Phase 1*, meskipun konsep dan konfigurasi *phase 1 dan 2* memiliki kesamaan sebenarnya arus lalu lintas data *(traffic)* dan konfigurasinya telah berubah. Perbedaan dari *phase 1* adalah:

- *Spoke to spoke tunnel* menjadi mungkin, lalu lintas data (*traffic*) antar *spoke* tidak perlu melalui *hub*. Hub akan menjadi pemantau lalu lintas data tersebut (tidak menjadi *priority next-hop*)
- Tidak mengizinkan *summarization* dan *default routing* pada *hub*.

2.3.4.3.DMVPN Phase 3

Konsep *DMVPN phase 3* juga berkesinambungan dengan *phase 1 dan 2* akan tetapi *phase 3* memiliki konfigurasi yang lebih kompleks. Perbedaan *phase 3* dengan *phase 1:*

- Pada phase 1 tidak terjadu spoke-to-spoke tunnel tetapi spoke secara dinamis mendaftarkan NBMA addres mereka ke hub. Spoke menggunakan p2p tunnels dan meroute semua traffic melaui hub.

- Perbedaan *phase 3* dan *phase 2:*

  Pada *phase 2* menggunakan trik “CEF” untuk menghubungkan *spoke-to- spoke tunnels*. Semua *spoke* butuh *merouting tab*le dengan tidak mengganti *next-hop- nya.*

2.3.5. Manfaat *Dynamic Multipoint VPN (DMVPN)*

Penggunaan *Dynamic Multipoint VPN* memiliki beberapa manfaat yang bisa didapatkan oleh klien. Manfaat yang diperoleh dalam penggunaan *Dynamic Multipoin*t diantaranya adalah sebagai berikut:

- Pengurangan Konfigurasi

1. Saat ini, untuk setiap *router* yang berbicara, ada blok baris konfigurasi terpisah pada *router hub* yang menentukan karakteristik peta kripto, daftar akses kripto, dan antarmuka terowongan *GRE.* Fitur ini memungkinkan pengguna untuk mengkonfigurasi antarmuka terowongan *mGRE* tunggal, profil *IPsec* tunggal, dan tidak ada daftar akses kripto di *router hub* untuk menangani semua *router* berbicara. Dengan demikian, ukuran konfigurasi pada *hub router* tetap konstan meskipun *spoke router* ditambahkan ke jaringan.
2. Arsitektur *DMVPN* dapat mengelompokkan banyak jari ke dalam satu antarmuka *GRE multipoint,* menghilangkan kebutuhan akan antarmuka fisik atau logis yang berbeda untuk setiap ruji dalam instalasi *IPsec* asli.

- Inisiasi Enkripsi *IPsec* Otomatis

GRE memiliki sumber peer dan alamat tujuan yang dikonfigurasi atau diselesaikan dengan NHRP. Dengan demikian, fitur ini memungkinkan *IPsec* untuk segera dipicu untuk tunneling GRE *point-to-point* atau ketika alamat peer GRE diselesaikan melalui NHRP untuk *tunnel GRE multipoint*.

1. Dukungan untuk *Router Spoke* yang Dialamatkan Secara Dinamis.

Saat menggunakan jaringan *VPN hub*-dan-*spoke GRE* titik-ke-titik dan *IPsec*, alamat *IP* antarmuka fisik dari *router* ruji harus diketahui saat mengkonfigurasi *router hub* karena alamat *IP* harus dikonfigurasi sebagai alamat tujuan terowongan GRE. Fitur ini memungkinkan *router spoke* memiliki alamat *IP* antarmuka fisik dinamis (umum untuk koneksi kabel dan DSL). Ketika *spoke router* menjadi *online*, ia akan mengirimkan paket pendaftaran ke *router hub*: di dalam paket pendaftaran ini, adalah alamat *IP* antarmuka fisik saat ini dari *spoke* ini.

2. Penciptaan Dinamis untuk Terowongan *Spoke-to-Spoke*.

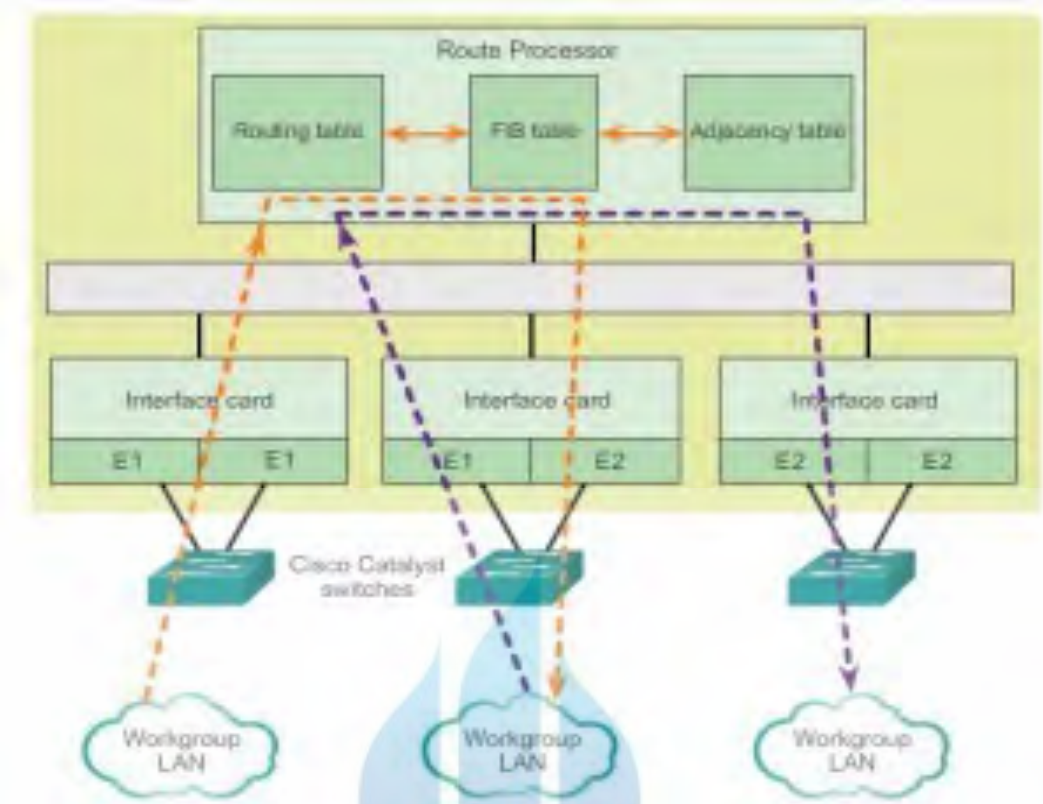
Fitur ini menghilangkan kebutuhan akan konfigurasi *spoke-to-spoke* untuk saluran langsung. Ketika *router spoke* ingin mengirimkan paket ke *router spoke* lain, *router* tersebut sekarang dapat menggunakan *NHRP* untuk secara dinamis menentukan alamat tujuan yang diperlukan dari *router spoke* target. (*Router hub* bertindak sebagai *server NHRP*, menangani permintaan untuk *router source spoke*). Kedua *router spoke* secara dinamis membuat terowongan *IPsec* di antara keduanya sehingga data dapat langsung ditransfer.

3. VRF Terintegrasi *DMVPN*

DMVPN dapat digunakan untuk memperluas jaringan *Multiprotocol Label Switching (MPLS)* yang digunakan oleh penyedia layanan untuk memanfaatkan kemudahan konfigurasi *hub* dan jari-jari, untuk memberikan dukungan bagi peralatan lokasi pelanggan (CPE) yang dialamatkan secara dinamis, dan untuk menyediakan penyediaan *zero-touch* untuk menambahkan jari-jari baru ke dalam *DMVPN*. **(*CISCO)**

2.4. *CEF (Cisco Express Forwarding)*

CEF adalah fitur dari Cisco untuk mengimplementasikan *fast-switching*. Perangkat Cisco yang mendukung layer 3 beralih menggunakan *Cisco Check Forwarding (CEF)*[3]. Metode penerusan ini cukup kompleks, tetapi untungnya seperti halnya teknologi baik, dilakukan di sebagian besar "di balik layar". Biasanya sangat sedikit konfigurasi *CEF* diperlukan pada perangkat Cisco.



Gambar 4. CEF

Pada dasarnya, CEF *decouples* biasa, saling ketergantungan antara *layer* 2 dan pengambilan keputusan *layer* 3, hal yang membuat *forwarding IP* paket lambat adalah konstan referensi kembali dan sebagainya antara *layer* 2 dan 3 lapisan konstruksi dalam perangkat jaringan. Jadi, sejauh yang *layer* 2 dan 3 lapisan struktur data dapat dipisahkan penerusan dipercepat. Dua komponen utama *CEF* operasi adalah:

A. Penerusan Informasi Dasar (FIB)

- *Adjacency Tabel*

FIB konseptual mirip dengan tabel *routing.* Sebuah *router* menggunakan tabel *routing* untuk menentukan jalan terbaik untuk tujuan jaringan berdasarkan bagian jaringan alamat *IP* tujuan. Dengan *CEF*, informasi yang sebelumnya disimpan di *cache rute*, Sebaliknya, disimpan dalam struktur data beberapa untuk *CEF switching*. Struktur data menyediakan dioptimalkan pencarian untuk efisien paket *forwarding*. Perangkat jaringan menggunakan

tabel pemeta FIB untuk membuat keputusan *switching* berbasis tujuan tanpa harus mengakses *cache* rute. FIB diperbarui ketika perubahan terjadi dalam jaringan dan berisi

semua rute yang dikenal pada waktu.

- Tabel *adjacency* mempertahankan *layer* 2 alamat *hop* berikutnya untuk semua *FIB entri.* Pemisahan informasi *reachability* (dalam tabel FIB) dan penerusan informasi (dalam tabel a*djacency*),menyediakan sejumlah manfaat:

a. Tabel *adjacency* dapat dibangun secara terpisah dari *table FIB*, memungkinkan baik dibangun tanpa paket apapun menjadi proses *switched*.

b. *MAC header* menulis ulang digunakan untuk menuruskan paket tidak disimpan dalam *entri cache,* sehingga perubahan dalam *MAC header* menulis ulang string tidak memerlukan penghapusan dari *entri cache*. CEF diaktifkan secara default pada Sebagian besar perangkat Cisco yang melakukan 3 *layer switching*.

2.5. *Internet Protocol Security (IPSec)*

IPSec (singkatan dari *IP Security*) adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. *IPSec* mendefiniskan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA *Reference Model (internetwork layer). IPSec* melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik *tunneling* untuk mengirimkan informasi melalui jaringan Internet atau dalam jaringan *Intranet* secara aman. *IPSec* didefinisikan oleh badan *Internet Engineering Task Force (IETF)* dan diimplementasikan di dalam banyak sistem operasi. *Windows 2000* adalah sistem operasi pertama dari *Microsoft* yang mendukung *IPSec*.[4]

IPSec (IP Security) merupakan kumpulan protokol yang dikembangkan oleh *IETF (Internet Engineering Task Force)* untuk mendukung pertukaran paket yang aman melalui *IP layer*. *IPSec* adalah protokol *security* berbasis kriptografi yang bekerja pada layer network, menyediakan keamanan transmisi data. *IPSec* dirancang untuk menyediakan keamanan berbasis kriptografi yang memiliki karakteristik *interoperable* dan berkualitas. *IPSec* memberikan layanan keamanan seperti *confidentiality*, *authentication*, dan *integrity*.

1. **Confidentiality**

Untuk menjamin kerahasiaan informasi data yang dipertukarkan agar tidak dapat dimengerti oleh pihak-pihak yang tidak berhak.

2. Integrity

Untuk menjamin bahwa data tidak berubah dalam perjalanan menuju tujuan.

3. Authentication

Untuk menjamin bahwa data yang dikirimkan memang berasal dari pengirim yang benar.

Secara teknis, *IPSec* terdiri atas dua bagian utama. Bagian pertama mendeskripsikan dua protokol untuk penambahan *header* pada paket yang membawa *security identifier*, dan mengenai *integrity control*, dan informasi keamanan lain, yaitu:

1. *Authentication Header (AH)* menyediakan data *integrity*, data *origin authentication*, dan proteksi terhadap *replay attack*.
2. *Encapsulating Security Payload* menyediakan layanan yang disediakan oleh AH ditambah dengan *confidentiality*.[5]

Penggunaan Bagian kedua berkaitan dengan protokol pembangkit dan distribusi kunci, yaitu implementasi protokol *IKE (Internet Key Exchange)* yang berfungsi dalam pembangkitan dan pertukaran *cryptographic key* secara otomatis. *Cryptographic key* digunakan dalam authentikasi *node* yang berkomunikasi dalam proses enkripsi dan dekripsi paket yang dikirimkan. Mode *IPSec* terdiri dari dua, yaitu:

- *Transport mode, protocol* menyediakan proteksi terhadap *layer* diatas *IP layer*. Hal ini dilakukan dengan penambahan *IPSec header* diantara *IP header* dengan *header protocol layer* diatas *IP* yang diproteksi.
- *Tunnel mode, protocol* menyediakan proteksi pada paket *IP* sehingga sekaligus melindungi layer diatas *IP layer.* Hal ini dilakukan dengan mengenkapsulasi paket *IP* yang akan diproteksi.[5]

IPSec diimplementasikan pada lapisan *transport* dalam *OSI Reference Model* untuk melindungi protokol *IP* dan protokol-protokol yang lebih tinggi dengan menggunakan beberapa kebijakan keamanan yang dapat dikonfigurasikan untuk memenuhi kebutuhan keamanan pengguna, atau jaringan. *IPSec* umumnya diletakkan sebagai sebuah lapsian tambahan di dalam *stack* protokol *TCP/IP* dan diatur oleh setiap kebijakan keamanan yang diinstalasikan dalam setiap mesin komputer dan dengan sebuah skema enkripsi yang dapat dinegosiasikan antara pengirim dan penerima. Kebijakan-kebijakan keamanan tersebut berisi kumpulan filter yang diasosiasikan dengan kelakuan

tertentu. Ketika sebuah alamat *IP*, nomor *port TCP dan UDP* atau protokol dari sebuah paket datagram *IP* cocok dengan *filter* tertentu, maka kelakukan yang dikaitkan dengannya akan diaplikasikan terhadap paket *IP* tersebut.

Dalam sistem operasi *Windows 2000, Windows XP,* dan *Windows Server 2003*, kebijakan keamanan tersebut dibuat dan ditetapkan pada *level domain Active Directory* atau pada *host individual* dengan menggunakan *snap-in IPSec Management* dalam *Microsoft Management Console (MMC).* Kebijakan *IPSec* tersebut, berisi beberapa peraturan yang menentukan kebutuhan keamanan untuk beberapa bentuk komunikasi. Peraturan-peraturan tersebut digunakan untuk memulai dan mengontrol komunikasi yang aman berdasarkan sifat lalu lintas *IP*, sumber lalu lintas tersebut dan tujuannya. Peraturan-peraturan tersebut dapat menentukan metode-metode autentikasi dan negosiasi, atribut proses *tunneling*, dan jenis koneksi.

Untuk membuat sebuah sesi komunikasi yang aman antara dua komputer dengan menggunakan *IPSec*, maka dibutuhkan sebuah *framework* protokol yang disebut dengan *ISAKMP/Oakley. Framework* tersebut mencakup beberapa algoritma kriptografi yang telah ditentukan sebelumnya, dan juga dapat diperluas dengan menambahkan beberapa sistem kriptografi tambahan yang dibuat oleh pihak ketiga. Selama proses negosiasi dilakukan, persetujuan akan tercapai dengan metode autentikasi dan kemanan yang akan digunakan, dan protokol pun akan membuat sebuah kunci yang dapat digunakan bersama *(shared key)* yang nantinya digunakan sebagi kunci enkripsi data. *IPSec* mendukung dua buah sesi komunikasi keamanan, yakni sebagai berikut:

- Protokol *Authentication Header (AH):* menawarkan autentikasi pengguna dan perlindungan dari beberapa serangan (umumnya serangan *man in the middle*), dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas si pengirim adalah benar adanya, dan data pun tidak dimodifikasi selama transmisi. Namun, *protocol AH* tidak menawarkan fungsi enskripsi terhadap data yang ditransmisikannya. Informasi *AH* dimasukkan kedalam *header* pake *IP* yang dikrimkan dan dapat digunakan secara sendirian atau bersamaan dengan *protocol Encapsulating Security Payload*.[6]
- Protokol *Encapsulating Security Payload (ESP):* Protokol ini melakukan enkapsulasi serta enskripsi terhadap data pengguna untuk meningkatkan

perlindungan dari beberapa sengan dan dapat digunakan secara sendirian informasi mengenai *ESP* juga dimasukkan ke dalam header paket *IP* yang dikirimkan.

Beberapa perangkat keras serta perangkat lunak dapat dikonfigurasikan untuk mendukung *IPSec*, yang dapat dilakukan dengan menggunakan enkripsi kunci publik yang disediakan oleh *Certificate Authority* (dalam sebuah *public key infrastructure*) atau kunci yang digunakan bersama yang telah ditentukan sebelumnya (skema *Pre-Shared Key/PSK*) untuk melakukan enkripsi secara privat.[7]

2.6. *EIGRP (Enhanced Interior Gateway Routing Protocol)*

EIGRP (Enhanced Interior Gateway Routing Protocol) adalah protokol *routing* yang termasuk proprietari Cisco, yang berarti hanya bisa dijalankan pada *router* Cisco, *EIGRP* bisa jadi merupakan protokol *routing* terbaik didunia jika bukan merupakan proprietari Cisco. Kelebihan utama yang membedakan *EIGRP* dari protokol *routing* lainnya adalah *EIGRP* termasuk satu-satunya protokol *routing* yang menawarkan fitur *backup route,* dimana jika terjadi perubahan pada *network*, *EIGRP* tidak harus melakukan kalkulasi ulang untuk menentukan *route* terbaik karena dapat langsung menggunakan *backup route.* Kalkulasi ulang *route* terbaik dilakukan jika backup *route* juga mengalami kegagalan. Berikut adalah fitur-fitur yang dimiliki *EIGRP*:

- Termasuk *protocol routing distance vector* tingkat lanjut *(advanced distance vector)*.
- Waktu *convergence* yang tepat.
- Mendukung VLSM dan subnet-subnet yang *discontiguous* (tidak bersebelahan / berurutan).
- *Partial updates*, tidak seperti RIP yang selalu mengirimkan keseluruhan *table routing* dalam pesan *update EIGRP* menggunakan partial updates atau *triggered update* yang berarti hanya mengirimkan *update* jika terjadi perubahan pada *network* (misalnya: ada *network* yang *down*).
- Mendukung *multiple protocol network.*
- Desain *network* yang *flexible*.
- *Multicast* dan *unicast*, *EIGRP* saling berkomunkasi dengan tetangga (*neighbor*)-nya secara *multicast* (224.0.010) dan tidak membroadcastnya.

- M*anual summarization*, *EIGRP* dapat melakukan *summarization* dimana saja.
- Menjamin 100% topologi *routing* yang bebas *looping*.
- Mudah dikonfigurasi untuk *WAN* dan *LAN*.
- *Load balancing* via jalur dengan *cost equa*l dan *unequal*, yang berarti *EIGRP* dapat menggunakan 2 link atau lebih ke suatu network destination dengan koneksi *bandwidth (cost metric)* yang berbeda dan melakukan *load sharing* pada *link-link* tersebut dengan beban yang sesuai yang dimiliki oleh link masing-masing, dengan begini pemakaian *bandwitdth* pada setiap link menjadi lebih efektif, karena link dengan *bandwidth* yang lebih kecil tetap digunakan dan dengan beban yang sepadan juga.

2.6.1. Struktur *Data EIGRP*

Paket yang digunakan oleh *EIGRP* yaitu :

- Hello Paket, dikirim secara *multicast* melalui *ip address*224.0.0.10. Hello paket digunakan untuk mengetahui jalur ke arah *router* lain masih hidup atau mati. Hello paket secara *default* dikirimkan setiap 15 detik secara simultan, Jika *router* lain tidak merespon hello paket ini melebihi *hold time* yaitu 45 detik maka jalur ke *router* lain tersebut akan dianggap mati dan DUAL akan mengkalkulasikan ulang dan mencari jalur lain.
- *Update* Paket, digunakan untuk menyampaikan tujuan yang dapat dijangkau oleh *router*. Ketika sebuah *router* baru ditemukan *update* paket dikirim secara *unicast* sehingga *router dapat membangun topologi table. Dalam kasus lain, Update paket dikirim secara multicast untuk perubahan link-cost.*
- *Query* Paket, adalah sebuah *request* atau permintaan yang dilakukan secara *multicast* yang akan meminta sebuah *route*. Selama mengirimkan *query* paket, setiap *router* akan melanjutkan untuk meneruskan *query* paket tersebut sampai sebuah router akan mengirimkan sebuah *reply* paket sebagai informasi bagaimana caranya untuk menuju ke sebuah jaringan tertentu.
- *Reply* Paket dikirim apabila router tujuan tidak memiliki *feasible successors*. *Reply* paket dikirim untuk merespon *query* paket yang

menginstrusikan bahwa *router* pengirim tidak memperhitunghkan ulang jalurnya karena *feasible successors* masih tetap ada. *Reply* paket adalah paket *unicast* yang dikirim ke *router* yang mengirimkan *query packet*.

2.6.2. Teknologi *EIGRP*

Untuk menyediakan proses *routing* yang handal EIGRP menggunakan 4 teknologi yang dikombinasikan dan membedakannya dengan *routing protocol* yang lain, yaitu :

- *Neighbour Discovery/Recovery*

  Mekanisme *neighbour discovery/recovery* mengijinkan *router* secara dinamis mempelajari *router* lain yang secara langsung terhubung ke jaringan mereka. *Router* juga harus mengetahui ketika *router* tetangganya tidak dapat lagi dijangkau. Proses ini dicapai dengan *low-overhead* yang secara periodik mengirimkan hello paket yang kecil. Selama *router* menerima Hello paket dari *router* tetangga, router tersebut menganggap bahwa router tetangga tersebut masih berfungsi dan keduanya masih bisa melakukan pertukaran informasi.

- *Reliable Transport Protocol (RTP)*

  Reliable Transport Protocol (RTP) bertanggung jawab untuk menjamin pengiriman dan penerimaan paket *EIGRP* ke semua *router*. *RTP* juga mendukung perpaduan pengiriman paket secara *unicast* ataupun *multicast*. Untuk efisiensi, hanya beberapa paket *EIGRP* yang dikirimkan. Pada jaringan multiakses yang mempunyai kemampuan untuk mengirimkan paket secara *multicast* seperti *ethernet*, tidak perlu mengirimkan hello paket ke semua *router neighbor* secara individu. Untuk alasan tersebut, *EIGRP* mengirimkan single multicast hello paket yang berisi sebuah *indicator* yang menginformasikan si penerima bahwa paket tidak

perlu dibalas. Tipe paket yang lain seperti update paket mengindikasikan bahwa balasan terhadap paket tersebut diperlukan.

- *DUAL finite-state Machine*

  DUAL finite-state machine menaruh keputusan proses untuk semua perhitungan jalur dengan mengikuti semua jalur yang telah dinyatakan oleh semua *router neighbor*. *DUAL* menggunakan informasi tentang jarak untuk memilih jalur yang efisien, *loop-free* dan memilih jalur untuk ditempatkan di dalam *routing table* berdasarkan *successors* yang telah dibuat oleh *DUAL*, *successor* adalah *router* yang berdekatan yang digunakan untuk meneruskan paket yang mempunyai nilai *cost* paling sedikit dengan *router* tujuan dan dijamin bebas dari dari *routing loop*. Ketika perubahan topologi terjadi, *DUAL* akan mencoba mencari *successors*.

- *Protocol-Dependent Module*

  Protocol-dependent module bertanggung jawab pada *layer network* yang memerlukan protokol khusus. Misalnya *IP - EIGRP module* yang bertanggung jawab untuk mengirim dan menerima paket *EIGRP* yang telah dienkapsulasi di dalam *protocol IP*.

2.7. *Tunnelling GRE*

Tunneling adalah suatu mekanisme enkapsulasi *PDU (Packet Data Unit)* dengan *protocol* yang lain dengan maksud untuk mengirimkan data pada *foreign network.*[8] Tiga komponen utama dalam *tunneling* adalah:

- *Passenger Protocol*, yaitu protokol yang dienkapsulasi.
- Carrier Protocol, yaitu protokol yang melakukan enkapsulasi.
- *Transport Protocol*, yaitu protokol yang membawa (mengirim) PDU yang telah dienkapsulasi.[9]

Generic Routing Encapsulation (GRE) merupakan sebuah protokol tunneling yang memilki kemampuan membawa lebih dari satu jenis protokol pengalamatan komunikasi. Paket yang akan dilewatkan melalui *foreign network* dienkapsulasi menjadi sebuah paket yang bersistem pengalamatan IP kemudian paket tersebut dilewatkan melalui *tunnel*.[9]

Popularitas *Virtual Private Network (VP*N) telah meningkat pesat selama beberapa tahun terakhir. Perangkat keras adalah point terpenting dalam hal ini, perangkat keras yang memungkinan akselerasi VPN dengan mengefektifkan biaya dan dapat dilakukan pada satu perangkat. GRE adalah sebuah *tunnel protocol* yang ditemukan oleh Cisco dan dapat meng-enkapsulasi bermacam-macam *network layer protocol* dalam skala besar secara *virtual* menghubungkan *point to point* melalui sebuah *Internet Protocol*.

OSI Layer	***Protocol***
5. Session	*X.225*
4. Transport	*UDP*
3. Network(GRE-encapsulated)	*IPv6*
Encapsulation	***GRE***
3. Network	*IPv4*
2. Data Link	*Ethernet*
1. Physical	*Ethernet physical layer*

Tabel 3. Contoh Protokol disetiap *Layer*

- *P2P GRE*

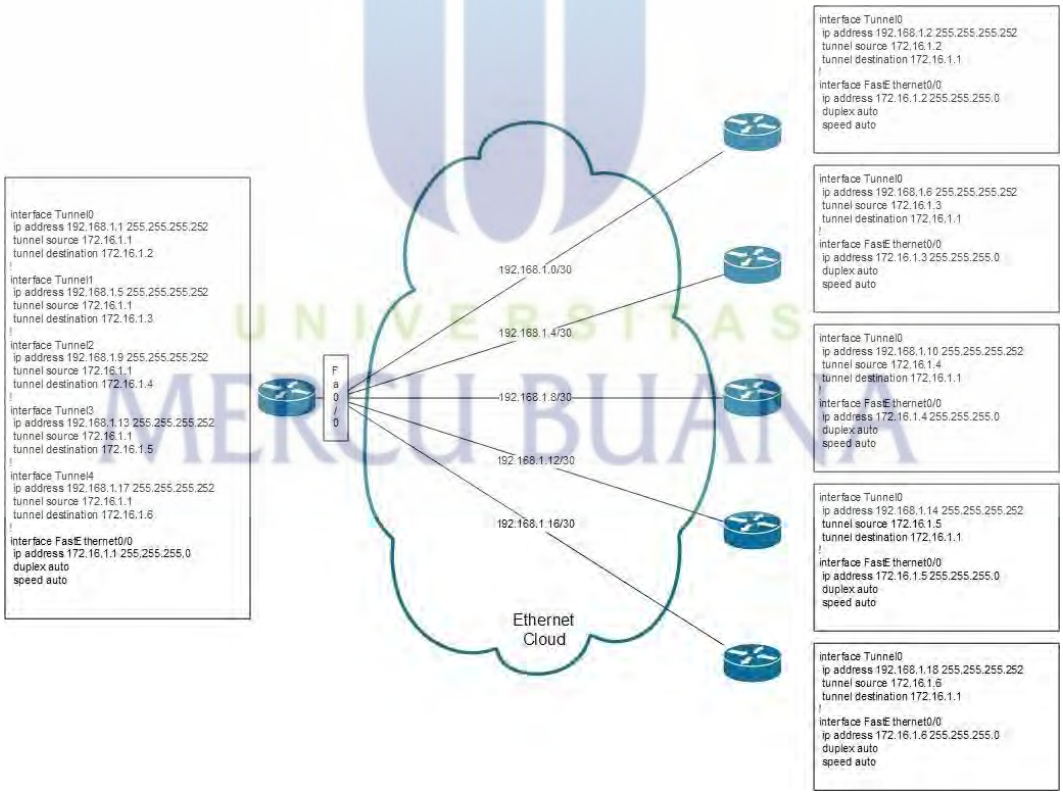
P2P merupakan singkatan dari *peer-to-peer* atau teknologi dari “ujung” ke “ujung” pertama kali di luncurkan dan dipopulerkan oleh aplikasi-aplikasi “berbagi-berkas” (*file sharing*) seperti Napster dan KaZaA. Pada konteks ini teknologi *P2P* memungkinkan para pengguna untuk berbagi, mencari dan mengunduh berkas.

Sistem *P2P* yang sebenarnya adalah suatu sistem yang tidak hanya menghubungkan “ujung” satu dengan lainnya, namun ujung-ujung ini saling berhubungan secara dinamis dan berpartisipasi dalam mengarahkan lalu lintas

komunikasi informasi-, pemrosesan-, dan penugasan pembagian *bandwidth* yang intensif, di mana bila sistem ini tidak ada, tugas-tugas ini biasanya diemban oleh *server* pusat.

Aplikasi *P2P* yang sebenarnya memerlukan satuan tim-tim kecil dengan ide cemerlang untuk mengembangkan perangkat lunak dan bisnis-bisnis yang mungkin dilakukan oleh perangkat tersebut – dan mungkin saja bisa membuat perusahaan besar yang sudah ada gulung tikar. *P2P* yang sebenarnya, bila diaplikasikan pada pasar yang sudah matang dan stabil adalah teknologi yang "mengganggu".

Ide mengenai konsep ini muncul kira-kira pada akhir dekade 1980-an, ketika jaringan komputer dan tentunya juga komputer telah mulai masuk ke dalam salah satu barang wajib dalam perusahaan, baik itu perusahaan kecil maupun besar. Tetapi, arsitektur ini berkembang dalam jaringan yang terlalu kecil untuk memiliki sebuah *server* yang terdedikasi, sehingga setiap komputer klien pun menyediakan layanan untuk berbagi data untuk melakukan kolaborasi antara pengguna.



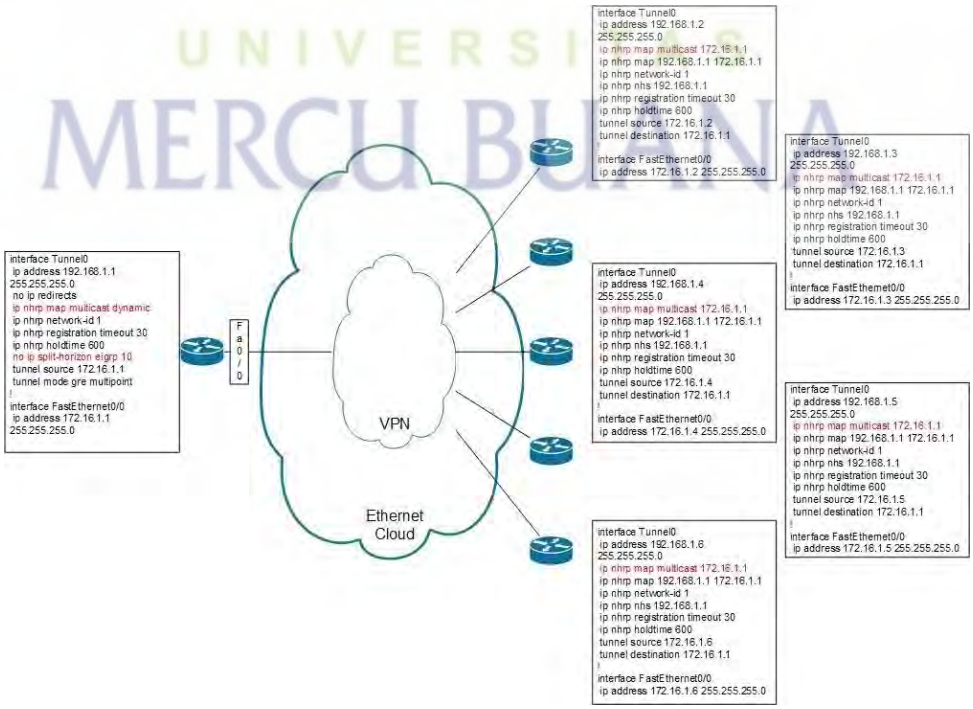
Gambar 5. Contoh P2P GRE

- *Multipoint GRE (mGRE)*

Sebuah *GRE tunnel* pada mulanya adalah *point-to-point* yang artinya menghubungkan antar satu titik ke titik lainnya. Untuk mendukung topologi jaringan yang kompleks seperti teknologi *hub-and-spoke* dan *spoke-to-spoke* menggunakan *point-to-point tunnel* adalah sebuah masalah. Sebagai contoh, jaringan dengan topologi mesh mengkonsumsi alamat *IP* yang cukup banyak karena setiap pasang dari *tunnel endpoint* menggunakan *subnet* yang berbeda. *Multipoint GRE (mGRE)* memungkinkan pengiriman data dengan destinasi yang banyak. Sebagai contoh *multiple spoke sites* yang di kelompokan menjadi sebuah *interface multipoint.*

Untuk membangun *tunnel* yang terhubung satu sama lain, *mGRE* menggunakan cara pengalamatan dengan *Next Hop Resolution Protocol (NHRP). Hub* akan bertindak sebagai *NHRP database* dan *spoke*. *NHRP* memiliki kegunaan yang sama dengan *ARP (Address Resolution Protocol)* pada *Ethernet*, yang mampu memetakan sebuah *IP Address Tunnel* dengan *logical (Non- Broadcast Multi-Access (NBMA));* memungkinkan *mGRE* secara dinamis untuk men-*setup tunnel* tanpa mengkonfigurasi pemetaan data antara *next-hop*

tujuan.[10]



Gambar 6. Contoh Multipoint GRE

Manfaat yang diperoleh dalam penggunaan *Dynamic Multipoint* diantaranya adalah sebagai berikut: Antarmuka Terowongan *mGRE* - Memungkinkan satu antarmuka *GRE* untuk mendukung beberapa terowongan *IPsec* dan menyederhanakan ukuran dan kompleksitas konfigurasi. Setiap ruji memiliki terowongan *IPsec* permanen ke *hub*, bukan ke jari-jari lain di dalam jaringan. Setiap berbicara terdaftar sebagai klien dari *server NHRP*.

2.8. *Next Hop Resolution Protocol (NHRP)*

Didalam jaringan komputer, *Next Hop Resolution Protocol (NHRP)* adalah sebuah protokol atau cara yang dapat digunakan komputer untuk mengirim data ke komputer lainnya dan menentukan jalur yang terhubung diantara mereka (menggunakan angka terkecil dan jalur tercepat dalam menentukan *hops*) untuk di terima oleh komputer lainnya. Jika komputer yang menerima berada dalam *subnetwork* yang sama, penggunaan *NHRP* akan memberitahu komputer pengirim bahwa komputer penerima berada pada jaringan lokal dan dapat mengirim paket data berikutnya langsung ke komputer yang menerima menggunakan alamat *subnetwork* dan bukan alamat jaringan global. Jika komputer yang menerima berada pada *subnetwork* yang berbeda, penggunaan *NHRP* akan memberitahu komputer pengirim bahwa komputer pada *subnetwork* berbeda, lalu *router* akan menyediakan jalur tercepat ke komputer penerima dan pengirim dapat mengirimkan paket data dan dapat meneruskannya ke *router* tersebut. *Cache* pada *hub* dan *spoke* dapat dibangun disalah satu cara berikut:

- Menambahkan entri Statis secara manual.
- *Hub* mempelajari permintaan registrasi dengan *spoke*.
- *Spokes* mempelajari permintaan resolusi yang digunakanb *spoke-to-spoke* untuk berkomunikasi.

BAGIAN 3 ANALISA SISTEM

Routing dan *switching* dengan metode lama seperti *P2P (peer to peer*) dan *static routing and switching* sangat rentan bagi perusahan, ini memudahkan *hacker* mencuri data yang dikirimkan dari suatu kantor cabang ke kantor pusat atau sebaliknya atau antar kantor cabang. Ini semua karena tidak adanya enkripsi terhadap data tersebut sehingga, perlu adanya sebuah metode untuk enkripsi data tersebut agar tidak mudah untuk dimodifikasi oleh pihak yang tidak bertanggung jawab.

3.1. Analisa Masalah

Penggunaan *routing* dalam perusahaan ini masih menggunakan routing yang sederhana, sehingga memungkinkan data atau *package loss* dalam pengiriman antar kantor cabang. Metode *routing* yang digunakan adalah metode *routing static*, metode ini sangat memerlukan upaya lebih ketika ada penambahan *devices* dan atau ada penambahan kantor cabang. Bila ada penambahan kantor cabang maka *network engineer* harus memulai konfigurasi pada alat baru tersebut selanjutnya menambah konfigurasi pada *router* yang sudah ada untuk menambahkan *routing* table baru. Dikarenakan *routing static* ini tidak memiliki *routing table* yang baik sehingga untuk men-*troubleshoot* memerlukan waktu yang cukup lambat. Apabila terjadi downtime kemungkinan paket akan *looping* hingga di-*drop* karena tidak menemukan alamat IP yang dituju.

3.2. Analisa Sistem

Analisa sistem merupakan langkah awal dari mengapa sistem ini perlu dikembangkan. Diperlukan beberapa cara yang dapat diterapkan untuk menjelaskan kebutuhan keamanan jaringan. Analisa sistem ini dibagi menjadi beberapa faktor diantaranya adalah pemilihan *device,* pemilihan *routing table* pemilihan cara mengenkripsi data, berikut ini adalah hasil analisa yang memungkinkan untuk diimplementasikan kepada perusahaan:

1. Pada perangkat keras, menggunakan *router* Cisco dengan *series* 3725, menggunakan IOS *version* diatas 12 (dua belas).
2. *Routing* dengan metode EIGRP (*Enhanced Interior Gateway Routing Protocol).*
3. *DMVPN (Dynamic multipoint virtual private Network) phase* 3.
4. *IP security*.
5. *Tunneling*.

3.3. Analisa Proses

Proses yang dilakukan pada sistem konfigurasi DMVPN ini merupakan suatu proses pemutakhiran sistem yang sudah ada. Pada awalnya, konfigurasi jaringan ini menggunakan jaringan statik. Pada jaringan statik memerlukan beberapa upaya.

Dalam prosesnya konfigurasi *DMVPN* menggunakan *IPSec* dan *routing EIGRP* membutuhkan *source* yang tidak murah. Akan tetapi dengan adanya keamanan jaringan ini menjadi awal untuk investasi dan diharapkan terjadinya kepercayaan di antara investor, pelanggan dan pemangku kebijakan karena keamanan data menjadi prioritas utama bagi seluruh lapisan tersebut.

Pada analisa proses ini langkah-langkah yang perlu dilakukan adalah sebagai berikut;

Pertama, menentukan perangkat yang akan digunakan. Dalam penulisan ini Menggunakan perangkat *router* Cisco dengan seri 7200. Perangkat ini digunakan di seluruh kantor pusat maupun kantor cabang dengan tujuan standarisasi perangkat dengan harapan memudahkan *engineer* untuk konfigurasi perangkat ini.

Kedua, menggunakan *routing* EIGRP (*Enhanced Interior Gateway Routing Protocol).* Metode rute ke ini sangat tepat dikarenakan EIGRP, hanya ada pada perangkat *router* dan *switch* Cisco dengan catatan menambah lisensi

baru Karena module ini tidak termasuk pada router maupun switch yang standar.

3.4. Analisis Perangkat

Tulisan dan Tugas Akhir ini dibuat dengan menggunakan beberapa perangkat baik perangkat lunak maupun perangkat keras. Berikut adalah pemaparan perangkat yang digunakan dalam penulisan ini:

3.4.1. Perangkat Keras (*Hardware*)

Perangkat keras (*hardware*) yang akan digunakan dalam penelitian ini adalah sebagai berikut;

a. **Laptop *MacBook Pro (2018)***

- *Operating system mac OS Catalina v 10.15.4.*
- *Monitor 16 inch.*
- *Processor Intel Core i7.*
- *Memory 16 GB 2400 MHz DDR4.Graphics Radeon Pro 555X 4 GB dan Intel UHD Graphics 630 1536 MB.*
- *SSD 256 GB.*

b. **Perangkat dan bahan yang dibutuhkan *(optional)***

- *Router Cisco series 7200 (4 unit).*
- Kabel UTP RJ45 3 buah.

3.4.2. Perangkat Lunak (*Software*)

a. ***GNS3* versi terbaru**.

GNS3 adalah aplikasi simulator jaringan (*Graphic Simulator Network*) berbasis GUI yang di rilis pada tahun 2008. Dengan GNS3 kita bisa mensimulasikan perangkat asli baik dengan bantuan emulator ataupun teknologi virtualisasi. Salah satu teknologi *emulator* yaitu dynamips, yang digunakan untuk mensimulasikan Cisco IOS.

***b. VM Machine* (*optional*).**

Virtual Machine (VM) adalah program perangkat lunak atau sistem operasi yang tidak hanya menunjukkan perilaku komputer yang terpisah, tetapi juga mampu melakukan tugas-tugas seperti menjalankan aplikasi dan program seperti komputer yang terpisah.

c. Wireshark.

Wireshark adalah program *Network Protocol Analyzer* alias penganalisa protokol jaringan yang lengkap. Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin

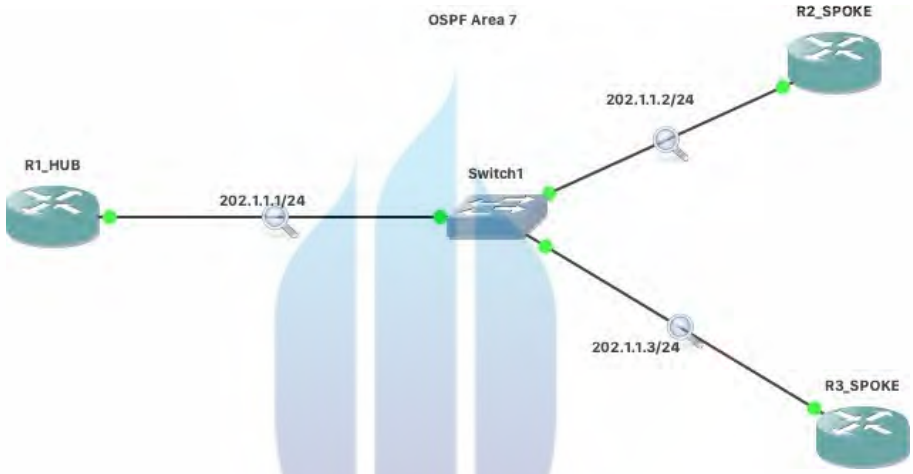
d. Image IOS Cisco 7200.

BAGIAN 4 PERANCANGAN

4.1. Skema dan Gambar Kerja

4.1.1. *Existing Configuration*

Bagian ini menjelaskan mengenai topologi yang sudah ada sebelumnya serta konfigurasi yang digunakan dalam interkoneksi antar *HUB* dan *SPOKE(s)*.

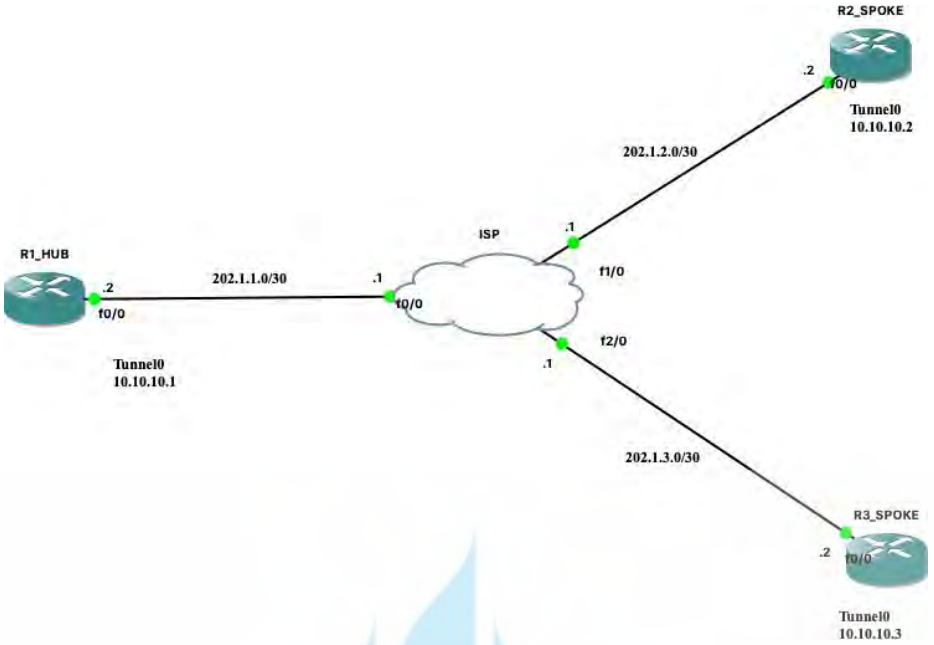


Gambar 7. Topologi jaringan *existing*.

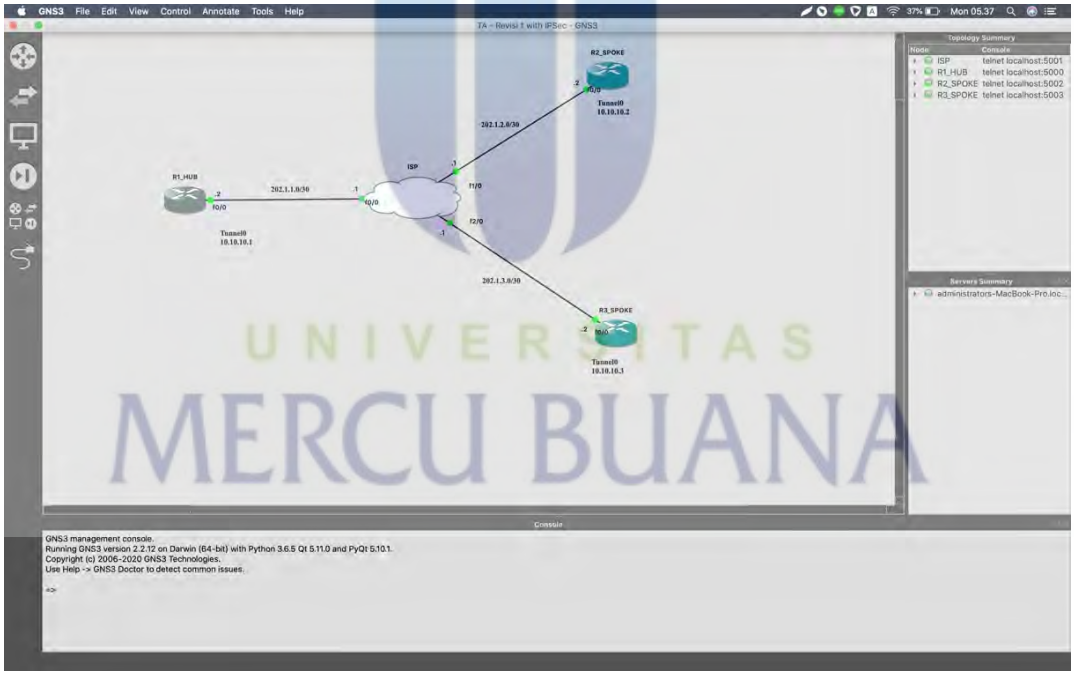
Saat ini, PT.Cahaya Kreatif Digital menggunakan konfigurasi *OSPF (Open Shorten Path First)* untuk menghubungkan antar kantor.

4.1.2. Topologi *DMVPN*

Pada bagian ini, topologi serta konfigurasi akan dijelaskan. Berikut ini topologi yang digunakan pada percobaan konfigurasi*DMVPN* menggunakan *IPSec* dan *Routing EIGRP* pada PT. Cahaya Kreatif Digital.



Gambar 8. Topologi jaringan *DMVPN*.



Gambar 9. Topologi jaringan pada GNS3.

Pada topologi jaringan di atas tersedia 3 buah router dan masing- masing diberi nama R1_HUB, ISP, R2_SPOKE dan R3_SPOKE. R1_HUB adalah *router hub* yang berfungsi sebagai penghubung antara spoke dan dihubungkan dengan ISP. ISP disini dianalogikan sebagai *ISP (Internet Service Provider*).

R2_SPOKE dihubungkan dengan ISP agar dapat berkomunikasi dengan R1_HUB maupun R3_SPOKE. R3_SPOKE dihubungkan dengan *router* ISP.

Tunneling proses terjadi melalui *router* ISP, antar router HUB dan SPOKE. Proses *tunneling* ini membuat transfer data menjadi lebih singkat sebagai contoh apabila R1_HUB ingin mengirimkan data menuju R2_SPOKE, seolah-olah antara kedua *router* ini memiliki suatu jalur khusus seperti terowongan yang menghubungkan dua titik. Contoh lainnya, apabila R2_SPOKE Mengirimkan data menuju R3_SPOKE ataupun sebaliknya kedua *router* tersebut tidak R1_HUB untuk berkomunikasi, ke kedua *router* ini memiliki terowongan untuk mentransfer data nya sendiri sehingga proses komunikasi atau transfer data menjadi lebih singkat dan dapat mengurangi beban *router* R1_HUB.

4.2. Konfigurasi Perangkat

Pastikan IOS yang terdapat di dalam keempat *router* tersebut mendukung untuk fitur *DMVPN*. Sebagai contoh apabila kita menggunakan *router* cisco tipe 3725 dan meng-*upgrade* IOS tersebut dengan *module* atau *license boot module security9*.

Setelah perangkat dan bahan disiapkan dan sudah dipasang sesuai topologi langkah selanjutnya yaitu proses konfigurasi tiap *router* dengan memberikan *IP address* dan memasukkan *command-command* terkait. Berikut adalah konfigurasi yang perlu dilakukan untuk menerapkan konfigurasi *DMVPN menggunakan IPSec dan EIGRP*:

4.2.1. Pilih *Router* dan IOS yang dapat mendukung teknologi DMVPN dan EIGRP

Router yang dapat melakukan ini adalah *router* dengan IOS diatas versi duabelas (12) seperti *router* Cisco 881, 1905, 2851, 3725, 7200 dan sebagainya. Apabila, IOS dibawah versi tersebut maka, harus di *upgrade* terlebih dahulu. Berikut ini langkah-langkah meng- *upgrade* module:

- Buka CLI pada *router*.
- Masukan konfigurasi seperti berikut:

R1_HUB#configuration terminal R1_HUB(config)# license boot module c2900 technology-package securityk9 ACCEPT? [yes/no]: yes R1_HUB (config)# do copy run start Destination filename [startup-config]? Building configuration... [OK] R1_HUB # Reload ***!untuk me-restart router***

Tabel 4. Upgrade module

4.2.2. Konfigurasi *IP address* sesuai topologi

Setelah mendapatkan *router* dan IOS yang sesuai dan sudah diubah *hostname*-nya maka langkah selanjutnya adalah memberikan *IP address* setiap port sesuai dengan topologi yang ada.

Router#configure terminal Router(config)#hostname R1_HUB ***!Untuk menggubah hostname*** R1_HUB(config)#int FastEthernet 0/0 ***!masuk kedalam interface Fa0/0*** R1_HUB(config-if)#ip address 202.1.1.2 255.255.255.252

R1_HUB(config-if)#speed 100
R1_HUB(config-if)#duplex full
R1_HUB(config-if)#no shutdown ***!untuk mengaktifkan interface fa0/0***
R1_HUB(config)#interface loopback0 ***!mengaktifkan interface Loopback 0***
R1_HUB(config-if)#ip address 192.168.1.1 255.255.255.0
R1_HUB(config-if)#no shutdown
R1_HUB(config-if)#exit
R1_HUB(config)#crypto isakmp policy 1 ***!DMVPN Phase 1***
R1_HUB(config-isakmp)#authentication pre-share
R1_HUB(config-isakmp)#exit
R1_HUB(config)#crypto isakmp key Ckd123! address 0.0.0.0 ***!harus sama antara hub dan spoke***

R1_HUB(config)#crypto ipsec transform-set TSET esp-des esp-md5-hmac
!DMVPN phase 2

R1_HUB(cfg-crypto-trans)#mode tunnel

R1_HUB(cfg-crypto-trans)#exit

R1_HUB(config)#crypto ipsec profile VPNPROF

R1_HUB(ipsec-profile)#set transform-set TSET

R1_HUB(ipsec-profile)#exit

R1_HUB(config)#interface Tunnel 0 ***!mengkatifkan interface tunnel 0***

R1_HUB(config-if)#ip address 10.10.10.1 255.255.255.0

R1_HUB(config-if)#no ip next-hop-self eigrp 1 ***!agar router tidak menjadi next hop***

R1_HUB(config-if)#ip nhrp map multicast dynamic

R1_HUB(config-if)#ip nhrp network-id 1 ***!harus sama antara hub dan spoke***

R1_HUB(config-if)#no ip split-horizon eigrp 1

R1_HUB(config-if)#tunnel source FastEthernet0/0

R1_HUB(config-if)#tunnel mode gre multipoint

R1_HUB(config-if)#tunnel key 7777 ***!harus sama antara hub dan spoke***

Tabel 5. Konfigurasi R1_HUB

Pada konfigurasi R1_HUB, terdapat inputan *crypto isakmp policy 1* Ini adalah proses input untuk mengaktifkan DMVPN fase pertama. Angka 1 setelah *policy* dapat diubah dengan angka berapa saja tapi perlu diingat angka ini menjadi titik acuan untuk mengkonfigurasi di *router* lainnya. Hal yang perlu diperhatikan selanjutnya adalah *ip nhrp network-id* 1, nhrp harus sama antara semua perangkat router. Nhrp adalah Next-Hop Resolution Protocol. crypto isakmp key Ckd123! address 0.0.0.0 , key ini adalah *password* enkripsi, sehingga perangkat dapat mengenkripsi dan dekripsi pesan dengan *password* yang telah ditentukan.

```
Router#configure terminal
Router(config)#hostname ISP
ISP(config)#interface fastEthernet 0/0
ISP(config-if)#ip address 202.1.1.1 255.255.255.252
ISP(config-if)#speed 100
ISP(config-if)#duplex full
ISP(config-if)#no shutdown
ISP(config)#interface fastEthernet 1/0
ISP(config-if)#ip address 202.1.2.1 255.255.255.252
ISP(config-if)#speed 100
ISP(config-if)#duplex full
ISP(config-if)#no shutdown
ISP(config)#interface fastEthernet 2/0
ISP(config-if)#ip address 202.1.3.1 255.255.255.252
ISP(config-if)#speed 100
ISP(config-if)#duplex full
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP#write
```

Tabel 6. Konfigurasi ISP


```
Router#configure terminal
Router(config)#hostname R2_SPOKE
R2_SPOKE(config)#interface fastEthernet 0/0
R2_SPOKE(config-if)#ip address 202.1.2.2 255.255.255.252
R2_SPOKE(config-if)#speed 100
R2_SPOKE(config-if)#duplex full
R2_SPOKE(config-if)#no shutdown
R2_SPOKE(config)#crypto isakmp policy 1
R2_SPOKE(config-isakmp)#authentication pre-share
R2_SPOKE(config-isakmp)#exit
R2_SPOKE(config)#crypto isakmp key Ckd123! address 0.0.0.0
```

```
R2_SPOKE(config)#crypto ipsec transform-set TSET esp-des esp-md5-
hmac
R2_SPOKE(cfg-crypto-trans)#mode tunnel
R2_SPOKE(cfg-crypto-trans)#exit
R2_SPOKE(config)#crypto ipsec profile VPNPROF
R2_SPOKE(ipsec-profile)#set transform-set TSET
R2_SPOKE(ipsec-profile)#exit
R2_SPOKE(config)#interface Tunnel 0
R2_SPOKE(config-if)#ip address 10.10.10.2 255.255.255.0
R2_SPOKE(config-if)#ip nhrp map 10.10.10.1 201.1.1.1
R2_SPOKE(config-if)#ip nhrp map multicast 201.1.1.1
R2_SPOKE(config-if)#ip nhrp network-id 1
R2_SPOKE(config-if)#ip nhrp nhs 10.10.10.1
R2_SPOKE(config-if)#tunnel source FastEthernet0/0
R2_SPOKE(config-if)#tunnel mode gre multipoint
R2_SPOKE(config-if)#tunnel key 7777
R2_SPOKE(config-if)#tunnel protection ipsec profile VPNPROF
R2_SPOKE(config)#router eigrp 1
R2_SPOKE(config-router)#network 192.168.2.0
R2_SPOKE(config-router)#network 10.0.0.0
R2_SPOKE(config-router)#exit
R2_SPOKE(config)#ip route 0.0.0.0 0.0.0.0 202.1.1.5
R2_SPOKE(config)#exit
R2_SPOKE#write
```

Tabel 7. Konfigurasi R2_SPOKE

```
Router#configure terminal
Router(config)#hostname R3_SPOKE
R3_SPOKE(config)#interface fastEthernet 0/0
R3_SPOKE(config-if)#ip address 202.1.3.2 255.255.255.252
R3_SPOKE(config-if)#speed 100
R3_SPOKE(config-if)#duplex full
R3_SPOKE(config-if)#no shutdown
R3_SPOKE(config)#crypto isakmp policy 1
R3_SPOKE(config-isakmp)#authentication pre-share
R3_SPOKE(config-isakmp)#exit
R3_SPOKE(config)#crypto isakmp key Ckd123! address 0.0.0.0
R3_SPOKE(config)#crypto ipsec transform-set TSET esp-des esp-md5-
hmac
R3_SPOKE(cfg-crypto-trans)#mode tunnel
R3_SPOKE(cfg-crypto-trans)#exit
R3_SPOKE(config)#crypto ipsec profile VPNPROF
R3_SPOKE(config-profile)#set transform-set TSET
R3_SPOKE(config-profile)#exit
```

```
R3_SPOKE(config)#interface Tunnel 0
_SPOKE(config-if)#ip address 10.10.10.3 255.255.255.0
R3_SPOKE(config-if)#ip nhrp map 10.10.10.1 202.1.1.1
R3_SPOKE(config-if)#ip nhrp map multicast 202.1.1.1
R3_SPOKE(config-if)#ip nhrp network-id 1
R3_SPOKE(config-if)#ip nhrp nhs 10.10.10.1
R3_SPOKE(config-if)#tunnel source FastEthernet0/0
R3_SPOKE(config-if)#tunnel mode gre multipoint
R3_SPOKE(config-if)#tunnel key 7777
R3_SPOKE(config-if)#tunnel protection ipsec profile VPNPROF
R3_SPOKE(config)#router eigrp 1
R3_SPOKE(config-router)#network 10.0.0.0
R3_SPOKE(config-router)#network 192.168.3.0
R3_SPOKE(config-router)#exit
R3_SPOKE(config)#ip route 0.0.0.0 0.0.0.0 202.1.1.9
R3_SPOKE(config)#exit
R3_SPOKE#write
```

Tabel 8. Konfigurasi R3_SPOKE

4.3. Verifikasi Hasil

Verifikasi hasil merupakan proses pengecekan konfigurasi yang telah kita masukkan, verifikasi tersebut berupa *show command* terkait dan dengan melakukan *test ping, traceroute* dan *debug.* Tujuan verifikasi hasil ini adalah untuk mengetahui apakah konfigurasi yang kita lakukan sudah berhasil seperti rencana semula atau belum. Berikut ini adalah hasil verifikasi DMVPN dari R1_HUB, ISP, R2_SPOKE, R3_SPOKE.

4.3.1. Verifikasi Hasil *R1_HUB*

R1_HUB#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete

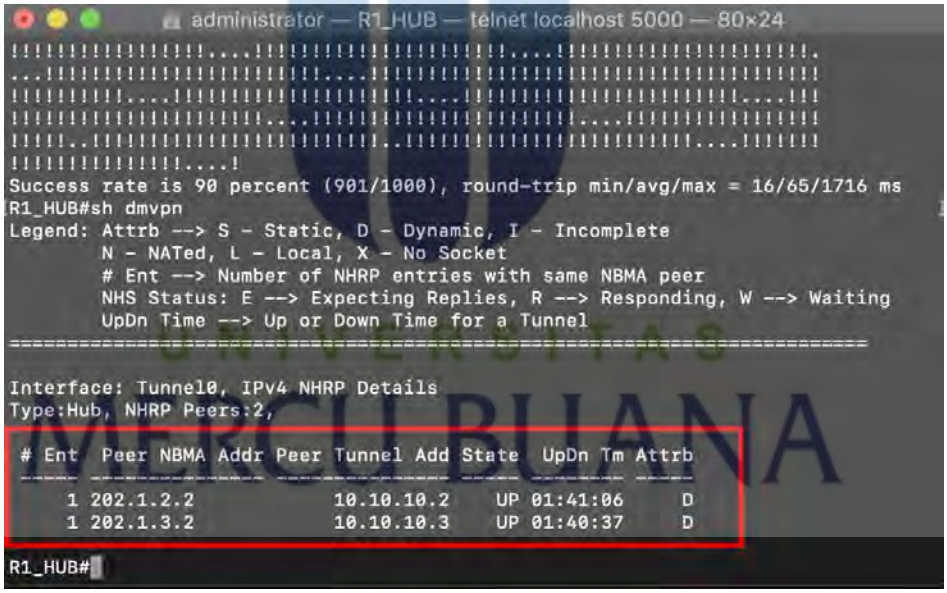
N - NATed, L - Local, X - No Socket

Ent --> Number of NHRP entries with same NBMA peer

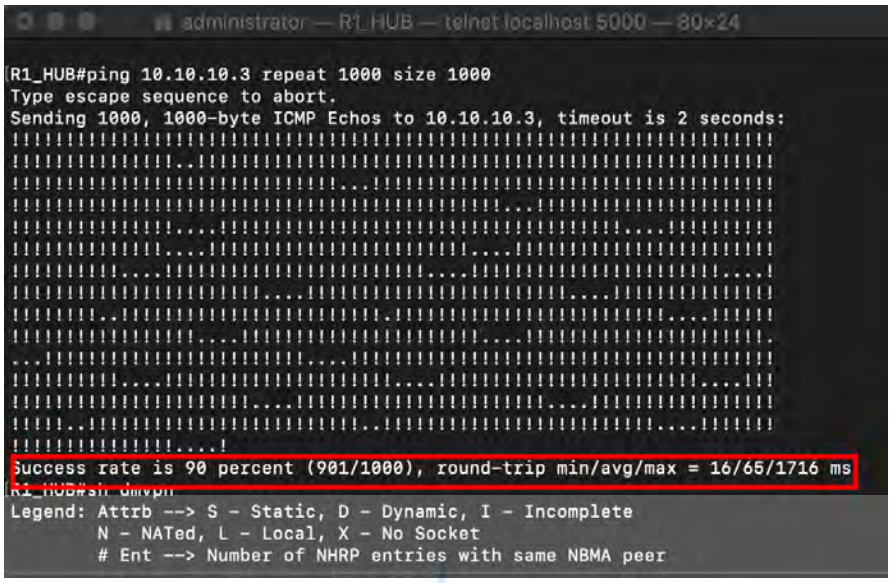
Tunnel0, Type:Hub, NHRP Peers:2,

# Ent	Peer NBMA Addr	Peer Tunnel Add	State	UpDn Tm	Attrb
1	202.1.1.6	10.10.10.2	UP	never	D
1	202.1.1.10	10.10.10.3	UP	never	D

Tabel 9. Hasil test R1_HUB

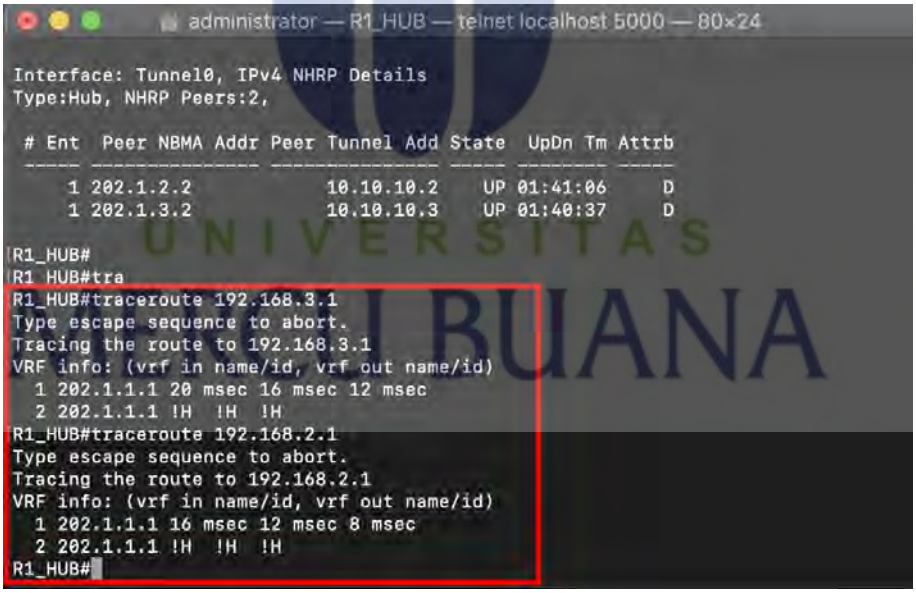


Gambar 10. *Show* dmvpn R1_HUB



Gambar 11. Hasil ping menuju R3_SPOKE

Pada gambar 4.4. adalah hasil *ping* sebanyak 1000 kali dengan bobot *package* 1000, tingkat keberhasilannya adalah 90%.



Gambar 12. Hasil traceroute ke kedua SPOKE

Pada gambar diatas menjelaskan mengeenai next-hop atau jalur yang dilalui oleh paket dari *router source* menuju *network destination*

4.3.2. Verifikasi Hasil *R2_SPOKE*

R2_SPOKE#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete

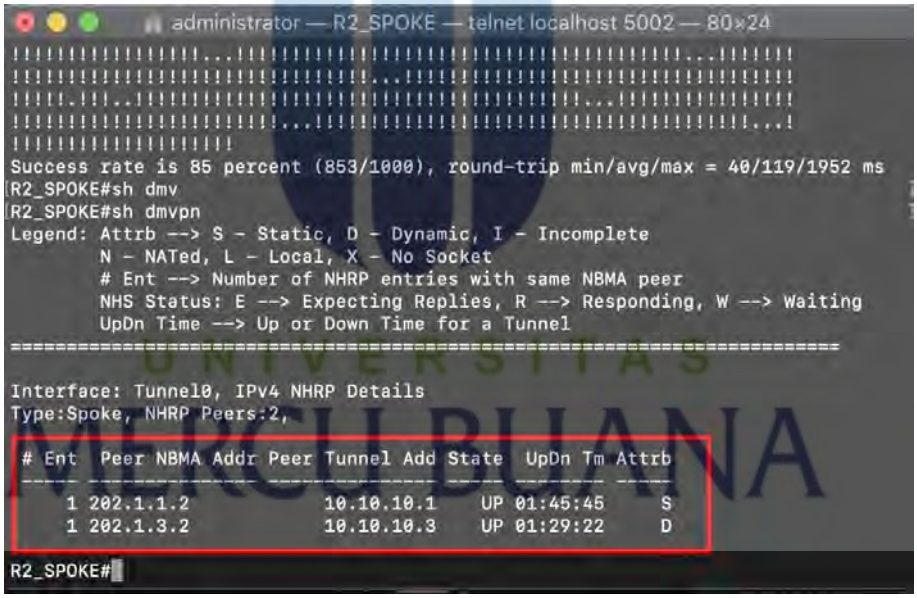
N - NATed, L - Local, X - No Socket

Ent --> Number of NHRP entries with same NBMA peer

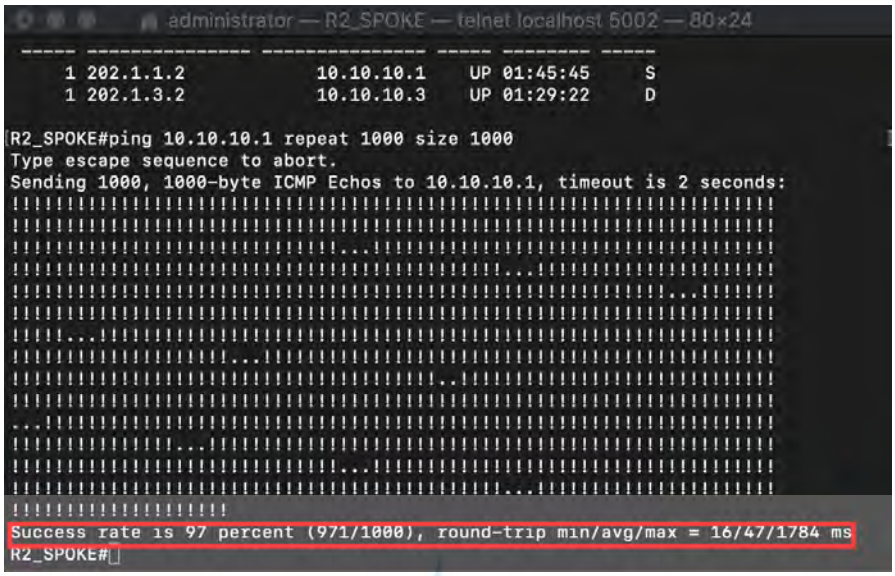
Tunnel0, Type:Spoke, NHRP Peers:1,

# Ent	Peer NBMA Addr	Peer Tunnel Add	State	UpDn Tm	Attrb
1	202.1.1.1	10.10.10.1	UP	00:03:11	S

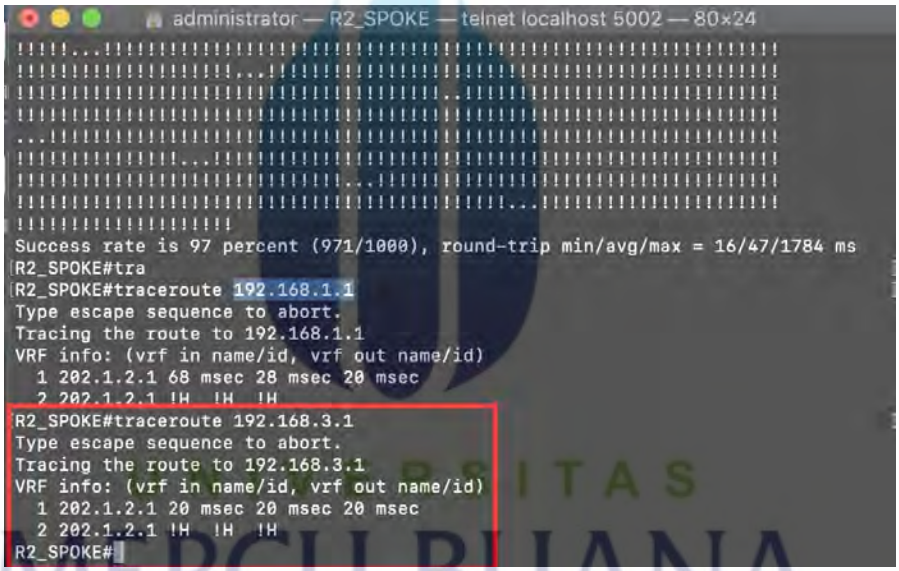
Tabel 10. Hasil test R2_SPOKE



Gambar 13. Show dmvpn pada R2_SPOKE



Gambar 14. Hasil ping menuju R1_HUB



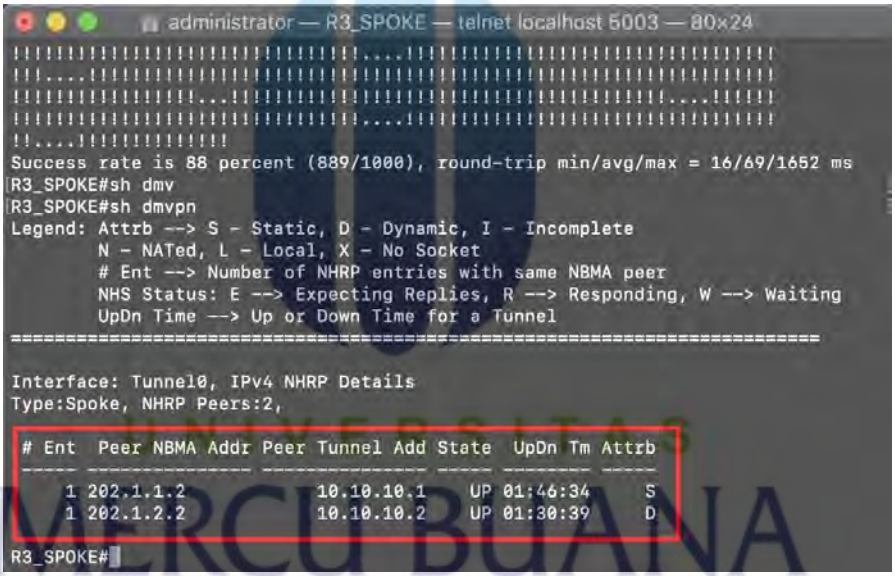
Gambar 15. Hasil traceroute menuju R1 dan R3

4.3.3. Verifikasi Hasil *R3_SPOKE*

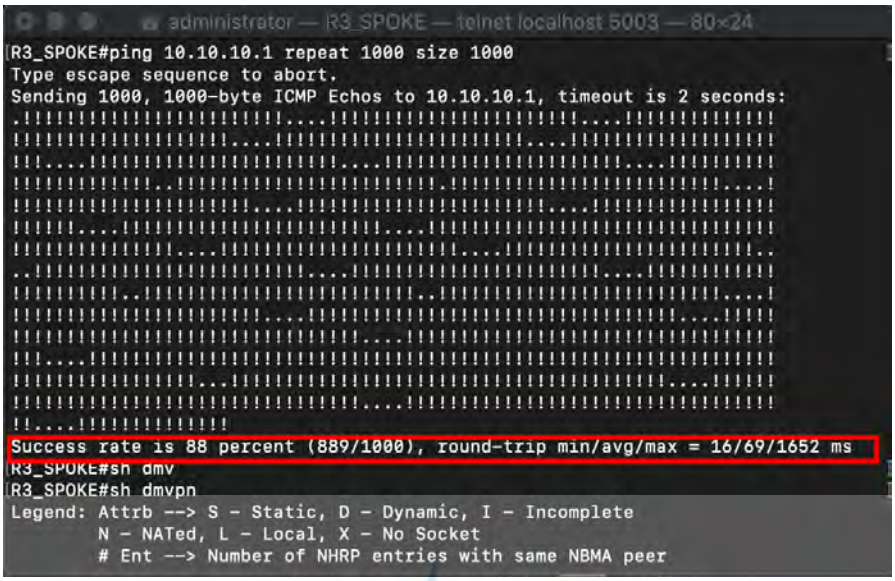
```
R3_SPOKE#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel0, Type:Spoke, NHRP Peers:1,
 # Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1       202.1.1.1       10.10.10.1    UP 00:03:41 S
```

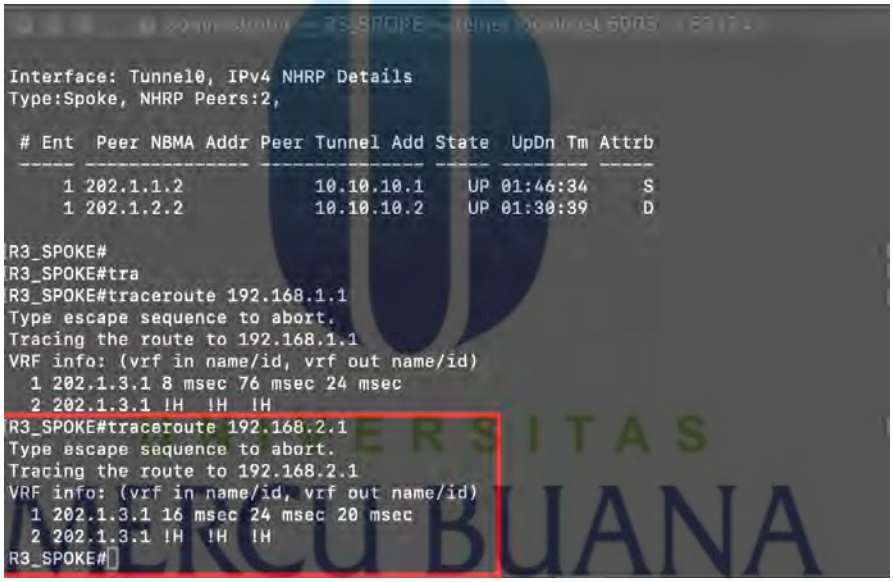
Tabel 11. Hasil test R3_SPOKE



Gambar 16. Show dmvpn pada R3_SPOKE



Gambar 17. Hasil ping menuju R1_HUB



Gambar 18. Hasil traceroute menuju R1 dan R2

Seperti yang kita lihat pada tabel R1_HUB, R2_SPOKE dan R3_SPOKE bahwa status DMVPN sudah UP. Pada ketiga *router* tersebut *Peer NBMA* menunjukkan *IP Public* dari setiap *router* dan *Peer Tunnel* adalah *IP Private* yang dimiliki oleh setiap router. Jadi konsepnya adalah sebelum melalui *IP Private* setiap *router* akan menanyakan *IP Public*-nya kepada HUB. Pada HUB ia akan menyimpan *data routing*

secara dinamis kita bisa mengetahuinya dari *Attrb*, hub akan menyimpan semua *IP Private* dan *IP Public* dari setiap spoke, sedangkan pada spoke kita hanya mengetahui *IP Private* dan *IP Public* dari hub.

4.4. Pengujian

Pada bagian ini, menjelaskan mengenai konfigurasi DMVPN. Pengujian ini menghasilkan *ping, jitter, package loss*, dan *next-hope* yang dilalui oleh paket data.

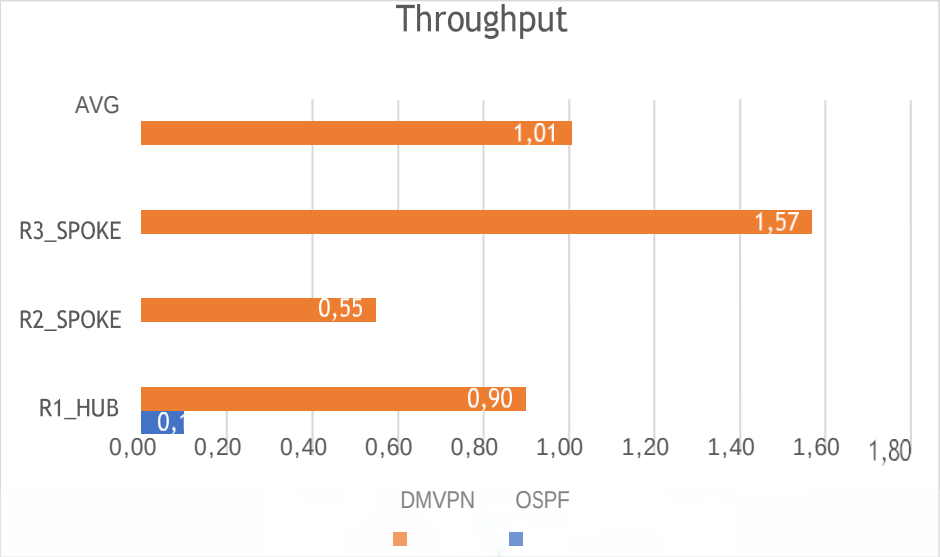
4.4.1. Hasil *Throughput*

Hasil *throughput* menunjukan kecepatan data di transfer sesungguhnya. Throughput adalah jumlah total kedatangan packet yang berhasil diamati pada tujuan selama interval tertentu.

Gambar 19. Throughput dari R1 to ISP

Gambar 20. Throughput dari R2 to ISP

Gambar 21. Throughput dari R3 to ISP

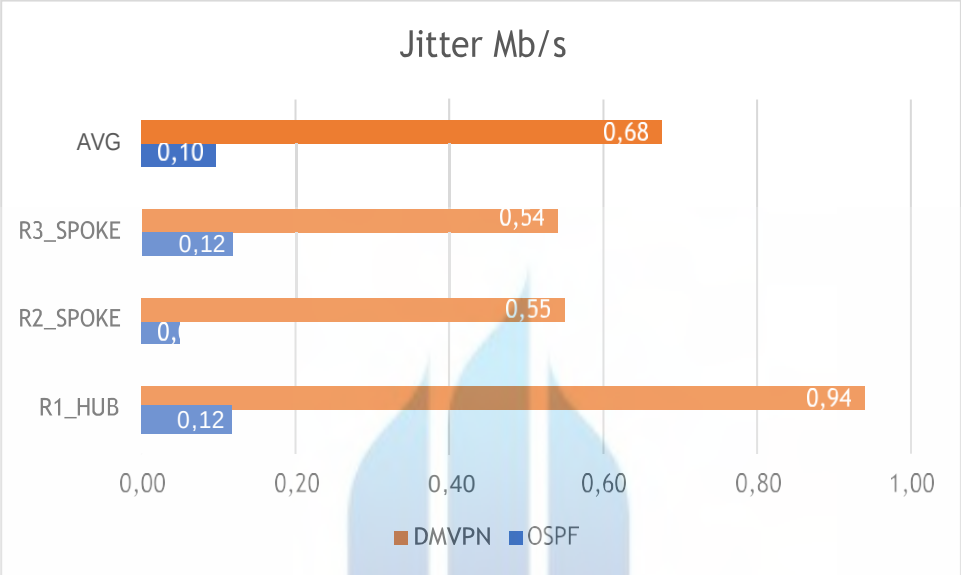


Gambar 22. Perbandingan hasil throughput.

Dari percobaan diatas, dapat disimpulkan bahwa penggunaan DMVPN lebih effiesien dalam proses transfer data. *Throughput* DMVPN secara rata-rata memiliki kecepatan 1,01Mbps sedangkan OSPF memiliki kecepatan rata-rata 0,26Mbps. DMVPN lebih cepat dan effiesien sekitar 74.17%.

4.4.2. Hasil *Jitter*

Jitter dapat didefinisikan sebagai variasi-variasi *delay* antar *block-block* yang berutan. Besarnya nilai jitter sanga berpengaruh oleh variasi-variasi beban trafik dan besarnya tumpukan antar *packet*.



Gambar 23. Perbandingan hasil jitter

Pada data diatas, *jitter* pada DMVPN lebih besar dibanding OSPF dengan perbedaan rata-rata 0,68Mbps.

BAGIAN 5 KESIMPULAN DAN SARAN

Bagian penutup berisi tentang kesimpulan-kesimpulan dari seluruh bagian yang telah dibahas. Pada bagian ini penulis juga berkesempatan menyampaikan saran-saran ataupun masukan dengan harapan dapat diterima dengan baik oleh semua pihak demi kemajuan bersama dimasa yang akan datang.

5.1. Kesimpulan

DMVPN merupakan sebuah solusi untuk perusahaan besar yang memiliki kantor cabang yang cukup banyak dan terlebih terletak di luar kota, pulau atau benua. *DMVPN* memiliki keunggulan dibanding *VPN* biasa yaitu dari fitur dimana *DMVPN* lebih mudah dalam mengkonfigurasi dan apabila ada *site* tambahan maka tidak perlu di konfigurasi dari ulang sehingga dapat mengefisiensikan waktu dan tenaga.

Routing adalah proses bagaimana *router* melewatkan paket ke jaringan yang dituju. *Routing protocol* adalah komunikasi yang digunakan antar *router-router*. *Routing protokol* mengijinkan satu *router* untuk sharing informasi dengan router- router lain berdasarkan jaringan yang diketahui dan jalur terbaik ke jaringan tersebut. Setiap router dalam *routing* protokol yang sama membangun tabel routingnya, berdasarkan informasi dari *router* tetangga untuk sharing informasi antar *router*.

EIGRP merupakan pengembangan dari *IGRP*. *EIGRP* merupakan *dynamic routing* yang di kembangkan oleh Cisco, dan *EIGRP* hanya dapat berjalan pada Cisco *devices.* Kelebihan utama yang membedakan *EIGRP* dari protokol routing lainnya adalah EIGRP termasuk satu-satunya protokol routing yang menawarkan fitur *backup route*, dimana jika terjadi perubahan pada *network*, *EIGRP* tidak harus melakukan kalkulasi ulang untukmenentukan rute terbaik karena bisa langsung menggunakan *backup route*. Kalkulasi ulang *route* terbaik dilakukan jika *backup route* juga mengalami kegagalan.

IPSecurity adalah sebuah teknologi untuk melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik tunneling untuk mengirimkan informasi melalui jaringan Internet atau dalam jaringan intranet secara aman.

Singkatnya, Konfigurasi *DMVPN* Menggunakan *IPSec* dan *Routing EIGRP* pada PT. Cahaya Kreatif Digital membuat kinerja *network engineer* menjadi lebih efisien. Dengan investasi dibidang keamanan jaringan, PT. Cahaya Kreatif Digital dapat menekan *cost* kemungkinan kerugian atas hilangnya data maupun kerugian waktu karena *network engineer* harus men-*troubleshoot* jaringan dengan *effort* lebih.

5.2. Saran

Penelitian ini dapat berkembang dimasa yang akan datang. Sehingga, penulis mengharapkan umpan balik dari pembaca untuk mengembangkan atau memodifikasi tulisan atau konfigurasi yang terdapat dalam tulisan ini sesuai dengan kebutuhan pembaca atau kebutuhan perusahaan.

DAFTAR PUSTAKA

[1] M. T. Kurniawan, *Buku Jaringan Komputer I.* .

[2] S. Jose, “Dynamic Multipoint VPN Configuration Guide , Cisco IOS XE Release 3S,” no. 6387, 2014.

[3] Cisco, “Cisco Express Forwarding,” *Architecture*, pp. 1–8, 2002, [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c/xcfcef.ht ml.

[4] R. Arlan, R. Munadi, and N. Andini, “Implementasi Dan Analisis Sistem Keamanan Ip Security (Ipsec) Di Dalam Multi Protocol Label Switching-Virtual Private Network (Mpls- Vpn) Pada Layanan Berbasis Ip Multimedia Subsystem (Ims),” *J. Chem. Inf. Model.*, vol. 3, no. 9, p. 4630, 2016, doi: 10.1017/CBO9781107415324.004.

[5] P.-C. Cheng, J. A. Garay, A. Herzberg, and H. Krawczyk, “Security architecture for the internet protocol,” *Comput. Stand. Interfaces*, vol. 20, no. 6–7, p. 409, 1999, doi: 10.1016/s0920-5489(99)90778-x.

[6] S. M. Janosik, “IP Authentication Header,” *NASPA J.*, vol. 42, no. 4, p. 1, 2005, doi: 10.1017/CBO9781107415324.004.

[7] F. F. Information, “Encrypted Preshared Key Restrictions for Encrypted Preshared Key Information About Encrypted Preshared Key Using the Encrypted Preshared Key Feature to Securely Store Passwords,” vol. 6, pp. 1–15, 2011.

[8] I. Warman and A. Hanafi, “Analisa Perbandingan Kinerja Generic Routing Encapsulation (GRE) Tunnel Dengan Point to Point Protocol over Ethernet (PPPoE) Tunnel Mikrotik Routeros,” *Teknoif*, vol. 7, no. 1, pp. 58–66, 2019.

[9] S. M. Janosik, “Generic Routing Encapsulation (GRE),” *NASPA J.*, vol. 42, no. 4, p. 1, 2005, doi: 10.1017/CBO9781107415324.004.

[10] A. Headquarters, “Segment Routing Configuration Guide , Cisco IOS XE Gibraltar 16 . 11 . x,” no. 6387.