

## **BAB 2**

### **LANDASAN TEORI**

Pada bab ini akan menjelaskan tentang teori yang berhubungan dengan perancangan sistem sebagai teori pendukung pada saat melakukan perancangan. Selain itu, pada bab ini menjelaskan tentang spesifikasi dari komponen perangkat keras dan sistem yang digunakan pada saat perancangan sistem.

#### **2.1 Konsep Jaringan Komputer**

Jaringan Komputer adalah sistem yang terdiri dari komputer-komputer, serta piranti-piranti yang saling terhubung sebagai satu kesatuan. Dengan dihubungkannya piranti-piranti tersebut, alhasil dapat saling berbagi sumber daya antar satu piranti lainnya.

Dalam istilah komputer, jaringan merupakan penghubung antar dua computer atau lebih yang tujuan utamanya adalah berbagi data. Jaringan komputer adalah gabungan antara hardware dan software. Jaringan komputer bisa diklasifikasikan beberapa kategori. Dijelaskan lebih lanjut di sub bab mengenal jenis jaringan komputer. Karena sebuah sistem, jaringan komputer terdiri atas komponen-komponen, dan perangkat jaringan lainnya yang bekerja Bersama-sama untuk mencapai suatu jtujuan yang sama. Tujuan dari jaringan komputer adalah:

- Membagi sumber daya, contohnya berbagi pemakaian printer, CPU, memori, harddisk.
- Komunikasi, contohnya surat elektronik, instant messaging, chatting.
- Akses informasi, contohnya web browsing.

Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan. Pihak yang meminta layanan disebut client dan yang memberikan layanan disebut server. [3]

### 2.1.1 Klasifikasi Jaringan Komputer

Berdasarkan daerah jangkauannya, jaringan dapat dibagi menjadi tiga macam yaitu :

1. Berdasarkan Teknologi Transmisi Dari teknologi Transmisi tersebut masih dibagi lagi menjadi 2 kelompok yaitu :
  - a. Jaringan Broadcasting Memiliki saluran komunikasi tunggal yang digunakan secara bersama-sama oleh semua komputer seluruh jaringan tersebut. Pesan berukuran kecil yang disebut Paket , dikirim oleh satu komputer dan diterima oleh komputer lainnya. Di dalam paket tersebut terdapat beberapa informasi seperti alamat pengiriman, alamat penerima, ukuran paket, dan isi dari paket tersebut. Ada tiga macam operasinya :
    - One resource to one destination, dimana pengirim ditujukan hanya untuk satu komputer tertentu.
    - Broadcasting, paket dikirim ke semua tujuan yang ada.
    - Multicasting.paket dikirim ke satu subset dari komputer.
  - b. Point to Point, Terdiri dari beberapa koneksi pasangan individu dari mesin-mesin. Untuk pergi dari sumber ke tempat tujuan, sebuah paket pada jaringan jenis ini mungkin harus melalui satu atau lebih mesin-mesin perantara. Seringkali harus melalui banyak route yang mungkin berbeda jaraknya. Karena itu algoritma routing memegang peranan penting pada jaringan point-to-point. [4]
2. Berdasarkan Geografis Jaringan Komputer terbagi menjadi Jaringan Wilayah Lokal atau *Local Area Network* (LAN) , Jaringan Wilayah Metropolitan atau *Metropolitan Area Network* (MAN) dan Jaringan Wilayah Luas atau *Wide Area Network* (WAN), Jaringan tanpa kabel (Nirkabel / Wi-Fi), *Internetwork*.
  - a. **LAN (Local Area Network)**

LAN merupakan jaringan komputer yang hanya mencakup wilayah kecil, seperti kampus, kantor, sekolah (Laboratorium), dll.

Kebanyakan LAN ini berbasis IEEE 802.3 Ethernet menggunakan perangkat switch yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s. Dengan perkembangan teknologi yang begitu pesat, teknologi Ethernet kini telah berkembang menjadi teknologi 802.11b atau sering disebut Wi-fi. Tempat-tempat yang menyediakan jaringan LAN atau Wi-Fi biasa disebut Hotspot.

**b. MAN (Metropolitan Area Network)**

Jaringan MAN merupakan jaringan LAN yang berukuran besar yang menggunakan teknologi yang sama dengan LAN. MAN diimplementasikan oleh sebuah perusahaan sebagai fasilitas publik, namun digunakan oleh individu maupun organisasi. Tingkat error dan delay pada jaringan MAN lebih tinggi daripada jaringan LAN, oleh karena itu MAN menghubungkan berbagai macam LAN dengan topologi yang berbeda. MAN hanya menggunakan satu atau dua buah kabel dan tidak mempunyai elemen switching, yang berfungsi untuk mengatur paket melalui kabel output. MAN dipisah dari kategori khusus karena ada standarisasi dari IEEE untuk MAN yaitu DQDB (Distributed Queue Dual Bus) atau lebih dikenal dengan sebutan 802.6

**c. WAN (Wide Area Network)**

Jaringan WAN merupakan jaringan yang mencakup area yang lebih luas sebagai contoh adalah jaringan komputer antar wilayah, antar Negara, maupun antar benua. Jaringan WAN ini bukan hanya terdiri dari media transmisi namun juga sejumlah router yang saling interkoneksi. WAN biasanya digunakan oleh perusahaan yang memiliki banyak cabang di berbagai tempat. WAN pada umumnya telah menggunakan satelit maupun kabel bawah laut. WAN terdiri dari kumpulan mesin-mesin yang bertujuan menjalankan program-program (aplikasi) pemakai/user [5].

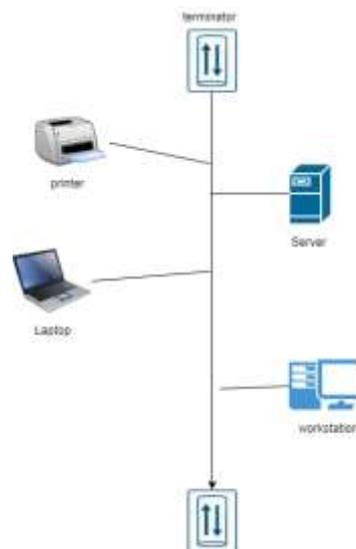
### 2.1.2 Topologi Jaringan Komputer

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, token ring, dan star. Dalam suatu jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan

komunikasi. Untuk itu maka perlu dicermati kelebihan/keuntungan dan kekurangan / kerugian dari masing - masing topologi berdasarkan karakteristiknya.

#### 1. Topologi BUS

Topologi bus terlihat pada Gambar 2. Media penghantar untuk jenis topologi BUS adalah kabel Koaksial.

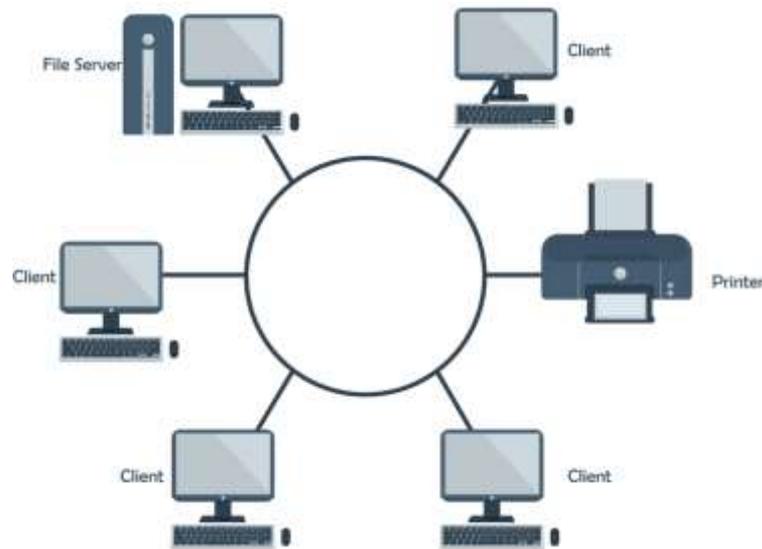


**Gambar 2. 1 Topologi BUS**

Topologi BUS menggunakan metode unicast, multicast dan broadcast. Unicast adalah komunikasi antara satu pengirim dengan satu penerima di jaringan. Multicast adalah komunikasi antara satu pengirim dengan banyak penerima di jaringan. Sedangkan pada Broadcast, setiap titik akan menerima dan menyimpan frame yang disalurkan/dihantarkan.

## 2. Topologi RING

Topologi Token RING terlihat pada Gambar 3. Metode token-ring (sering disebut ring saja) menghubungkan komputer sehingga berbentuk ring (lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai loop, data dikirimkan kesetiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan.

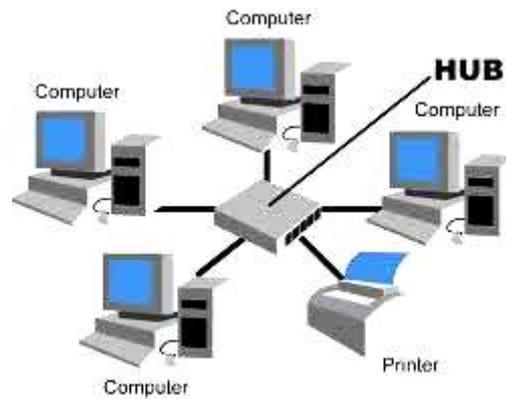


**Gambar 2. 2 Topologi RING**

## 3. Topologi STAR

Topologi ini merupakan kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya. Simpul pusat dinamakan stasiun primer atau server dan lainnya dinamakan stasiun sekunder atau client server. Setelah hubungan

jaringan dimulai oleh server maka setiap client server sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server [4].



**Gambar 2. 3 Topologi STAR**

## 2.2 Multi-Protocol Label Switching

MPLS (*Multi Protocol Label Switching*) adalah salah satu metoda yang dapat digunakan untuk tuning jaringan agar lebih meningkatkan performa jaringan. MPLS merupakan teknik untuk mengintegrasikan IP dengan ATM dalam jaringan backbone yang sama. Teknologi MPLS mempersingkat proses – proses yang ada di IP routing tradisional dengan mengandalkan sistem label switching [6].

Fungsi label pada MPLS adalah sebagai proses penyambungan dan pencarian jalur dalam jaringan komputer. MPLS menggabungkan teknologi switching di layer 2 dan teknologi routing di layer 3 sehingga menjadi solusi jaringan terbaik dalam menyelesaikan masalah kecepatan, scalability, QOS (Quality of Service), dan rekayasa trafik. Tidak seperti ATM yang memecah paket-paket IP, MPLS hanya melakukan enkapsulasi paket IP, dengan memasang header MPLS. Header MPLS terdiri atas 32 bit data, termasuk 20 bit label, 2 bit eksperimen, dan 1 bit identifikasi stack, serta 8 bit TTL. Label adalah bagian dari header, memiliki panjang yang bersifat tetap, dan merupakan satu-satunya tanda identifikasi paket. Label digunakan untuk proses forwarding, termasuk proses *traffic engineering* [7].

Dengan informasi label switching yang didapat dari routing network layer, setiap paket hanya dianalisa sekali di dalam router di mana paket tersebut masuk

ke dalam jaringan untuk pertama kali. Router tersebut berada di tepi dan dalam jaringan MPLS yang biasa disebut dengan Label Switching Router (LSR).

Ide dasar teknik MPLS ini ialah mengurangi teknik pencarian rute dalam setiap router yang dilewati setiap paket, sehingga sebuah jaringan dapat dioperasikan dengan efisien dan jalannya pengiriman paket menjadi lebih cepat. Jadi MPLS akan menghasilkan high-speed routing dari data yang melewati suatu jaringan yang berbasis parameter *quality of service* (QoS). Berikut ini perbandingan dari label switching dan routing pada IP konvensional

**Tabel 2. 1 konvensional Routing vs Label Switching**

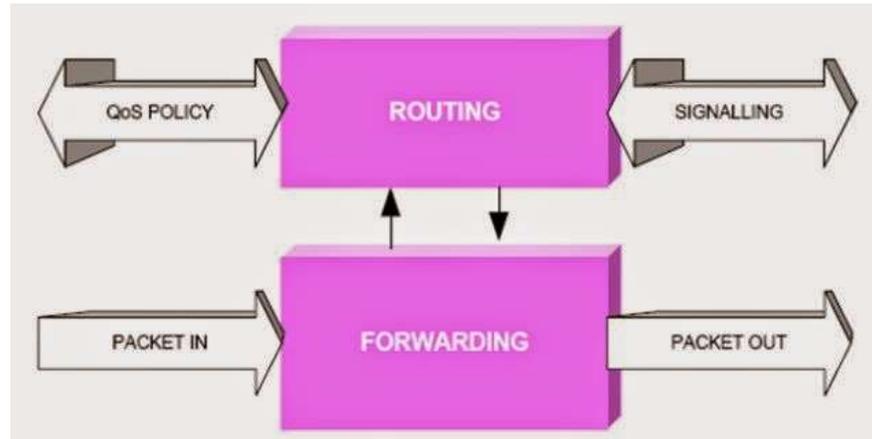
	<b>Konvensional Routing</b>	<b>Label Switching</b>
Analisis Header IP	Dilakukan pada tiap-tiap hop lintasan paket dari suatu jaringan	Dilakukan hanya sekali pada saat paket memasuki lintasan dari suatu jaringan
Support Unicast dan Multicast Data	Memerlukan algoritma forwarding dan routing multicast yang khusus	Memerlukan hanya sebuah algoritma forwarding
Penentuan Routing	Berdasarkan pada alamat tujuan yang terdapat pada header IP	Berdasarkan pada jumlah parameter, juga termasuk alamat tujuan pada header IP, seperti quality of service (QoS), type data (suara, gambar) dll.

Jaringan baru ini memiliki beberapa keuntungan diantaranya :

1. Mengurangi banyaknya proses pengolahan di IP Routers, serta memperbaiki proses pengiriman suatu paket data.
2. Menyediakan QoS dalam jaringan backbone, sehingga setiap layanan paket yang dikirimkan akan mendapat perlakuan sesuai skala prioritas.

### 2.2.1 Arsitektur MPLS

Arsitektur MPLS dipaparkan dalam RFC-3031 (Rosen 2001) adalah sebagai berikut :



**Gambar 2. 4 Arsitektur MPLS**

Network MPLS terdiri atas sirkuit yang disebut *label-switched path* (LSP), yang menghubungkan titik-titik yang disebut *label-switched router* (LSR). LSR pertama dan terakhir disebut ingress dan egress. Setiap LSP dikaitkan dengan sebuah *forwarding equivalence class* (FEC), yang merupakan kumpulan paket yang menerima perlakuan forwarding yang sama di sebuah LSR. FEC diidentifikasi dengan pemasangan label.

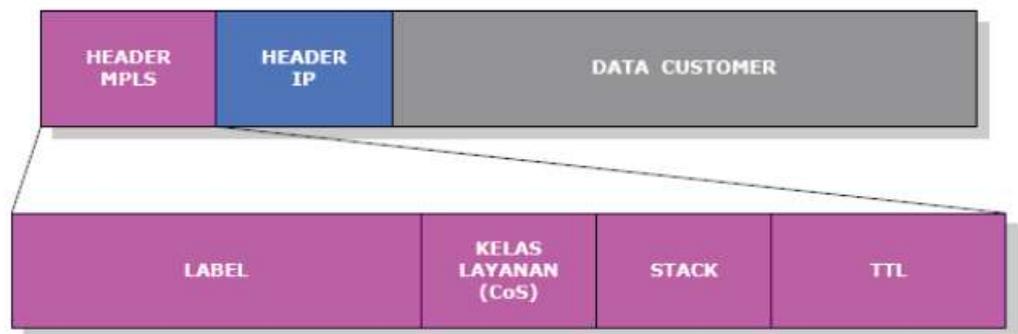
Untuk membentuk LSP, diperlukan suatu protokol persinyalan. Protokol ini menentukan forwarding berdasarkan label pada paket. Label yang pendek dan berukuran tetap mempercepat proses forwarding dan mempertinggi fleksibilitas pemilihan path. Hasilnya adalah network datagram yang bersifat lebih *connection-oriented*.

#### 2.2.1 Enkapsulasi Paket

Tidak seperti ATM yang memecah paket-paket IP, MPLS hanya melakukan enkapsulasi paket IP, dengan memasang header MPLS. Header MPLS terdiri atas 32 bit data, termasuk 20 bit label, 2 bit eksperimen, dan 1 bit identifikasi stack,

serta 8 bit TTL. Label adalah bagian dari header, memiliki panjang yang bersifat tetap, dan merupakan satu-satunya tanda

identifikasi paket. Label digunakan untuk proses forwarding, termasuk proses traffic engineering.



**Gambar 2. 5 Skema Header MPLS**

Setiap LSR memiliki tabel yang disebut *label-switching table*. Tabel itu berisi pemetaan label masuk, label keluar, dan link ke LSR berikutnya. Saat LSR menerima paket, label paket akan dibaca, kemudian diganti dengan label keluar, lalu paket dikirimkan ke LSR berikutnya.

Selain paket IP, paket MPLS juga bisa dikapsulasikan kembali dalam paket MPLS. Maka sebuah paket bisa memiliki beberapa header. Dan *bit stack* pada *header* menunjukkan apakah suatu header sudah terletak di dasar tumpukan header MPLS itu.

### 2.2.2 Distribusi Label

Untuk menyusun LSP, *label-switching table* di setiap LSR harus dilengkapi dengan pemetaan dari setiap label masukan ke setiap label keluaran. Proses melengkapi tabel ini dilakukan dengan protokol distribusi label. Ini mirip dengan protokol persinyalan di ATM, sehingga sering juga disebut protokol persinyalan MPLS. Salah satu protokol ini adalah *Label Distribution Protocol* (LDP)

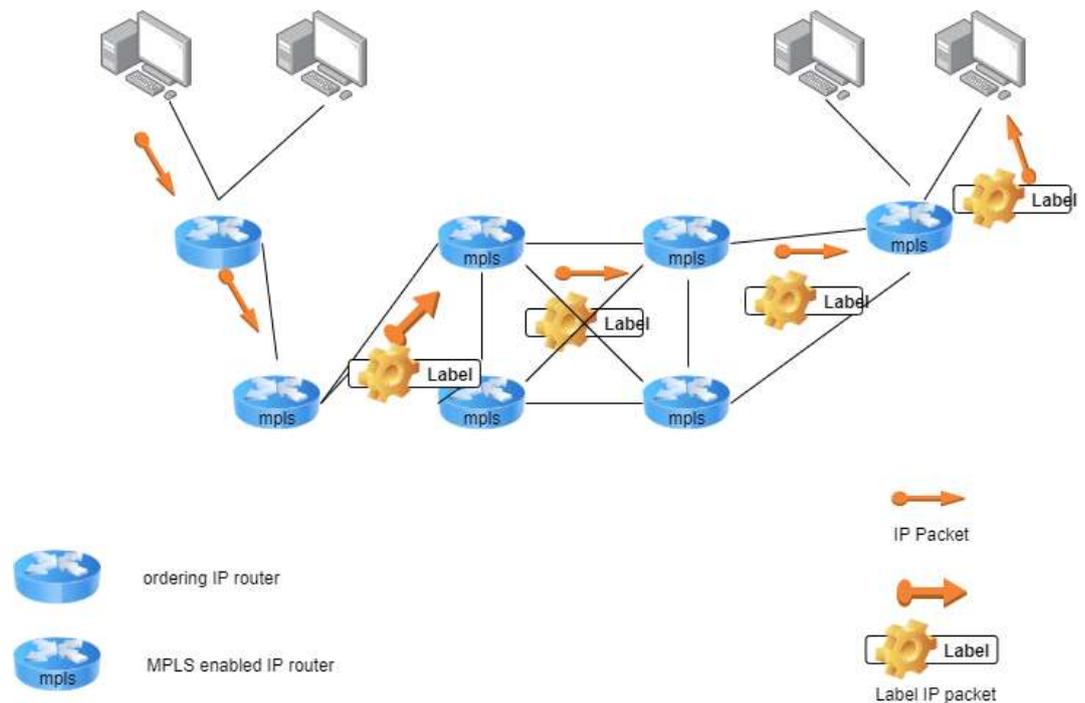
### 2.2.3 Penggunaan MPLS

Penggunaan MPLS sebagai berikut :

1. MPLS *Virtual Private Networks* (VPNs) - memberikan “MPLS- enabled IP networks” untuk koneksi Layer 3 dan Layer 2. Berisi 2 komponen utama yaitu layer 3 VPNs yang menggunakan Border Gateway Protocol dan layer 2 VPNs yang menggunakan *Any Transport over MPLS* (AToM).
2. MPLS *Traffic Engineering* (TE) - menyediakan peningkatan utilisasi dari bandwidth jaringan yang ada dan untuk “*protection services*”.
3. MPLS Quality of Service (QoS) - menggunakan mekanisme IP QoS existing, dan menyediakan perlakuan istimewa untuk type trafik tertentu, berdasarkan atribut QoS (seperti MPLS EXP).

#### **2.2.4 Cara Kerja Jaringan MPLS**

Jaringan MPLS terdiri dari rangkaian node-node yang bisa men- switch dan menroute berdasarkan label yang dipasang pada setiap paket. Domain MPLS terdiri dari serangkaian node MPLS yang saling menyambung. Node-node ini disebut *Label Switched Router* (LSR). Label- labelnya menentukan aliran paket diantara kedua endpoint (titik akhir). Jalur khusus melalui jaringan LSR untuk setiap alirannya yang disebut Forwarding Equivalence Class (FEC) telah ditentukan. MPLS adalah teknologi yang berorientasi sambungan. Setiap FEC memiliki karakterisasi lalu lintasnya yang menentukan persyaratan QoS untuk aliran tersebut. Karena LSR mengirim paket yang didasarkan pada nilai labelnya, maka proses pengirimannya lebih sederhana dari pada dengan router IP



**Gambar 2. 6** Cara kerja router dengan mpls

Sebelum paket dikirim, untuk paket-paket dalam FEC tertentu harus ditentukan terlebih dahulu jalurnya melalui jaringan yang disebut *Label Switched Path* (LSP). Selain itu yang harus ditentukan pula adalah parameter QoS-nya. Parameter QoS menentukan seberapa banyak sumberdaya yang diberikan kepada jalur tersebut dan kebijakan queuing (mengantri) dan discard (membuang) pada setiap LSR untuk FEC-nya. Untuk melakukan hal di atas itu dibutuhkan *protocol gateway interior* seperti OSPF untuk informasi *routing* dan *reachability*. Setiap paket dalam FEC diberikan label. Label ini hanya berlaku untuk lokal saja. Protokol seperti *Label Distribution Protocol* (LDP) atau RSVP dengan versi yang telah ditingkatkan digunakan untuk menentukan route dan nilai (angka) label. Ini bisa juga ditentukan secara manual oleh operator.

Paket masuk ke dalam domain MPLS melalui ingress edge LSR. Disinilah paket itu diolah untuk menentukan kebutuhannya akan layanan layer jaringan, yang mendefinisikan QoS-nya. LSR memberikannya kepada FEC tertentu dan LSP, lalu setelah itu pakatnya dikirimkan. Setiap LSR yang menerima paket berlabel mengambil label yang masuk dan memasang label yang keluar

pada paket tersebut, dan kemudian mengirimkan paket itu ke LSR berikutnya dalam LSP. Jalan ke luar (egress edge) LSR mengambil label tersebut, membaca header paket IP-nya, dan mengirimkan paket itu ke tujuan akhirnya.

Salah satu fitur MPLS yang paling penting adalah label stacking (penumpukan label). Paket yang telah diberi label bisa membawa banyak label yang disusun berdasarkan urutan last-in-first-out (yang terakhir masuk yang pertama keluar). Pengolahannya menurut label yang paling atas. Dalam setiap LSR-nya, label bisa ditambahkan pada tumpukannya (stack) atau diambil dari tumpukannya. Jadi dengan cara ini, kumpulan LSP bisa dibuat ke dalam satu LSP untuk bagian rute yang membentuk *tunnel*.

FEC untuk sebuah paket bisa ditentukan oleh satu atau lebih parameter, seperti sumbernya atau alamat tujuan IP, sumber atau point tujuan, IP protokol ID, code point layanan yang berbeda-beda atau label aliran IPv6. per-hop *behavior* (PHB) bisa ditentukan pada LSR untuk FEC. PHB menentukan prioritas *queuing* (antri atau urutan) paket untuk FEC ini serta kebijakan discard-nya. Paket yang dikirim ke end-point yang sama masuk kedalam FEC yang lain dan akan diberi label yang berbeda dengan PHB yang berbeda pula pada setiap LSR-nya dan bergerak di dalam jalur yang lain melalui jaringannya. Esensi dari fungsionalitas MPLS ini adalah bahwa lalulintas itu dikelompokkan ke dalam FEC-FEC. Lalulintas dalam sebuah FEC membawa domain MPLS sepanjang LSP. Setiap paket didalam FEC secara sendiri-sendiri merupakan bagian dari FEC tertentu dengan memiliki label lokalnya masing-masing.

Pemilihan rute mengacu kepada pemilihan LSP untuk FEC tertentu. MPLS mendukung routing hop-by-hop serta routing eksplisit. Dengan routing hop-by-hop ini, masing-masing LSP bebas memilih hop berikutnya untuk setiap FEC-nya. Pilihan ini menggunakan protokol routing biasa seperti OSPF. Ini memiliki beberapa kelebihan, tapi karena penggunaan metrik kinerjanya yang terbatas, routing hop-by hop tidak bisa langsung mendukung traffic engineering atau kebijakan yang berkaitan dengan QoS dan keamanan. Pada routing eksplisit satu LSR bisa menentukan beberapa atau seluruh LSR

di dalam LSP untuk sebuah FEC. Routing eksplisit memberikan semua keuntungan MPLS, termasuk kemampuan melakukan traffic engineering dan routing kegijakan. Routing eksplisit dinamis memberikan skop terbaik untuk traffic engineering. di dalam mode ini LSR yang menentukan LSP membutuhkan informasi tentang topologinya serta informasi yang berkaitan dengan QoS untuk domain MPLS. Versi OSPF yang telah ditingkatkan untuk MPLS memiliki sejumlah metrik yang lebih baru yang bisa digunakan dalam routing dengan hambatan termasuk link data rates maksimum, reservasi kapasitas saat itu, packet loss rate serta link propagation delay (keterlambatan penyebaran hubungan).

Dalam memilih rute ditentukan LSP-nya untuk FEC. Ada sebuah fungsi yang terpisah, yakni menentukan LSP yang sesungguhnya dan untuk ini masing-masing LSR pada LSP harus :

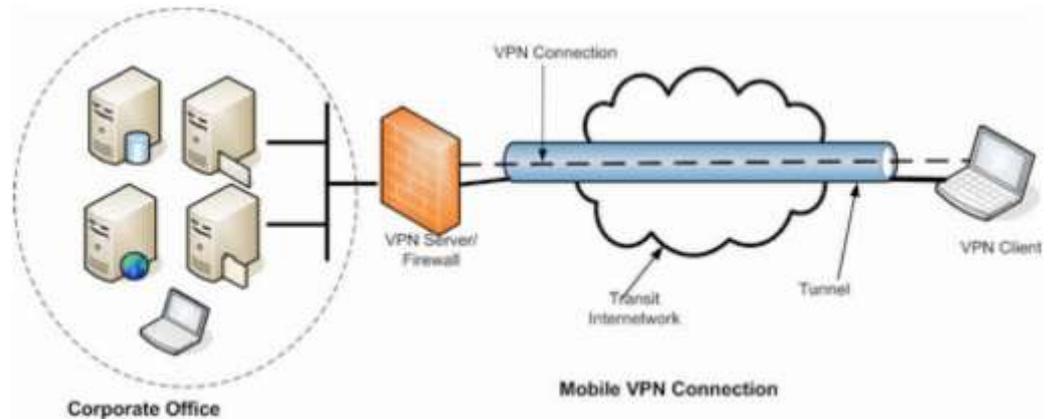
1. Memberikan label pada LSP yang akan digunakan untuk mengenali paket-paket yang masuk termasuk kedalam FEC-nya yang sesuai.
2. Memberitahukan node-node upstream (aliran hulu) yang potensial dari label yang diberikan oleh LSR ini kepada FEC-nya.
3. Mempelajari hop berikut untuk LSP ini serta label yang telah diberikan node down stream (aliran hilir) kepada FEC tersebut.

### **2.3 Virtual Privat Network (VPN)**

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan public dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

Dari cara pandang jaringan, salah satu masalah jaringan internet (IP public) adalah tidak mempunyai dukungan yang baik terhadap keamanan. Sedangkan dari cara pandang perusahaan, IP adalah kebutuhan dasar untuk melakukan pertukaran data antara kantor cabang atau dengan rekanan perusahaan. VPN muncul untuk mengatasi persoalan tersebut. Sebuah jaringan perusahaan

yang menggunakan infrastruktur IP untuk berhubungan dengan kantor cabangnya dengan cara pengalamatan secara private dengan melakukan pengamanan terhadap transmisi paket data.



**Gambar 2. 7 Jaringan VPN**

Teknologi VPN menyediakan tiga fungsi utama untuk penggunaannya. Ketiga fungsi utama tersebut antara lain sebagai berikut:

1. *Confidentially* (Kerahasiaan), Dengan digunakannya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melauinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah[8].
2. *Data Integrity* (Keutuhan Data), Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

3. Origin Authentication (Autentikasi Sumber), Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

#### **2.4 Aplikasi Monitoring Paket Data**

Untuk melakukan monitoring paket data diperlukan aplikasi monitoring yang cukup banyak tersedia dipasaran, baik yang bersifat komersil maupun gratis. Aplikasinya tersebut yaitu :

1. Ping

Merupakan aplikasi sederhana yang terdapat pada sistem operasi Windows maupun linux

2. Wireshark

Aplikasi GUI yang dapat melakukan sniffing paket data yang lewat dalam suatu jaringan komputer. Dengan *tool* ini dapat melihat secara detail informasi yang ada pada paket data.

#### **2.5 Simulator Jaringan**

Untuk mensimulasikan suatu jaringan komputer diperlukan alat atau aplikasi khusus yang dapat memperlihatkan topologi yang digunakan dan bisa memperlihatkan proses ping sebagai tanda sukses atau tidaknya paket data terkirim.

Beberapa aplikasi simulasi jaringan yaitu:

1. *Packet tracer*

*Cisco Packet Tracer* adalah sebuah software *simulator tools* jaringan cisco yang sering digunakan untuk latihan dan pembelajaran sebelum menggunakan perangkat aslinya, dan software ini dibuat langsung oleh

*Cisco Systems* disediakan secara gratis untuk siswa dan juga *network administrator*.

2. *iNetwork*

*iNetwork Simulator* adalah tool pembelajaran interaktif mengenai komunikasi jaringan (komputer). Program ini dikembangkan oleh Fakultas Teknik UTS (Universitas Teknologi Sidney, Australia).

3. *Boson Netsim*

*Boson Netsim* merupakan Router Simulator yaitu simulasi yang khusus untuk Router. peralatan yang ada disini yang pasti adalah Router, tersedia berbagai Series mulai dari Series 800, 1000, 1600 1700, 2500, 2600, 3600, 4500. Selain Router juga ada Switches tersedia berbagai Series diantaranya Series 1900, 2900, 3500. Untuk Connectornya yaitu Ethernet, Serial, ISDN. Selain itu masing masing pelatan dilengkapi dengan Informasi mengenai Class, Speed, Model.

4. GNS3

GNS3 (Graphic Network Simulator) adalah software simulasi jaringan komputer berbasis GUI yang mirip dengan Cisco Packet Tracer. Namun pada GNS3 memungkinkan simulasi jaringan yang kompleks, karena menggunakan operating system asli dari perangkat jaringan seperti cisco dan juniper. Sehingga kita berada kondisi lebih nyata dalam mengkonfigurasi router langsung daripada di Cisco Packet Tracer. GNS3 adalah alat pelengkap yang sangat baik untuk laboratorium nyata bagi network engineer, administrator dan orang-orang yang ingin belajar untuk sertifikasi seperti Cisco CCNA, CCNP, CCIP dan CCIE serta Juniper JNCIA, JNCIS dan JNCIE.