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*.

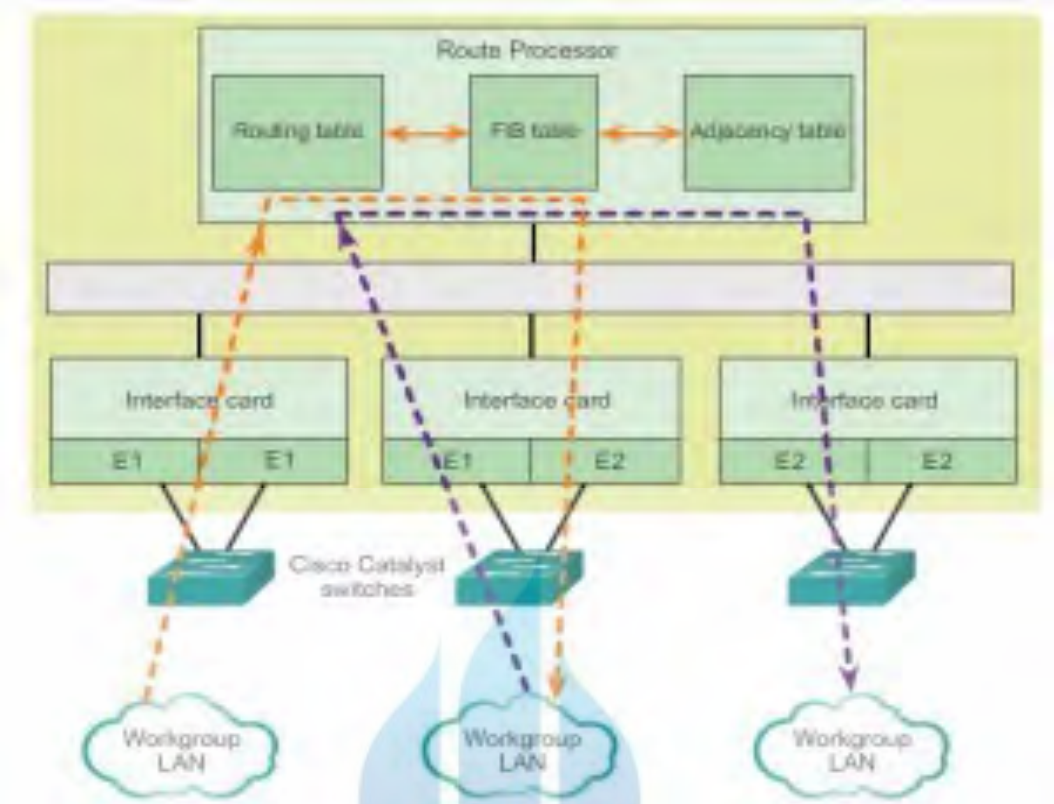
Fitur ini menghilangkan kebutuhan akan konfigurasi *spoke-to-spoke* untuk saluran langsung. Ketika *router spoke* ingin mengirimkan paket ke *router spoke* lain, *router* tersebut sekarang dapat menggunakan *NHRP* untuk secara dinamis menentukan alamat tujuan yang diperlukan dari *router spoke* target. (*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*

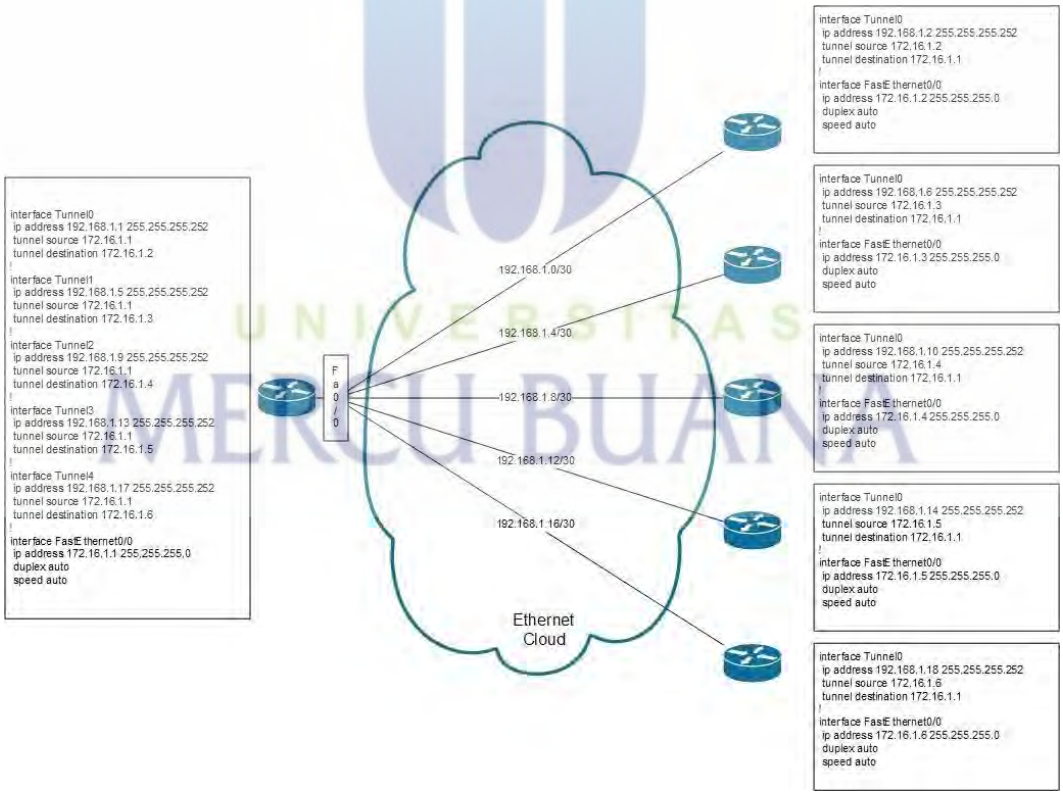
P2P merupakan singkatan dari *peer-to-peer* atau teknologi dari “ujung” ke “ujung” pertama kali di luncurkan dan dipopulerkan oleh aplikasi-aplikasi “berbagi-berkas” (*file sharing*) seperti Napster dan KaZaA. Pada konteks ini teknologi *P2P* memungkinkan para pengguna untuk berbagi, mencari dan mengunduh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



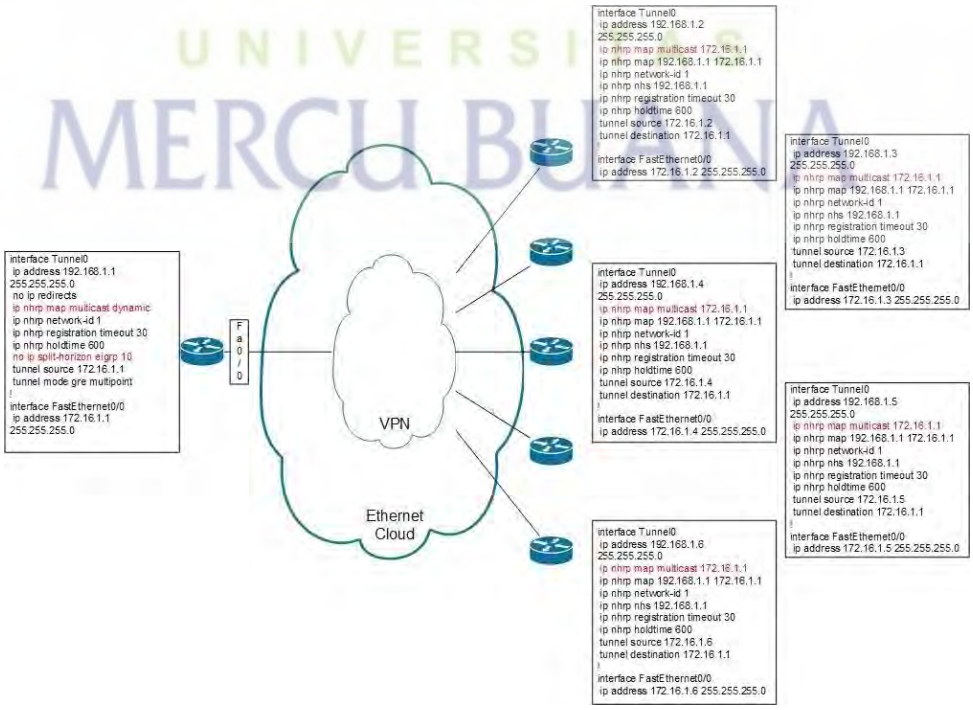
Gambar 5. Contoh P2P GRE

- *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.