BAB II
DASAR TEORI

2.1 Kajian Pustaka

Penelitian oleh Gebere Akele Tizazu, Abraham Belay Berhe dan Ki-Hyung Kim pada tahun 2017 mengenai DMVPN yang memanfaatkan dua buah *router* sebagai pusat komunikasi dengan menerapkan *routing protocol* EIGRP, OSPF, RIP. Parameter-parameter uji dalam penelitian tersebut mencakup *time convergence, link utilization,* dan *end-to-end delay.* Dikemukakan bahwa baik penggunaan OSPF maupun EIGRP paling cocok untuk digunakan pada DMVPN yang berskala besar karena kecepatan waktu konvergensi dan *link utilization* menghasilkan parameter bagus selama kapasitas CPU yang digunakan pada *router* cabang cukup baik, akan tetapi peneliti tersebut lebih menyarankan untuk menggunakan OSPF dikarenakan sifatnya *open standard* sehingga bisa diterapkan pada perangkat jaringan manapun[4].

Penelitian oleh Michelle Claudia dan Muhammad Rifqi pada tahun 2021 mengenai perbandingan performansi pada *router spoke* DMVPN saat menggunakan protokol *Hot Standby Router Protocol* (HSRP) dan *Gateway Load Balancing Protocol* (GLBP). Parameter-parameter yang diujikan pada penelitian tersebut meliputi *throughput, delay, waktu transfer,* dan *down time.* Penelitian tersebut memberikan solusi untuk redundansi pada *router spoke* untuk meningkatkan ketersediaan pada jaringan. Hasil yang didapatkan pada *throughput, delay, waktu transfer,* dan *down time* pada protokol HSRP lebih baik daripada protokol GLBP[5].

Penelitian oleh Nanda Iryani dan Dyas Dendi Andika pada tahun 2021 mengenai unjuk kerja DMVPN ketika menggunakan *router* berbasis *open source* dengan mensimulasikan sebuah DMVPN pada perangkat *open source router Free Range Routing* yang dijalankan dengan routing BGP. Parameter parameter yang dihasilkan dalam penelitian tersebut mengungkapkan apabila nilai *throughput, jitter,* dan *packet loss* jika merujuk kedalam kategori *tiphon etsi* terbilang sangat baik. Penelitian tersebut memaparkan bila secara fungsionalitas dan performansi

dari *open source router* tidak kalah dengan *router-router* konvensional seperti cisco, mikrotik, juniper atau yang lain[6].

Penelitian oleh Siti Ummi Masruroh, Khairul Hamdi Putra Widya, Andrew Fiade, Imelda Ristanti Julia pada tahun 2018 membahas mengenai evaluasi performansi DMVPN *phase* 1, 2 dan *phase* 3 menggunakan *routing protocol* RIP, OPSF, dan EIGRP dengan aspek pengujiannya berupa *throughput, jitter* dan *packet loss*. Hasil yang didapatkan adalah untuk *throughput, jitter* dan *packet loss*, DMVPN *Phase 2* lebih baik dibandingkan dengan phase 1 dan 3. Akan tetapi dari penelitian tersebut DMVPN *phase 3* mempunyai skalabilitas lebih baik dibandingkan kedua *phase* lainnya[7].

Penelitian Oleh Towhidul Alam, dkk pada tahun 2018 mengenai penerapan DMVPN bersamaan *service* jaringan lain, dalam penelitian tersebut mencoba mengimplementasi jaringan DMVPN dengan *service* lain yang biasa ditemukan pada perangkat *router* yaitu HSRP *(Hot StandBy Routing Protocol)*. Implementasi yang dilakukan yaitu menjalankan dua buah *router* yang dijadikan sebagai pusat dari komunikasi DMVPN, DMVPN yang dikombinasikan dengan HSRP tersebut dijalankan dengan routing EIGRP. Skema pengujian yang dilakukan dalam penelitian tersebut berupaya mencari nilai *throughput*, *time response* dan *measure times* pada *services* FTP (*File Transfer Protocol)* dan *WWW (World Wide Web).* Pengujian tersebut didapatkan dengan dua jenis skenario berbeda, skenario pertama ketika semua perangkat dalam jaringan hidup, dan skenario kedua ketika salah satu komponen pusat dalam DMVPN dimatikan. Hasilnya dipaparkan bahwa secara keseluruhan nilai parameter-parameter uji yang dihasilkan DMVPN dari dua skenario yang ada menghasilkan nilai parameter-parameter yang sangat baik dengan *thoughput* dan *measure time* terbaik dihasilkan ketika menggunakan skenario pertama, sedangkan pada *time response* keduanya sama baiknya. Penelitian tersebut mengatakan bahwa kedepannya DMVPN yang diterapkan dengan protokol lain (HSRP) akan lebih sering diimplementasikan[8].

Penelitian oleh N. Angelescu, D.C. Puchianu, G. Predusca, L.D. Circiumarescu, dan G. Movila pada tahun 2017 mengkaji secara umum performa DMVPN yang berjalan pada *software Network Simulator* GNS3. Peneliti

mengungkapkan jika dengan penggunaan DMVPN pada suatu jaringan dapat mengurangi jumlah *hop count* yang fungsinya untuk mengurangi *transit delay*[9].

Pada tabel 2.1 menunjukkan perbandingan tinjauan pustaka terhadap penelitian sebelumnya yang terkait dalam penelitian penulis.

Tabel 2.1 Perbandingan dengan Penelitian Sebelumnya

Peneliti	Judul	Komponen Penelitian				
		Konfigurasi DMVPN	Parameter Pengujian	Jenis *Router*	Protokol *routing*	Kesamaan
Gebere Akele Tizazu, dkk	*Dynamic Routing Influence on Secure Enterprise Network Based on* DMVPN	*Dual hub dual cloud*	Waktu konvergensi, *link utilization*, *delay*	Cisco	OSPF & EIGRP	menggunakan *dual hub*
Michelle Claudia, Muhammad Rifqi	Analisa Perbandingan Performansi *Hot Standby Router Protocol* (HSRP) dengan *Gateway Load Balancing Protocol* (GLBP) Pada *Router Spoke* DMVPN	Redundansi pada *router spoke*	*throughput*, *delay*, waktu transfer, *down time*	Cisco		Redundansi / *high availability* & *load balancing*
Nanda Iryani, Dyas Dendi	Analisis Performansi *Dynamic Multipoint Virtual Private Network* pada *Routing Protocol* BGP dengan FRRouting	menggunakan *router open source*	*throughput, delay, jitter, packet loss*	*Free Range Routing*	BGP	*router open source*
Siti Ummi Masruroh, dkk	*Performance Evaluation* DMVPN *Using Routing Protocol* RIP, OSPF, *And* EIGRP	DMVPN *Phase* 1, 2, 3	*throughput, jitter, packet loss*	Cisco	RIP, OSFP, EIGRP	menggunakan *phase* 3
Towhidul Alam, dkk	*Design and Implementation of a Secured Enterprise Network using Dynamic Multipoint* VPN *with* HSRP *Protocol*	*Dual hub* menggunakan protokol HSRP	*Throughput, response time, measure time*	Cisco	EIGRP	menggunakan *dual hub*
N. Angelescu, dkk	DMVPN *simulation in* GNS3 *network simulation software*	DMVPN *Phase* 2	*Delay* & jumlah hop	Cisco	-	DMVPN secara umum
Anandya Saifurrahman	Analisis Performansi *Dynamic Multipoint Virtual Private Network Dual Hub Single Cloud* Berbasis *Load Balancing Fail Over* Dengan *Open-Source Router* VyOS	DMVPN *Dual Hub Single Cloud*	*Throughput, delay, jitter* dan *packet loss*	VyOS	OSPF	

Dari tabel perbandingan dengan penelitian sebelumnya, pembeda pada penelitian ini menggunakan *dual hub* yang merupakan pengembangan dari *single*

hub bertujuan untuk meningkatkan ketersediaan jaringan dan menghilangkan *single point of failure.* Penggunaan *single cloud* untuk meminimalkan infrastruktur dibandingkan dengan *dual cloud* yang membutuhkan dua jalur ISP. Apabila menggunakan dua *router hub* secara otomatis berfungsi *load balancing* karena jalur pengiriman informasi dari *client* ke *hub* terbagi menjadi dua jalur. Penggunaan *phase* 3 ini agar DMVPN menjadi lebih *scalable* dengan meringkat rute *default* dengan perintah NHRP *redirect* dan NHRP *shortcut*. Sedangkan penggunaan *routing* OSPF karena pada penelitian ini menggunakan *router open source* dari VyOS.

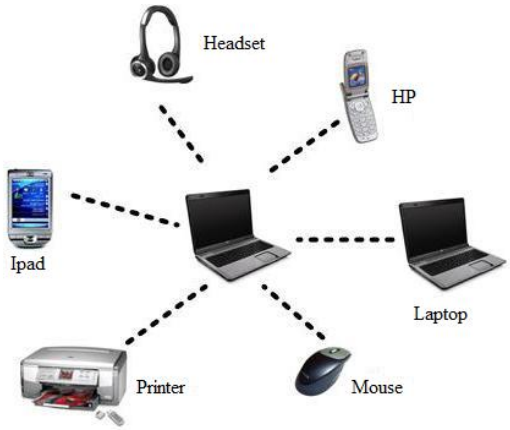
2.2 Dasar Teori

2.2.1 Jaringan Komputer

A. Jenis-Jenis Jaringan Komputer

1. *Personal Area Network* (PAN)

   Personal Area Network biasa disingkat dengan PAN, yaitu jaringan computer yang menghubungkan antara dua atau lebih perangkat yang berjarak dekat, hanya sekitar 4 sampai 6 meter. Contoh penerapan untuk jaringan PAN adalah menghubungkan komputer dengan perangkat *smartphone* seperti pada gambar 2.1 berikut ini[10].

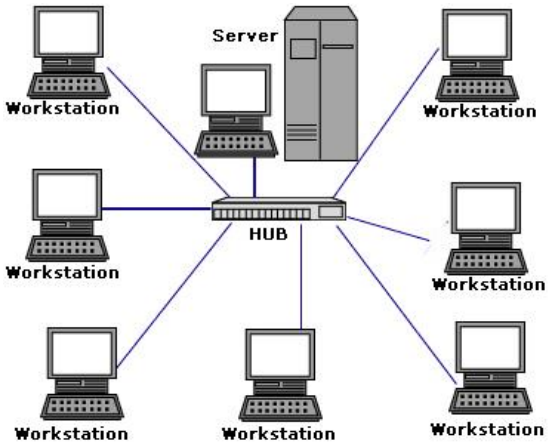


Gambar 2.1 *Personal Area Network*

2. *Local Area Network* (LAN)

   Local Area Network merupakan jaringan telekomunikasi dengan cakupan area yang kecil. LAN sering kali dijumpai di lapangan seperti sekolah, kampus, perkantoran untuk menghubungkan antar perangkat komputer dalam satu

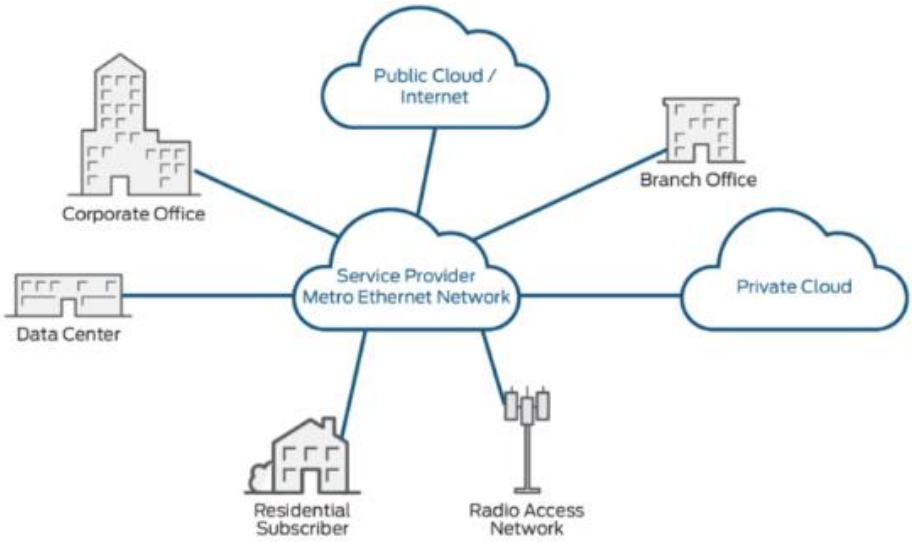
ruangan atau satu Gedung. Jenis jaringan ini sangat dipengaruhi oleh desain topologi jaringan seperti pada gambar 2.2.



Gambar 2.2 *Local Area Network*

3. Metropolitan Area Network (MAN)

Metropolitan Area Network merupakan jenis jaringan komputer dengan cakupan area yang lebih luas dibanding LAN. MAN memiliki kemampuan pengiriman data berkecepatan tinggi dan digunakan untuk menghubungkan suatu lokasi seperti sekolah, kampus atau perkantoran di dalam satu kota seperti pada ilustrasi gambar 2.3.

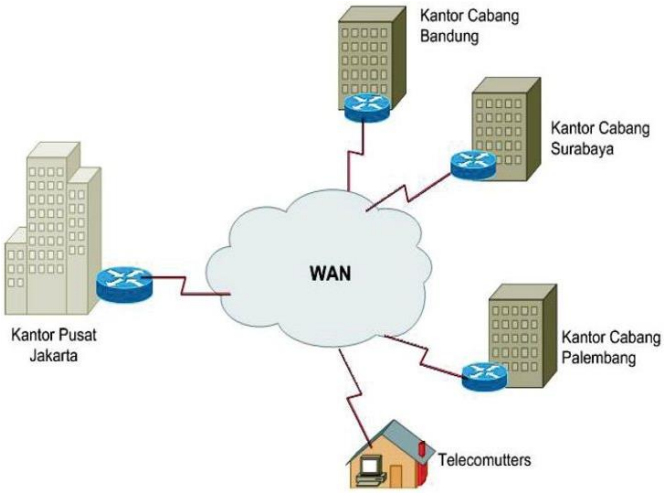


Gambar 2.3 *Metropolitan Area Network*

4. *Wide Area Network* (WAN)

Jaringan WAN merupakan jaringan komputer dengan cakupan area yang lebih besar dibandingkan dengan jaringan MAN. Implementasi jaringan WAN

yaitu menghubungkan suatu wilayah dengan wilayah lain atau suatu negara dengan negara lain[11], seperti pada gambar 2.4.

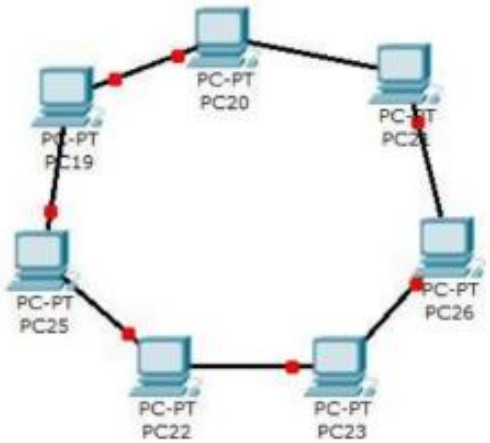


Gambar 2.4 *Metropolitan Area Network*

B. Topologi Jaringan

1. Topologi Ring

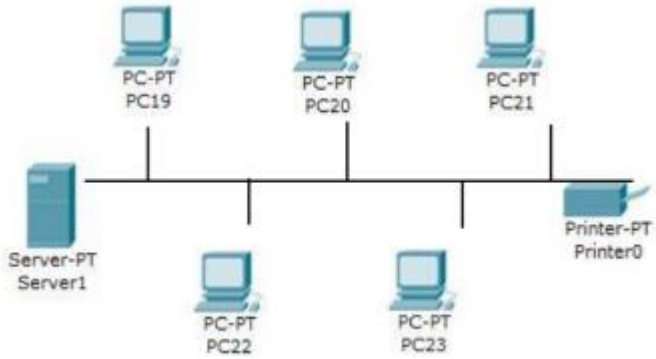
Pada topologi ring terdapat dua komputer atau lebih yang saling terhubung hingga Kembali ke komputer pertama, sehingga membentuk seperti lingkaran. Gambar 2.5 merupakan contoh ilustrasi topologi ring.



Gambar 2.5 Topologi Ring

2. Topologi Bus

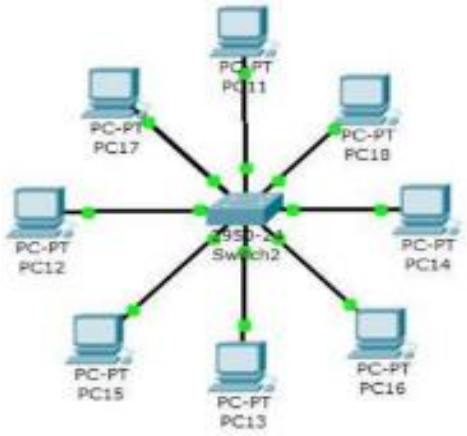
Topologi bus berbentuk seperti antrian dan menggunakan satu buah kabel *coaxial*, menghubungkan seluruh komputer menggunakan konektor BNC lalu kedua ujung pada kabel tersebut harus diakhiri oleh perangkat terminator. Gambar 2.6 merupakan contoh ilustrasi topologi bus.



Gambar 2.6 Topologi Bus

3. Topologi Star

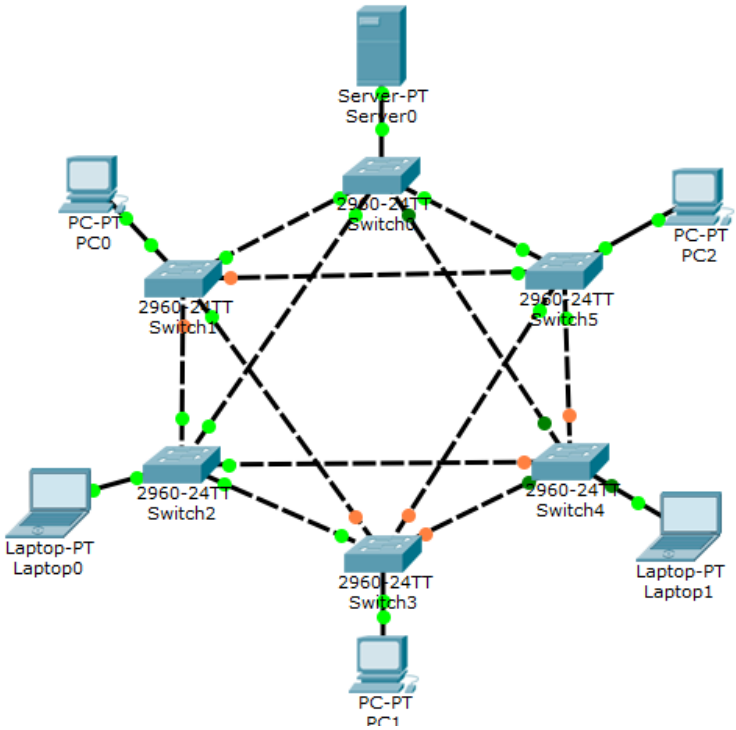
Topologi star menghubungkan seluruh komputer menggunakan *switch* melalui kabel *twisted pair*. *Switch* tersebut akan menjadi pusat dari jaringan yang berfungsi mengatur lalu lintas data. Topologi ini merupakan topologi yang cukup mudah diterapkan. Gambar 2.7 merupakan contoh ilustrasi topologi star.



Gambar 2.7 Topologi Star

4. Topologi Mesh

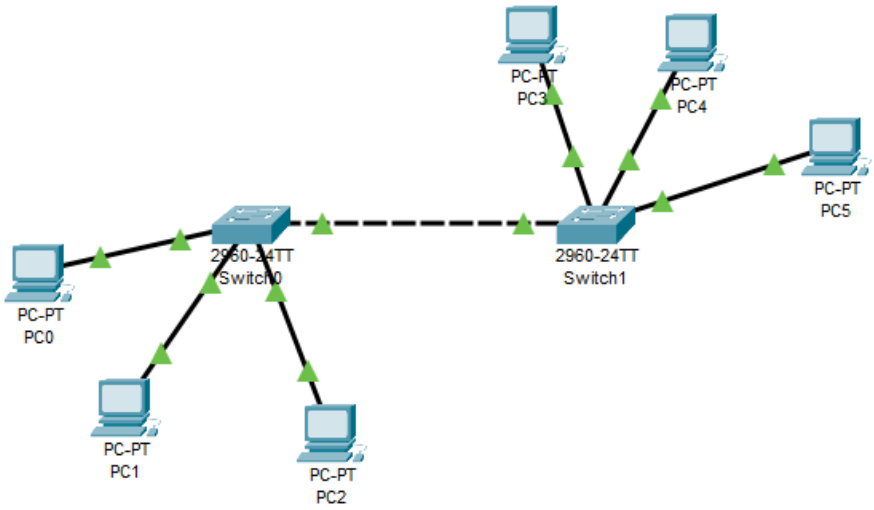
Pada topologi ini setiap komputer pada jaringan akan terhubung langsung dengan komputer lain. Pengiriman data akan langsung menuju computer tujuan tanpa melewati komputer lain. Gambar 2.8 merupakan contoh ilustrasi topologi mesh.



Gambar 2.8 Topologi Mesh

5. Topologi *Tree*

Topologi ini merupakan gabungan dari dua atau lebih topologi *star* yang dihubungkan dengan topologi bus. Biasanya pada topologi *tree* ada beberapa tingkatan jaringan, dan jaringan yang berada pada tingkat yang lebih tinggi bisa mengatur jaringan yang tingkatnya lebih rendah[12]. Gambar 2.9 merupakan contoh ilustrasi topologi *Tree*.



Gambar 2.9 Topologi *Tree*

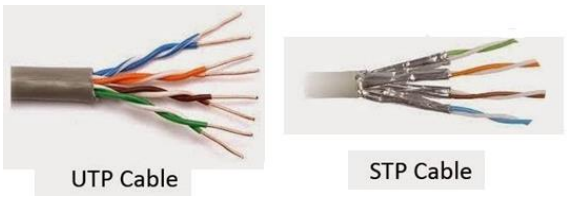
C. Media Transmisi Jaringan

1. Media Transmisi Kabel

Media transmisi kabel adalah media transmisi yang dibuat dengan wujud tertentu agar dapat mengirimkan sinyal transmisi. Media transmisi kabel dapat dipasang di atas tanah maupun di bawah tanah. Beberapa contoh media transmisi kabel.

a. *Twisted Pair*

Kabel *twisted pair* adalah salah satu contoh transmisi fisik yang terdiri dari dua konduktor yang digabungkan. Fungsi dari penggabungan tersebut adalah untuk mengurangi/meniadakan interfensi elektromagnetik dari luar, seperti radiasi elektromagnetik dari UTP dan *crosstalk* yang terjadi di antara kabel yang saling berdekatan. Kabel *twisted pair* terbagi menjadi 2 yaitu STP dan UTP. Gambar 2.10 merupakan kabel *twisted pair.*



Gambar 2.10 Kabel Twisted Pair

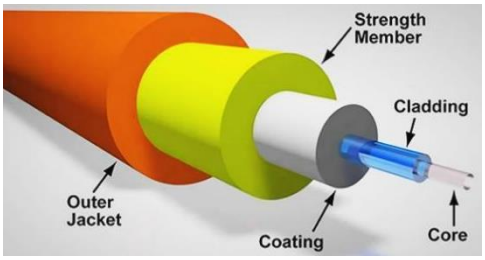
b. *Coaxial*

Kabel *coaxial* merupakan kabel yang biasa dipakai untuk memancarkan sinyal frekuensi tinggi. Pada kabel *coaxial* terdapat ukuran diameter kabel yang besar maupun yang kecil. Kabel *coaxial* memiliki kemampuan untuk mentransmisikan informasi hingga 900 saluran telepon dan juga bisa dipasang di bawah tanah. Gambar 2.11 merupakan kabel *coaxial*.

Gambar 2.11 Kabel *Coaxial*

c. Fiber *Optic*

Kabel fiber *optic* merupakan media transmisi yang terbuat dari serat kaca yang digunakan untuk mengirimkan sinyal berbentuk cahaya. Fiber *optic* terdapat beberapa jenis yaitu *single* mode step *index*, multi mode step *index* dan multi mode *grade index*[13]. Gambar 2.12 merupakan kabel fiber *optic*[14].



Gambar 2.12 Kabel *Fiber Optic*

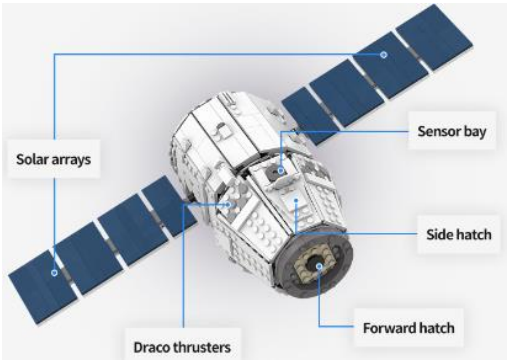
2. Media Transmisi Nirkabel

a. Gelombang Mikro

Gelombang mikro atau *microwave* merupakan gelombang yang menggunakan frekuensi tinggi, seperti UHF, EHF dan SHF. Gelombang mikro memiliki kemampuan mengirim data dalam jumlah yang besar namun dengan biaya yang murah, karena frekuensi tinggi atau gelombang pendek hanya membutuhkan antena berukuran kecil.

b. Satelit

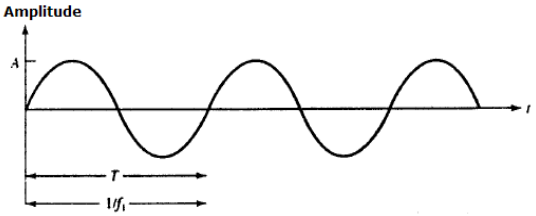
Satelit merupakan media transmisi yang berfungsi untuk menerima sinyal dari stasiun bumi lalu mengirimkan Kembali ke stasiun bumi lain. Orbit satelit mengitari bumi pada ketinggian 36.000 kilometer di atas bumi. Dengan satelit ini memiliki kemampuan untuk menjangkau permukaan bumi yang cukup luas dan melacak lalu lintas telekomunikasi antar benua. Gambar 2.13 merupakan ilustrasi satelit.



Gambar 2.13 Satelit

c. Gelombang Radio

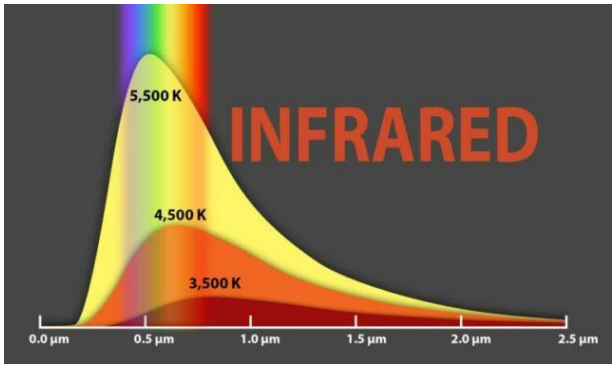
Gelombang radio memiliki fungsi untuk mengirimkan data maupun suara. Gelombang radio memiliki kemampuan untuk mengirimkan isyarat dengan posisi acak maupun bergerak. Gambar 2.14 merupakan ilustrasi dari gelombang radio.



Gambar 2.14 Gelombang Radio

d. Inframerah

Inframerah merupakan media transmisi untuk jarak dekat. Inframerah biasa digunakan untuk *remote control* televisi maupun perangkat elektronik yang lain. Kelebihan inframerah yaitu kebal terhadap interferensi radio dan elektromagnetik dan mudah diaplikasikan namun jarak penggunaan yang terbatas dan tidak dapat menembus dinding[13]. Gambar 2.15 merupakan ilustrasi dari inframerah[14].

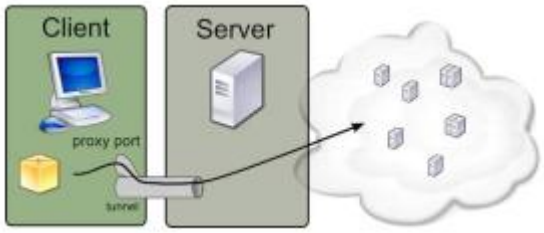


Gambar 2.15 Inframerah

2.2.2 Teknologi VPN

A. *Tunneling*

Tunneling merupakan bagian yang menjadi fundamental dasar jaringan VPN, dengan adanya *tunneling* suatu paket yang ada dalam suatu jaringan akan dibungkus (*encapsulation*) kedalam *packet protocol* lain. Sifat dari *tunneling* ini akan menyediakan sebuah koneksi *point to point logical*, yang artinya tidak menampakkan fisiknya seperti bentuk kabel sepanjang jaringan yang dibangun yang sifatnya adalah *connectionless*[15]. Gambar 2.16 merupakan ilustrasi dari *tunneling*.



Gambar 2.16 Ilustrasi *Tunneling*

Tunneling hanya akan berfokus terhadap komunikasi yang ada di dalam jaringan *private* yang dibangun sendiri, dan tidak terikat dengan paket-paket lain yang tidak melintasi jaringannya, sehingga dengan adanya *tunneling* ini otomatis komunikasi yang ada pada jaringan tersebut dijamin tidak akan diinterferensi oleh pihak luar yang tidak berkepentingan [16].

B. *Virtual Private Network* (VPN)

VPN adalah sebuah teknologi yang digunakan untuk bertukar informasi, berkomunikasi dari satu pihak ke pihak yang lain melalui suatu jaringan *local* yang hanya bisa diakses oleh pihak yang bersangkutan tersebut. VPN tetap dibangun di atas jaringan internet atau bisa dibilang memerlukan jaringan internet, akan tetapi ketika suatu komunikasi telah menggunakan VPN, komunikasi yang ada tersebut tidak nampak secara fisik hanya berupa sebuah jaringan virtual yang sifatnya pribadi. Artinya, dengan VPN bisa membuat suatu jaringan yang berada di internet seolah olah sebagai suatu jaringan lokal saja, meskipun pihak yang sedang berkomunikasi terpisah dengan geografis yang jauh[16].

C. *Dynamic Multipoint Virtual Private Network* (DMVPN)

DMPVN merupakan sebuah teknologi VPN yang dikembangkan oleh Cisco yang digunakan untuk membangun suatu komunikasi antara beberapa *site* dengan

cara yang dinamis, cepat dan otomatis[17]. DMVPN yang pada dasarnya VPN ini bisa menciptakan suatu jaringan aman yang digunakan untuk berkomunikasi, bertukar data. Berbeda dari VPN pada umumnya pada DMVPN, koneksi yang terbentuk bukan secara *point to point*, melainkan secara *point to multipoint* oleh sebab itu DMVPN ini sangat cocok diterapkan kepada suatu kantor dengan memiliki kantor cabang yang banyak. Hal tersebut disebabkan karena DMVPN akan membuat sebuah topologi *full mesh* VPN yang akan menghubungkan semua kantor-kantor yang ada. Kantor-kantor yang telah menerapkan DMVPN akan saling terhubung secara *private* seolah-olah komunikasi hanya di dalam perusahaanya sendiri walaupun sebenarnya komunikasi yang ada tersebut melewati jaringan *public* dan posisi antar *site* atau kantornya terpisah secara geografis[18]. Bagian dalam DMVPN secara garis besar hanya terdiri dari *router hub* dan *router spoke*. *Hub* pada DMVPN nantinya akan bertindak sebagai pusat komunikasi atau dikatakan *server* dari DMVPN, sedangkan *spoke* yang menjadi *client* DMVPN yang nantinya akan dihubungkan dengan kantor-kantor cabangnya. Walaupun model DMVPN berbasis *client server* akan tetapi komunikasi DMVPN bisa memungkinkan kantor-kantor cabang yang ada saling bertukar informasi secara langsung tanpa harus melewati *hub router*nya terlebih dahulu. Setiap *site* atau kantor cabang (*router spoke*) dapat terhubung langsung dengan site yang lain, dimanapun posisinya[15].

D. Komponen DMVPN

DMVPN merupakan sebuah teknologi yang tidak hanya tersusun dari satu komponen saja. Tetapi terdapat beberapa komponen yang diperlukan, antara lain

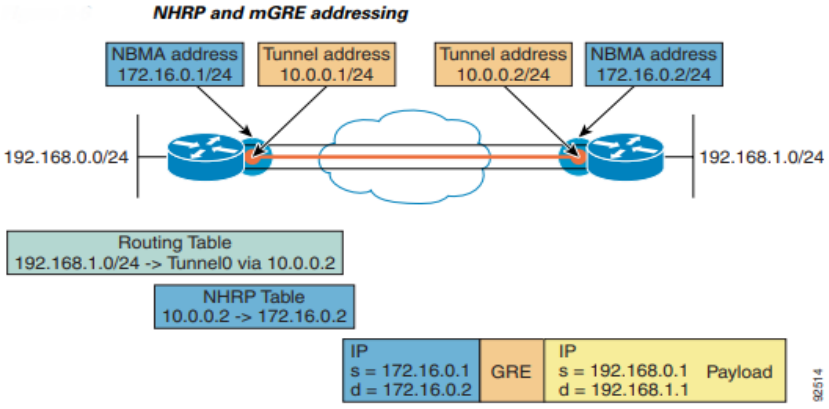
1. *Generic Routing Encapsulation Tunnel.*

   Generic Routing Encapsulation (GRE) merupakan *protocol* yang difungsikan untuk mengenkapsulasi lebih dari satu jenis paket *protocol* yang berbeda kedalam paket *layer* 3, yaitu IP. GRE sendiri dikembangkan oleh Cisco. Komunikasi dengan model *tunnel* ini berfungsi untuk meneruskan suatu paket dari satu jaringan menuju jaringan yang lain. GRE akan membuat sebuah terowongan *virtual* pada masing-masing ujung perangkat *router* Cisco sehingga paket-paket akan didistribusikan melalui sistem *tunnel* tersebut[18]. Mode *GRE Tunnel* ini bisa dikembangkan sifatnya menjadi *point to multipoint*

artinya tidak hanya menghubungkan satu peranġkat ke satu perangkat juga. Tetapi bisa menghubungkan satu perangkat dengan banyak perangkat.

2. *Next Hop Resolution Protocols* (NHRP)

Mengacu pada *rfc* 2332 NHRP adalah *protocol* dan juga *cache* resolusi alamat *Layer* 2, NHRP ini bisa dikatakan seperti ARP (*Address Resolution Protocol)* dan *Frame Relay Inverse-ARP*. Dalam jaringan DMVPN, keberadaan dari NHRP digunakan oleh *router* cabang atau *spoke router* yang terhubung dengan sebuah alamat IP fisik *router* lain atau dikenal dengan istilah NBMA (*Non Broadcast Multiple Address)* yang bertindak sebagai *tunnel source* untuk menentukan alamat IP dari NBMA *hop* berikutnya. NBMA *next hop* tersebut bisa *router* cabang lain atau bisa juga berupa *router hub*. Gambar 2.17 menunjukkan bagaimana proses pengalamatan yang terjadi pada NHRP dan MGRE[19].



Gambar 2.17 Pengalamatan NHRP dan MGRE

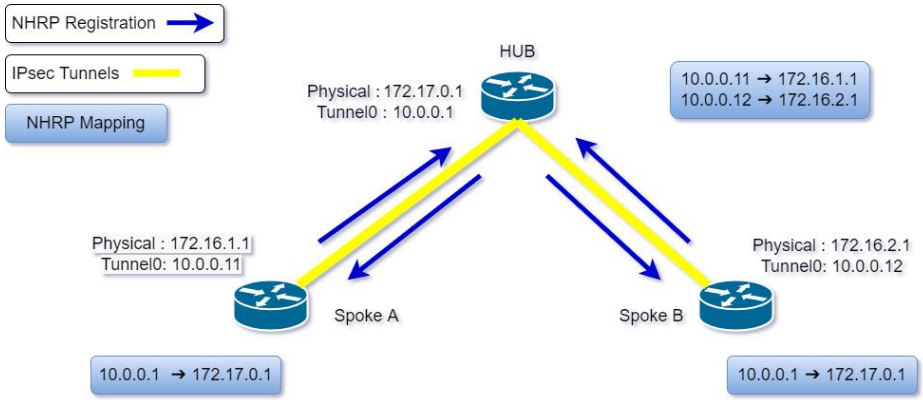
E. Desain dan Implementasi DMVPN

Teknologi *DMVPN* terdapat 3 jenis atau model desain dalam penerapannya, dimana setiap jenis yang ada memiliki karakteristik yang berbeda antara satu dengan yang lain. Model desain ini yang kemudian disebut dengan *phase.* Penentuan penggunaan *phase* akan mempengaruhi pola lalu lintas *spoke-to-spoke* untuk mendukung desain perutean dan skalabilitas[20].

1. *Phase* 1

Phase 1 dalam teknologi DMVPN memiliki karakteristik bekerja secara *hub* dan *spoke*. Trafik yang ada di *phase* 1 akan melalui *hub*, oleh sebab itu apabila sebuah *router* cabang (*spoke*) ingin berkomunikasi dengan *spoke* yang

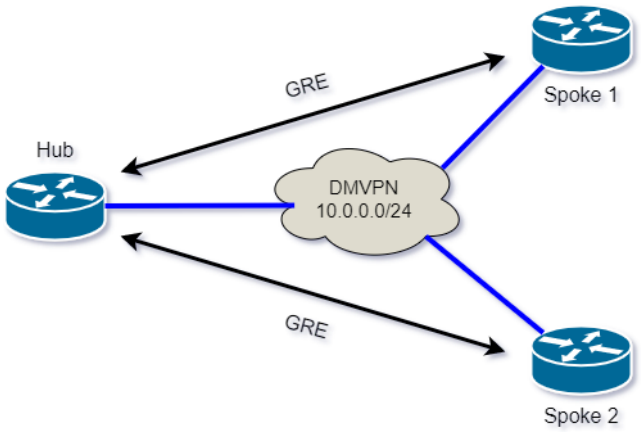
lain maka harus melewati *hub* terlebih dahulu sebagai pusat lalu lintas DMVPN seperti pada gambar 2.18 [21].



Gambar 2.18 DMVPN *Phase* 1

2. *Phase* 2

Phase 2 akan menggunakan *multipoint* GRE *tunnel interface* pada *spoke*nya yang sebelumnya pada *phase* 1 hanya pada router *hub*. *Spoke* yang menerapkan *Multipoint* GRE akan membuat komunikasi antar *spoke* yang ada bisa secara langsung tanpa harus melewatkan trafik yang ada tersebut menuju *hub*. Cara kerja dari *phase* 2 ini akan memanfaatkan *protocol* NHRP, *router spoke* yang berada di dalam DMVPN akan mengirim pesan *request* kepada *router hub* berbentuk NHRP *resolution,* setelah itu akan diteruskan ke *spoke* lain[22]. NHRP *resolution* ini bertujuan agar *router spoke* bisa menemukan alamat NHRP dari *spoke* yang lainnya seperti pada gambar 2.19.

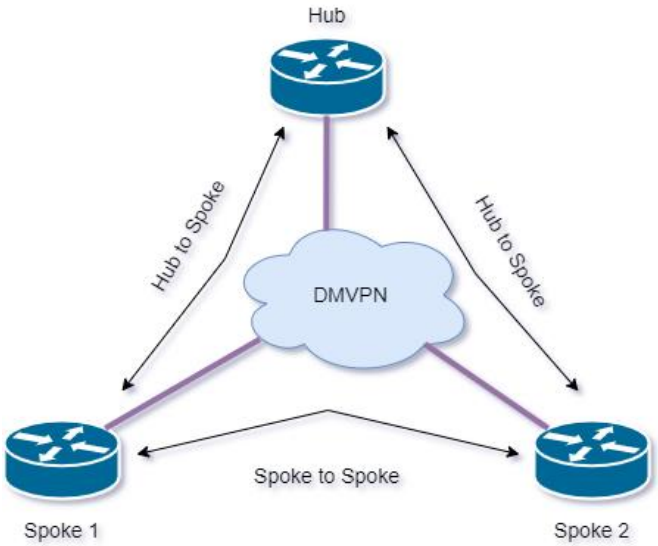


Gambar 2.19 DMVPN *Phase* 2

3. *Phase* 3

Phase terakhir dari DMVPN adalah *phase* 3. *Phase* 3 menggabungkan fitur peringkasan tabel *routing* yang ada di *phase* 1 dan komunikasi *direct*

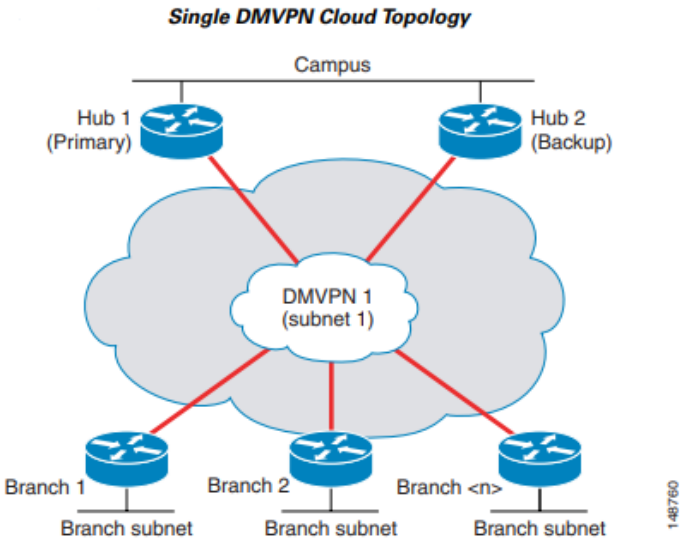
spoke-spoke yang ada di *phase* 2, oleh sebab itu *phase* 3 ini akan membuat DMVPN menjadi lebih *scalable*. Prinsip kerjanya pada *phase* 3 akan meminta *hub* untuk meringkas rute *default* atau meringkas semua *prefix* pada *spoke* yang kemudian dilanjut dengan pengaktifan pesan NHRP *redirect*. NHRP *redirect* yang dikirimkan *router hub* perlu direspon oleh *router spoke* dengan mengaktifkan juga pesan NHRP *shortcut*[23]. Gambar 2.20 merupakan DMVPN *Phase* 3.



Gambar 2.20 DMVPN *Phase* 3

F. DMPVN *Dual Hub Single Cloud*

Merupakan implementasi lanjutan dari desain *DMVPN* dengan penambahan sebuah *Router Hub* yang digunakan sebagai redudansi apabila *hub* utama *down* dimana memiliki satu buah MGRE *tunnel* untuk menghubungkan *hub* dan *spoke.* Menyediakan *high availability* dengan penggunaan *router hub* kedua, yang berada di *subnet* DMVPN yang sama dengan *router* utama. Ini yang disebut sebagai topologi *dual hub single cloud* seperti pada gambar 2.21[19].

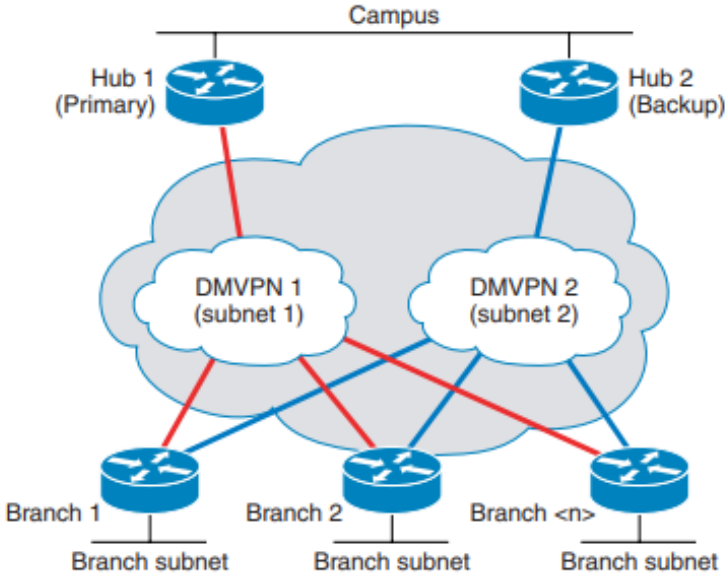


Gambar 2.21 DMVPN *Dual Hub Single Cloud*

Penggunaan *dual hub* dan *single cloud* pada topologi ini merupakan satu kesatuan dan tidak bisa berjalan sendiri-sendiri karena dari topologi dasar DMVPN yang menggunakan satu buah *hub* dan satu buah *cloud.*

G. DMVPN *Dual Hub Dual Cloud*

Merupakan model yang sama seperti *dual hub single cloud*, akan tetapi memliki lebih dari satu jalur MGRE *tunnel*nya yang mengarahkan dari *hub* menuju *spoke* dimana jalur berwarna merah merupakan MGRE *tunnel* pertama dan jalur berwarna biru merupakan MGRE *tunnel* kedua. Masing-masing *spoke* akan terhubung dengan dua jalur MGRE seperti pada gambar 2.22 [19].



Gambar 2.22 DMVPN *Dual Hub Dual Cloud*

2.2.3 Protokol *Routing*

Routing yaitu proses pengiriman informasi dengan meneruskan paket data dari jaringan satu ke jaringan yang lain. Pada *routing* dinamis, terdapat beberapa macam *routing* protokol.

A. *Open Shortest Path First*

Open Shortest Path First (OSPF) merupakan protokol *routing* yang dikembangkan oleh *Internet Engineering Task Force* (IETF). OSPF memiliki 2 karakteristik utama. Pertama protokol ini bersifat *open* atau terbuka yang berarti spesifikasi dari protokol ini terbuka untuk umum tidak hanya vendor tertentu saja. Kedua yaitu OSPF merupakan *routing protocol* yang berbasis pada algoritma *Shortest Path First* (SPF). OSPF adalah protokol *routing* yang termasuk dalam kategori *routing* dinamis, yang bisa mendeteksi perubahan topologi yang terjadi di dalam sebuah jaringan, perubahan topologi yang dimaksud disini apabila sebuah *interface* yang mati atau tidak berfungsi atau salah satu node dalam OSPF yang diganti, ketika terjadi hal tersebut OSPF akan segera melakukan perhitungan rute baru terbaik yang bebas dari perulangan. OSPF termasuk dalam kategori *routing protocol link-state*. OSPF menggunakan suatu paket LSA untuk berkomunikasi sesama *router* dalam jaringan OSPF. LSA *(Link State Advertisement)* adalah suatu paket yang berisi kumpulan informasi dimana informasi tersebut mencakup mengenai status *link* pada router. LSA akan dikirim secara periodik ke semua jaringan *router* yang terhubung dengan jaringan OSPF. Secara lengkapnya informasi paket yang berada dalam LSA berisi *link id, state of the link,* dan *cost* menuju *network* lawan. OSPF juga memiliki sebuah fitur untuk mengelompok *router-router* yang dikenal dengan sistem area. Penerapan area dalam OSPF ini akan mengelompokkan dan juga mengisolasikan *router* yang bekerja dalam area tertentu saja sehingga membuat informasi mengenai area tersebut tidak bisa diketahui oleh area lainnya. Penggunaan area ini juga akan menyebabkan trafik *routing* yang berjalan dalam jaringan OSPF akan mengalami penurunan yang signifikan[24].

Cost dari sebuah *interface* di OSPF merupakan indikasi dari *overhead* yang diperlukan untuk mengirim paket pada / di *interface* tertentu. *Cost interface* berbanding terbalik dengan *bandwidth interface*.

Adapun perhitungan *cost* dilakukan melalui persamaan (2.1) [25].

$$cost = \frac{bandwidth\ referensi}{bandwidth\ interface} \quad (2.1)$$

OSPF bergantung pada nilai *cost* yang berbanding terbalik dengan *bandwidth link*. Oleh karena itu, *bandwidth link* yang lebih tinggi lebih diprioritaskan daripada yang lebih rendah. Nilai *cost default* bergantung pada jenis *interface* yang digunakan. *Bandwidth* referensi *default* 100 Mbps digunakan untuk perhitungan *cost* OSPF. Sebagai contoh, jika pengguna memiliki *interface Ethernet* (10 Mbps), nilai *cost* jalur OSPF adalah 100 Mbps / 10 Mbps = 10. Adapun nilai *Cost default* berdasarkan jenis *interface* terdapat pada tabel 2.2[26].

Tabel 2.2 Nilai *Cost Default*

Jenis *Interface*	*Bandwidth Interface*	Nilai *Cost Default*
Gigabit Ethernet	1 Gbps	1
Fast Ethernet	100 Mbps	1
Ethernet	10 Mbps	10
DS1	1.544 Mbps	64
DSL	768 Kbps	133

OSPF dapat melakukan *load balancing* menggunakan *equal cost load balancing*. Ketika melakukan pengiriman data terdapat beberapa rute dengan nilai *cost* yang sama dan dengan tujuan yang sama, maka OSPF akan melakukan *load balancing*. Routing OSPF dapat membuat *load balancing* berdasarkan *per-packet* atau *per-destination*. *Per-destination load balancing* yaitu paket yang diberikan host sumber dan tujuan tertentu dijamin menggunakan jalur yang sama, termasuk apabila terdapat lebih dari satu jalur *routing*. Sedangkan pada *per-packet load balancing* akan menggunakan metode *round-robin* untuk menentukan jalur mana yang akan dilewati setiap paket ke alamat tujuan. Secara *default* konfigurasi yang digunakan yaitu *per-destination load balancing*[27]

B. *Routing Information Protocol*

Routing Information Protocol biasa disingkat RIP bekerja menentukan jalur routing berdasarkan jarak terdekat dengan router tujuan. Jarak dari router pengirim ke router tujuan disebut hop count sedangkan jarak dari router satu ke router selanjutnya disebut hop. Pada routing RIP terdapat versi 1 dan 2.

C. *Enhanced Interior Gateway Routing Protocol*

Enhanced Intertior Gateway Routing Protocol atau EIGRP merupakan protokol *routing* yang hanya terdapat pada *router cisco* atau *cisco proprietary*. Untuk menentukan pemilihan jalur *routing*, pada *routing protocol* EIGRP tidak menggunakan *hop count* seperti pada RIP.

D. *Intermediate System – Intermediate System*

Protokol routing *Intermediate System – Intermediate System* (IS-IS) merupakan protocol routing yang pemilihan jalur routingnya menggunakan algoritma Dijkstra dan juga terdapat konsep area seperti pada protokol *routing* OSPF.

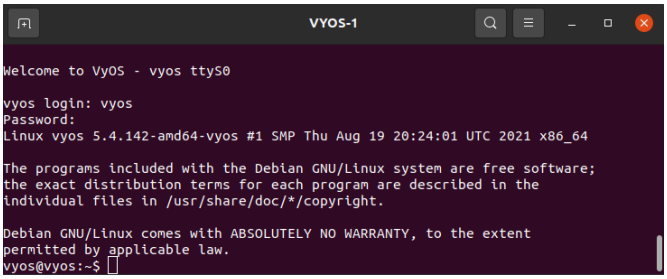
E. *Border Gateway Protocol*

Border Gateway Protocol (BGP) merupakan kategori routing advanced distance vector. Namun dalam menentukan jalur, routing BGP tak hanya menggunakan jarak, tetapi juga menggunakan parameter dan atribut lain yang cukup kompleks[28].

2.2.4 Sistem Operasi *Router*

A. VyOS

VyOS merupakan sebuah perangkat yang difungsikan sebagai *router*, *firewall* dan VPN dimana tersusun dari *kernel linux debian* dan bersifat *open source*. VyOS menggunakan sintaks konfigurasi dan *command line interface* yang mengadopsi dari Juniper JunOS seperti yang dimodelkan oleh XORP *Project* yang menjadi *original routing engine* dari Vyatta. Saat ini VyOS menggunakan FRRouting sebagai *routing engine*. Fitur-fitur yang ada pada VyOS ini mencakup kemampuan menjalankan berbagai *routing protocol* seperti OSPF, RIP, BGP, VRRP, dan routing *policy mapping* dan *filtering* yang luas dimana *support* IPV4 dan IPV6. Terkait kemampuan VPN mencakup OpenVPN, IPSec, Wireguard, DMVPN, Ikea dan masih banyak lagi. VyOS juga bisa berjalan pada fisikal ataupun *virtual platform* yang ada[29]. Gambar 2.23 merupakan halaman awal *interface* dari VyOS.



Gambar 2.23 VyOS

B. *Cisco* IOS

Cisco IOS adalah perangkat lunak infrastruktur jaringan yang digunakan pada perangkat Cisco. Saat ini Cisco IOS beroperasi pada jutaan sistem aktif, mulai dari router rumah kantor kecil hingga sistem inti jaringan penyedia layanan internet[30].

C. RouterOS

RouterOS merupakan sistem operasi milik Mikrotik. Sistem operasi ini biasa diinstal di perangkat *Routerboard* Mikrotik. Selain itu bisa juga diinstal pada PC dan mengubah fungsinya menjadi sebuah router.

D. ClearOS

ClearOS merupakan sistem operasi untuk sistem server, jaringan dan gateway. Sistem operasi ini dapat juga digunakan secara virtual atau digunakan sebagai sistem operasi host ke mesin virtual lainnya[31].

2.2.5 Standar Kinerja

A. *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON)

TIPHON merupakan standar penilaian parameter *Quality of Service* (QoS) yang dikeluarkan oleh badan standar *European Telecommunications Standards Institute* (ETSI). ETSI adalah organisasi standarisasi dunia di bidang informasi dan komunikasi. Organisasi ETSI mendukung pengembangan dan pengujian standar teknis global untuk sistem, aplikasi, dan layanan yang mendukung Teknologi Informasi dan Komunikasi (TIK)[32].

B. *International Telecommunication Union - Telecommunication Standardization Sector* (ITU – T)

Standar ITU-T didirikan pada tahun 1956 sebagai Komite Konsultasi Telepon dan Telegraf Internasional atau *Comité consultatif international téléphonique et télégraphique* (CCITT). Sektor ini melakukan standardisasi telekomunikasi global (kecuali untuk radio). Pada tahun 1993, CCITT berubah menjadi ITU-T. Pekerjaan standardisasi dilakukan oleh *Study Groups* yaitu *Study Groups* 13 untuk jaringan dan *Study Groups* 16 untuk multimedia. Badan induk dari *Study Groups* adalah *World Telecommunication Standardization Assembly* yang diadakan per empat tahunan[33].

2.2.6 *Quality Of Service*

Quality of Service (QoS) adalah kemampuan untuk menyediakan layanan yang baik guna dilewati trafik dalam berkomunikasi antar atau dalam jaringan. *QoS* merupakan sebuah *system* arsitektur *end to end* dan bukan merupakan sebuah fitur yang dimiliki oleh jaringan. *Quality of Service* suatu jaringan mengacu ke tingkat kecepatan dan keandalan pengiriman berbagai jenis trafik atau data yang dikirimkan dalam suatu komunikasi. Tiap-tiap Aplikasi yang berbeda membutuhkan suatu persyaratan QoS tersendiri supaya selama proses pengiriman trafik yang ada tidak terlalu banyak paket yang hilang, menyediakan layanan *real-time* yang bagus, *delay* dan *jitter* yang rendah, dan alokasi *bandwidth* yang bagus. Parameter-parameter yang ada pada QoS biasanya terdiri dari *troughput*, *delay*, *jitter* dan *paket loss*[34].

A. *Throughput*

Yaitu kecepatan transfer data efektif, yang diukur dalam *bps*. *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diterima oleh tujuan selama selang waktu tertentu yang dibagi oleh durasi selang waktu tersebut[35].

Perhitungan *Throughput* menggunakan persamaan (2.2).

$$Throughput = \frac{jumlah\ data\ yang\ berhasil\ lewat\ (bit)}{lama\ waktu\ pengantaran\ (second)} \qquad (2.2)$$

Tabel 2.3 Klasifikasi Standarisasi Throughput [36]

Kategori *Throughput*	*Throughput*	*Indeks*
Sangat bagus	>2,1 Mbps	4
Bagus	1200 kbps – 2,1 Mbps	3
Sedang	700 – 1200 kbps	2

Kategori *Throughput*	*Throughput*	*Indeks*
Jelek	338 – 700 kbps	1
Sangat Jelek	0 – 338 kbps	0

B. *Delay*

Delay merupakan lamanya waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* bisa dipengaruhi oleh beberapa faktor seperti jarak, media fisik, kongesti atau juga waktu proses yang lama[35].

Perhitungan delay menggunakan persamaan (2.3)

$$delay = \frac{panjang\ paket\ (bit)}{link\ bandwitdh\ (second)} \quad (2.3)$$

Tabel 2.4 Klasifikasi Standarisasi Delay[36]

Kategori *delay*	Besar *delay*	*Indeks*
Sangat bagus	<150 ms	4
Bagus	150 s/d 250 ms	3
Sedang	250 s/d 350 ms	2
Jelek	350 s/d 450 ms	1

C. *Jitter*

Jitter sering disebut sebagai variasi *delay*, dimana jitter ini berhubungan erat dengan *delay*. Jitter menunjukkan banyaknya variasi *delay* pada pengiriman data yang ada di jaringan. Tumpukan delay pada *router* dan *switch* dapat menyebabkan *jitter*[35].

Perhitungan *Jitter* menggunakan persamaan (2.4)

$$jitter = \frac{Total\ Variasi\ Delay}{Total\ Paket\ diterima} \quad (2.4)$$

Tabel 2.5 Klasifikasi Standarisasi Jitter[36]

Kategori *jitter*	Besar *jitter*	*Indeks*
Sangat bagus	0 ms	4
Bagus	0 ms s/d 75 ms	3
Sedang	75 ms s/d 125 ms	2
Jelek	125 s/d 225 ms	1

D. *Packet Loss*

Packet loss adalah suatu parameter yang digambarkan sebagai berapa jumlah paket yang hilang selama proses pengiriman terjadi yang dapat disebabkan oleh *collision* ataupun *congestion*[35].

Perhitungan *packet loss* menggunakan persamaan (2.5)

$$Packet\ loss\ = \frac{Paket\ data\ dikirim - paket\ data\ diterima}{Paket\ data\ yang\ dikirim}\ x\ 100 \qquad (2.5)$$

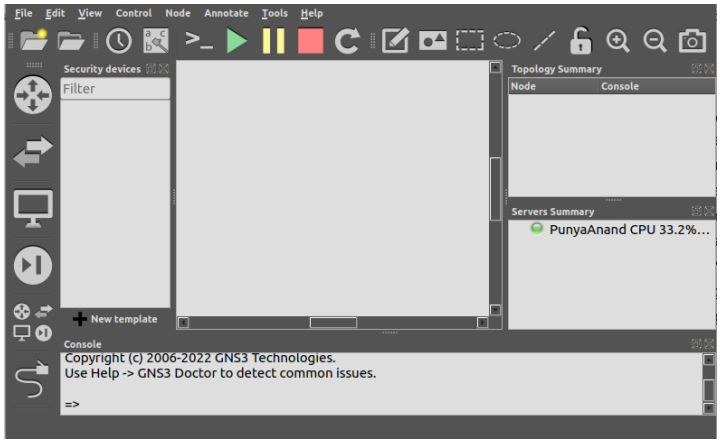
Tabel 2.6 Klasifikasi Standarisasi *Packet Loss* [36]

Kategori Degradasi	*Packet loss (%)*	*Indeks*
Sangat bagus	0	4
Bagus	3	3
Sedang	15	2
Jelek	25	1

2.2.7 Aplikasi Simulasi Jaringan

A. *Graphical Network Simulator 3*

GNS *(Graphical Network Simulator 3)* adalah aplikasi *open source* simulasi jaringan yang dapat bekerja secara sinergi mensimulasikan hampir semua sistem operasi. GNS3 sebuah aplikasi yang masih belum bisa dikatakan sempurna, masih terdapat beberapa segmen yang terus dikembangkan namun GNS3 adalah satu-satunya aplikasi simulasi jaringan yang mampu melakukan simulasi jaringan secara nyata. GNS3 memiliki antarmuka grafis yang mampu dipahami sehingga mempermudah untuk merancang dan mengkonfigurasi jaringan virtual[37]. Gambar 2.23 merupakan tampilan dari GNS3.



Gambar 2.24 GNS3

B. *Cisco Packet Tracer*

Cisco Packet Tracer merupakan *software* simulasi jaringan yang dikembangkan oleh perusahaan yang terkenal di bidang jaringan yaitu *Cisco Systems*. *Cisco Packet Tracer* memberikan *environtment* pembelajaran simulasi dan visualisasi yang realistis, memliki kemampuan untuk melihat proses internal secara *real time*, memungkinkan untuk multi *user*, kolaborasi *real time* dan juga kompetisi untuk pembelajaran yang dinamis.

C. *iNetwork*

iNetwork merupakan aplikasi simulasi jaringan yang memiliki sifat pembelajaran interaktif yang dapat mengajarkan para penggunanya mengenai jaringan. Aplikasi ini dibuat berbasis grafis sehingga cukup mudah dalam penggunaannya. iNetwork memiliki beberapa fitur yaitu dapat melakukan simulasi cara kerja DHCP server, DNS, web server, *routing* dan *firewall*. Selain itu *iNetwork* memiliki fitur *command prompt*[38].

2.2.8 Aplikasi Pengujian Jaringan

A. *Distributed Internet Traffic Generator*

*Distributed Internet Traffic Generator (*D-ITG*)* adalah platform yang mampu menghasilkan trafik IPv4 dan IPv6 dengan mereplikasi beban kerja aplikasi internet saat ini secara akurat. Pada saat yang sama D-ITG juga merupakan alat pengukuran jaringan yang dapat mengukur kinerja yang paling umum (misalnya *throughput, delay, jitter, packet loss*). D-ITG mampu mereplikasi properti statistik trafik dari berbagai aplikasi terkenal seperti *Telnet, VoIP* - G.711, G.723, G.729, *Voice Activity Detector,* RTP dengan DNS, *game online*)[39].

B. *Iperf*

Iperf merupakan *tool* yang berfungsi untuk mengukur *throughput* pada sebuah jalur *network*. Agar dapat dilakukan pengukuran, *iperf* harus terpasang pada sisi pengirim dan juga penerima. *Iperf* dapat digunakan juga untuk mengukur performa *link* pada TCP maupun UDP[40].

C. *Axence NetTools*

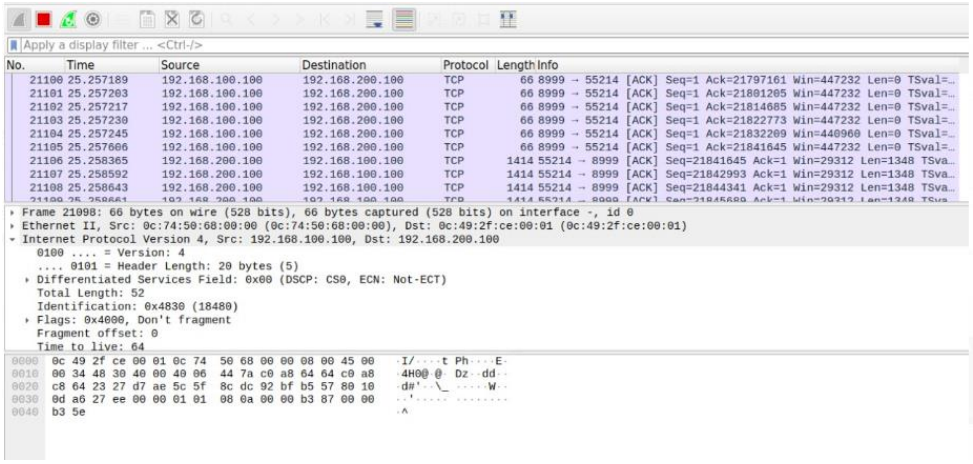
NetTools merupakan tool untuk mengukur performa jaringan, memindai jaringan, alat administrasi, keamanan dan mendiagnosa permasalahan pada

jaringan. NetTools memiliki beberapa *tool* populer seperti *trace*, *lookup*, *port scanner*, dan SNMP browser. Dengan *user interface* membuat NetTools menjadi mudah untuk digunakan[41].

2.2.9 Aplikasi Monitoring Jaringan

A. *Wireshark*

Wireshark tergolong kedalam kategori *software sniffer freeware*. Program *sniffer* sendiri merupakan adalah sebuah *tool* yang dapat digunakan apabila kita ingin melihat kondisi di dalam sebuah jaringan, Jaringan yang bisa dilihat ini bisa jaringan *Ethernet* maupun *non-ethernet*. *Wireshark* yang sifatnya bisa melakukan *sniffing* pada suatu jaringan ini biasanya seringkali digunakan untuk menemukan adanya suatu permasalahan pada jaringan. Fungsi *wireshark* yaitu menganalisis data yang melintas pada media transmisi dan mempresentasikan informasi yang didapat secara logis sesuai dengan model *OSI Reference Model*. *Wireshark* bersifat *cross – platform* dan menggunakan *pcap* untuk meng*capture* paket jaringan. *Wireshark* dapat berjalan pada hampir semua sistem operasi yang tersedia[16]. Gambar 2.25 merupakan tampilan dari *Wireshark.*



Gambar 2.25 *Wireshark*

B. *Tcpdump*

Tcpdump merupakan *tool* yang berfungsi untuk melakukan *capture* dan inspeksi terhadap lalu lintas jaringan. Untuk penggunaannya yaitu melalui baris perintah. Lalu lintas data yang dapat ditangkap oleh *tcpdump* tidak hanya paket TCP tetapi juga UDP, ARP maupun ICMP[42].

2.2.10 *High Availability*

High availability (HA) merupakan sebuah konsep pada suatu infrastruktur yang akan mencegah suatu sistem yang berjalan pada infrastruktur tersebut mengalami kegagalan pengoperasian. Dalam istilah lain HA sering disebut sebagai *failover* yang berarti sebuah mode *backup* ketika suatu perangkat mengalami kegagalan sistem baik dari segi *power, service, database* ataupun jaringannya. HA ini umumnya bertujuan untuk meningkatkan ketersediaan layanan ketika terdapat suatu *down* pada sistem [43][44]. Terdapat model yang biasa dikenal dalam *High Availability*, yaitu konsep *load balancing* dan *failover*

A. *Load balancing*

Load balancing adalah suatu teknik yang digunakan untuk memisahkan antara dua atau lebih jalur koneksi. Dengan mempunyai banyak jalur maka optimalisasi utilisasi sumber daya, *throughput*, atau *response time* akan semakin baik karena mempunyai lebih dari satu jalur yang bisa berfungsi untuk penyeimbang beban, saling mem-*backup* pada saat jaringan *down* dan menjadi cepat pada saat jaringan kondisi normal jika memerlukan 100% koneksi *uptime* dan yang menginginkan koneksi *upstream* yang berbeda dan dibuat saling mem-*backup*[45].

B. Failover

Model yang lain adalah *failover*. *Failover* adalah teknik yang menerapkan dua atau lebih jalur komunikasi untuk mencapai suatu *network* tujuan. *Failover* biasa digunakan untuk meningkatkan ketersediaan jalur komunikasi. Dalam keadaan normal hanya akan ada satu jalur yang digunakan. Jalur yang lain berfungsi sebagai cadangan dan hanya akan digunakan apabila jalur utama terputus[45].