BAB 2
TINJAUAN PUSTAKA

2.1 Profil Tempat Penelitian

Profil tempat penelitian yang akan dibahas pada subbab ini meliputi sejarah instansi, visi dan misi instansi, logo instansi, badan hukum instansi dan struktur organisiasi dan deskripsi pekerjaan.

2.1.1 Sejarah Instansi

Institut Teknologi Bandung (ITB), didirikan pada tanggal 2 Maret 1959. Kampus utama ITB saat ini merupakan lokasi dari sekolah tinggi teknik pertama di Indonesia. Walaupun masing-masing institusi pendidikan tinggi yang mengawali ITB memiliki karakteristik dan misi masing-masing, semuanya memberikan pengaruh dalam nperkembangan yang menuju pada pendirian ITB.

Sejarah ITB bermula seja awal abad kedua puluh, atas prakarsa masyarakat penguasa waktu itu. Gagasan mula pendirianya terutama dimaksudkan untuk memenuhi kebutuhan tenaga teknik yang menjadi sulit karena terganggunya hubungan antara negeri Belanda dan wilayah jajahannya di kawasan Nusantara, sebagai akibat pecahnya Perang Dunia Pertama. *De Techniche Hoogeschool te Bandung* berdiri tanggal 3 Juli 1920 dengan satu fakultas *de Faculteit van Technische Wetenschap* yang hanya mempunyai satu jurusan *de afdeeling der Weg en Waterbouw*.

Didorong oleh gagasan dan keyakinan yang dilandasi semangat **perjuangan** Proklamasi Kemerdekaan serta wawasan ke masa depan, Pemerintah Indonesia meresmikan berdirinya Institut Teknologi Bandung pada tanggal 2 Maret 1959 . Berbeda dengan harkat pendirian lima perguruan tinggi teknik sebelumnya di kampus yang sama, Institut Teknologi Bandung lahir dalam suasana penuh dinamika mengemban misi pengabdian ilmu pengetahuan dan teknologi, yang berpijak pada kehidupan nyata di bumi sendiri bagi kehidupan dan pembangunan bangsa yang maju dan bermartabat.

Kurun dasawarsa pertama tahun 1960-an ITB mulai membina dan melengkapi dirinya dengan kepranataan yang harus diadakan. Dalam periode ini dilakukan persiapan pengisian-pengisian organisasi bidang pendidikan dan pengajaran, serta melengkapkan jumlah dan meningkatkan kemampuan tenaga pengajar dengan penugasan belajar ke luar negeri.

Kurun dasawarsa kedua tahun 1970-an ITB diwarnai oleh masa sulit yang timbul menjelang periode pertama. Satuan akademis yang telah dibentuk berubah menjadi satuan kerja yang juga berfungsi sebagai satuan sosial-ekonomi yang secara terbatas menjadi institusi semi-otonomi. Tingkat keakademian makin meningkat, tetapi penugasan belajar ke luar negeri makin berkurang. Sarana internal dan kepranataan semakin dimanfaatkan.

Kurun dasawarsa ketiga tahun 1980-an ditandai dengan kepranataan dan proses belajar mengajar yang mulai memasuki era modern dengan sarana fisik kampus yang makin dilengkapi. Jumlah lulusan sarjana makin meningkat dan program pasca sarjana mulai dibuka. Keadaan ini didukung oleh makin membaiknya kondisi sosio-politik dan ekonomi negara.

Kurun dasawarsa keempat tahun 1990-an perguruan tinggi teknik yang semula hanya mempunyai satu jurusan pendidikan itu, kini memiliki dua puluh enam Departemen Program Sarjana, termasuk Departemen Sosioteknologi, tiga puluh empat Program Studi S2/Magister dan tiga Bidang Studi S3/Doktor yang mencakup unsur-unsur ilmu pengetahuan, teknologi, seni, bisnis dan ilmu-ilmu kemanusiaan.

Dasawarsa ini akan menghantarkan ITB ke fajar abad baru yang ditandai dengan munculnya berbagai gagasan serta pemikiran terbaik untuk pengembangannya. Beberapa diantaranya antara lain:

Bahwa cepatnya pelipatgandaan informasi di abad baru akan menuntut pelaksanaan pendidikan yang berpercepatan, tepat waktu, terpadu, berkelanjutan, dan merupakan upaya investasi terbaik. Dalam upaya ini ITB ingin menegakkan Program Sarjana di atas pondasi penguasaan ilmu-ilmu dasar yang kokoh sehingga lulusannya senantiasa mampu menyesuaikan diri terhadap perubahan-perubahan yang datang

dengan cepat. Program Pasca Sarjana menjadi ujung tombak peningkatan kualitas dan kuantitas, efisiensi dan efektivitas, serta relevansinya terhadap kebutuhan, sehingga kontribusi ITB bagi pembangunan nasional akan menjadi lebih besar dan tinggi nilainya.

Bahwa penguasaan dan pengembangan ilmu pengetahuan dan teknologi perlu dilakukan secara utuh dan terpadu, dalam suatu kiprah **sebagai** Research and Development University**.** Pengembangan keilmuan dan teknologi di ITB didasarkan pada kebutuhan untuk menunjang pelaksanaan pembangunan bangsa. Dengan demikian ITB akan mengembangkan dirinya dalam riset dan manufaktur, teknologi komunikasi dan informasi, transportasi darat-laut dan dirgantara, lingkungan, serta bio-teknologi dan biosains.

Bahwa misi pengabdian kepada masyarakat diharapkan dapat membangun wawasan bisnis untuk kemandirian yang merupakan modal awal untuk menegakkan otonomi perguruan tinggi. Wawasan bisnis untuk kemandirian tersebut diarahkan guna meraih prestasi pelaksanaan kewajiban dan tugas pendidikan dan penelitian setinggi-tingginya.

Bahwa pengembangan ITB diharapkan berpijak pada kekuatan institusi berupa penggunaan informasi sebaik-baiknya, terpeliharanya Staf Pengajar yang kompeten yang tinggi mutu kemampuan dan pengabdiannya, sistem pendidikan yang terintegrasi, dan kerjasama yang terjalin erat dengan pemerintah, industri dan lembaga penelitian dan pendidikan di dalam dan luar negeri. Sehingga pengembangan yang direncanakan dapat dipantau secara berkelanjutan dan terukur menurut pelaksanaan tridharma perguruan tinggi, pengembangan sumber daya manusia, sarana fisik, kepranataan norma dan tata kerja, serta ekonomi, sosial budaya dan keamanan. [7]

Bahwa keinginan untuk mengembangkan ITB terungkap dengan semangat dan sikap ITB yang mengakui adanya kebenaran keilmuan, kebenaran keilmuan yang dapat didekati melalui observasi disertai analisis yang rasional. Bahwasanya mengejar dan mencari kebenaran ilmiah tersebut adalah hak setiap insan di bumi, dan ilmu

pengetahuan serta teknologi agar dimanfaatkan sebesar-besarnya untuk mensejahterakan umat manusia, dan masyarakat bangsa Indonesia pada khususnya.

Kurun dasawarsa kelima tahun 2000-an Institut Teknologi Bandung yang status hukumnya sebagai instansi pemerintah dalam bentuk jawatan negeri pada tanggal 26 Desember 2000, Pemerintah melalui Peraturan Pemerintah No. 155 tahun 2000 telah menetapkan Institut Teknologi Bandung sebagai suatu Badan Hukum Milik Negara.

Dalam menunjang kegiatan belajar mengajar ITB mendirikan DitSTI (Direktorat Sitem Teknologi dan Infromasi) sebagai penanggung jawab layanan IT dan pengembangan IT dilingkungan kampus ITB. Direktorat Sistem Teknologi dan Informasi Institut Teknologi Bandung (DitSTI ITB) adalah Direktorat yang bertugas sebagai penyelarasan Sistem dan Teknologi Informasi dengan proses bisnis dilingkungan ITB, melakukan dan bertanggung jawab segala hal tentang layanan IT yang ada di lingkungan ITB seperti email, internet, system informasi ITB, aplikasi online ITB, hosting, VPN dan proxy.

2.1.2 Visi dan Misi Instansi

Visi adalah suatu pandangan tentang perusahaan dan tujuan suatu perusahaan dan apa yang harus dilakukan untuk mencapai tujuan tersebut pada masa yang akan datang. Misi adalah pernyataan tentang apa yang harus dikerjakan oleh lembaga dalam usahanya mewujudkan visi. [8]

Visi instansi Institut Teknologi Bandung (ITB) berdasarkan keputusan adalah Menjadi Perguruan Tinggi yang unggul, bermartabat, mandiri, dan diakui dunia serta memandu perubahan yang mampu meningkatkan kesejahteraan bangsa Indonesia dan dunia. (Sumber: 09/SK/I1-SA/OT/2011).

Misi instansi Institut Teknologi Bandung (ITB) berdasarkan keputusan adalah Menciptakan, berbagi dan menerapkan ilmu pengetahuan, teknologi, seni dan kemanusiaan serta menghasilkan sumber daya insani yang unggul untuk menjadikan Indonesia dan dunia lebih baik. (Sumber: 09/SK/I1-SA/OT/2011). [9]

2.1.3 Logo Instansi

Logo adalah suatu identitas yang dipergunakan untuk menggambarkan citra dan karakter suatu lembaga, perusahaan atau organisasi. Berikut adalah gambar 2.1 tentang logo instansi dari ITB:



Gambar 2. 1 Logo Instansi

Berdasarkan Gambar 2.1 tentang logo instansi ITB mempunyai arti lambang sebagai berikut:

1.	Kapak	:	Lambang Sifat Ksatria.
2.	Cawan	:	Lambang sumber ilmu pengetahuan yang tiada habisnya.
3.	Gading (Patah	:	Lambang pengorbanan diri untuk menyelesaikan masalah yang merintangi kemajuan ilmiah.
4.	Tasbih	:	Lambang kebijaksanaan.
5.	Selendang	:	Lambang kesucian.
6.	Buku	:	Lambang keilumuan.

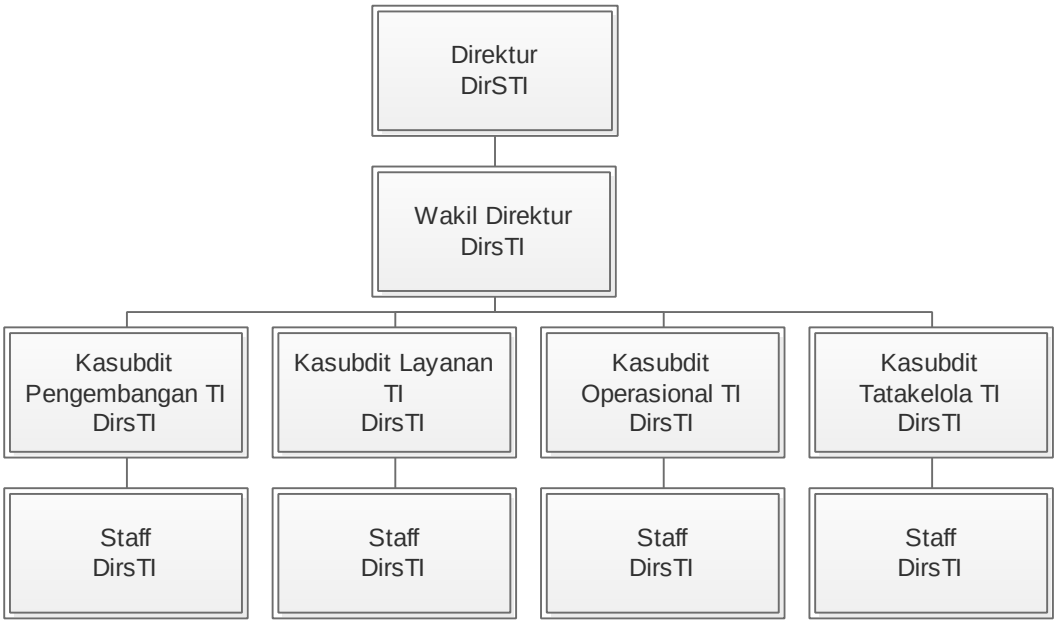
2.1.3 Badan Hukum Instansi

Perguruan Tinggi Negeri dengan status Badan Hukum adalah sesuatu tanpa preseden dalam sejarah Pendidikan Tinggi di Indonesia. Hal ini diawali dengan terbitnya PP No. 61 tahun 1999 tentang Penetapan Perguruan Tinggi Negeri sebagai Bahan Hukum yang kemudian disusul diterbitnya PP No. 155 tahun 2000 tentang

Penetapan Institut Teknologi Bandung menjadi Bahan Hukum Milik Negara. Maka dengan terbitnya PP 155 tersebut, sejak tanggal 26 Desember 2000 yang lalu ITB resmi menjadi Badan Hukum sebagaimana layaknya badan hukum lainnya yang dibenarkan melaksanakan segala perbuatan hukum yang tidak melanggar hukum serta peraturan perundang-undangan yang berlaku. Pertimbangan pertama yang ditinjau dalam PP No. 61 secara singkat adalah adanya globalisasi yang menimbulkan persaingan yang tajam. Maka untuk meningkatkan daya saing nasional dibutuhkan PT yang dapat membangun masyarakat madani yang demokratis dan mampu bersaing secara global. Untuk itu PT, termasuk ITB, harus memperoleh kemandirian, otonomi dan tanggung jawab yang lebih besar. Penekannya ada pada adanya proses globalisasi [7].

2.1.4 Struktur Oraganisasi dan Deskripsi Pekerjaan

Direktorat Sistem Teknologi dan Informasi (DirSTI) mempunyai struktur organisasi untuk mencapai tugas dan tanggung jawab yang diberikan, pada struktor organisasi ini dibagi berbagai macam divisi, berikut adalah gambar 2.2 struktur organisasi DirSTI:



Gambar 2.2 Struktur Organisasi DirSTI

berdasarkan gambar 2.2 Sturktur Organisasi DirSTI, adapun jobdesk dari tiap struktur organisasi diatas adalah sebagai berikut:

1. Direktur : Mempunyai tugas pokok memimpin, memantau dan mengkoordinasikan kegiatan kerja kepada masing-masing Kasubdit TI, dan juga melakukan koordinasi kerja dengan direktorat lain atau fakultas lain.
2. Wakil Direktur : Membantu pekerjaan Direktur dan sebagai tambahannya mengkoordinasikan tugas kerja dengan pihak ke 3 universitas lain atau perusahaan lain untuk mengembangkan TI di ITB.
3. Kasubdit Pengembangan TI : Mempunyai tugas pokok sebagai pemimpin dalam bidang pengembangan TI di ITB, seperti development teknologi baru dan layanan baru yang akan diimplementasi.
4. Kasubdit Layanan TI : Mempunyai tugas pokok sebagai pemimpin dalam bidang layanan yang disediakan DirSTI, membuat aturan untuk layanan sesuai standar ISO.
5. Kasubdit Operasional TI : Mempunyai tugas pokok sebagai pemimpin dalam bidan operasional contohnya memantu kinerja perangkat jaringan dan server yang ada di lingkungan ITB.
6. Kasubdit Tatakelola TI : Mempunyai tugas pokok sebagai pemimpin untuk melaksanakan, mengelola kepegawaian, menyusun rencana kegiatan dan anggaran

DirSTI dalam memaksimalkan kinerja perusahaan

2.2 Landasan Teori

Pada subbab ini akan dibahas beberapa landasan teori antara lain jaringan komputer, topologi jaringan, OSI Layer, TCP/IP *(transmission control protocol/internet protocol)*, IPv4, IPv6, BGP, OSPF, MPLS, Metode PDIOO.

2.2.1 Jaringan Komputer

Jaringan komputer adalah sekelompok komputer otonom yang dihubungkan satu dengan yang lainnya menggunakan protocol komunikasi melalui media transmisi atau media komunikasi sehingga saling berbagi data informasi, program-program, share peranagkat keras seperti printer atau hardisk. Tujuan dibangunnya suatu jaringan komputer adalah membawa data informasi dari sisi pengirim menuju penerima secara cepat dan tepat tanpa adanya kesalahan melalui media transmisi atau media komunikasi.

2.2.1.1 Jenis Jaringan Komputer

Jaringan komputer yang digunakan saat ini dapat dikelompokkan berdasarkan area yang dapat dijangkau. Area ini mulanya ditentukan berdasarkan jarak jangkau dalam satuan meter. Namun dalam perkembangan selanjutnya berdasarkan peralatan dan fasilitas. Penggunaan peralatan–peralatan yang dimaksud adalah peralatan–peralatan *internet* jaringan seperti *repeater, Router* atau *gateway* dari peralatan tersebut dapat dilihat jangkauan area jaringan dan luasan segmen jaringan yang dibangun.

Berdasarkan kriteria–kriteria tersebut secara umum jaringan komputer dapat digolongkan sebagai Berikut ini merupakan:

1. *Local Area Network (LAN)*

Sebuah LAN adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya sekitar 1 km persegi.. Komputerkomputer yang terhubung ke dalam jaringan itu biasanya disebut dengan *workstation.* Kebanyakan LAN menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya.

2. Metropolitan Area Network (MAN)

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

3. Wide Area Network (WAN)

Biasanya WAN agak rumit dan sangat kompleks, menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN ke dalam komunikasi global seperti Internet. Tapi bagaimanapun juga antara LAN, MAN dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu diantara yang lainnya. beberapa menit. Biasanya WAN agak rumit dan sangat kompleks, menggunakan

Banyak sarana untuk menghubungkan antara LAN dan WAN ke dalam komunikasi global seperti Internet. Tapi bagaimanapun juga antara LAN, MAN dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu diantara yang lainnya.

4. Wireleess Network

Wireless Network merupakan peralatan *end-user* untuk megakses jaringan dengan menggunakan transmisi radio pendek atau sedang. *Wireless* WAN : GSM (sampai 20 Kbps) *Wireless* LAN/MAN : WaveLAN (2-11 Mbps, sampai 150 m) *Wireless* PAN (*Personal Area Network*) : *Bluetooth (*sampai 2 Mbps, jarak < 10 m*)*

Tabel 2. 1 Susunan Jaringan Komputer menurut Jarak

	Range	***Bandwidth* (Mbps)**	**Latency (ms)**

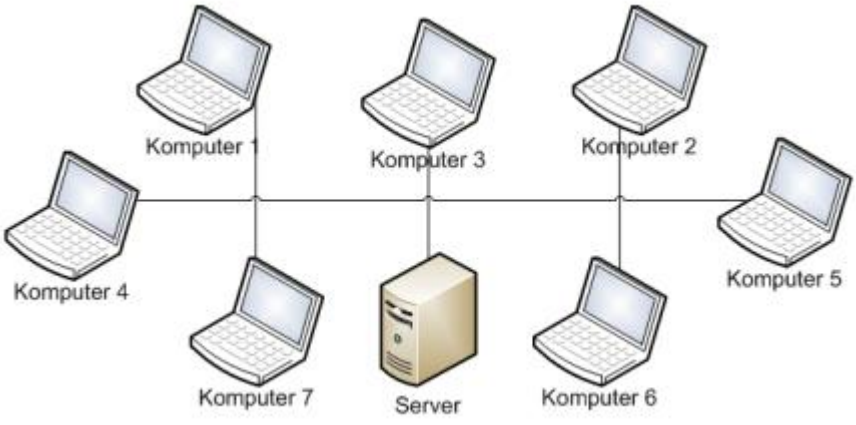
LAN	1-2 kms	10-1000	1-10 ms
WAN	*Worldwide*	0.010-600	100-50 ms
MAN	2-50 kms	1-150	10 ms
Wireless LAN	0.15-1.5 km	2-11	5-20 ms
Wireless WAN	*Worldwide*	0.010-2	100-500 ms
Internet	*Worldwide*	0.010-2	100-500

2.2.2 Topologi Jaringan

Topologi jaringan merupakan suatu struktur atau bagaimana menghubungkan antara simpul dan pusat dalam suatu jaringan. Tiap struktur mempunyai keuntungan dan kerugiannya masing-masing. Bentuk-bentuk arsitektur jaringan komputer secara fisik adalah sebagai Berikut ini merupakan:

1. Topologi Bus

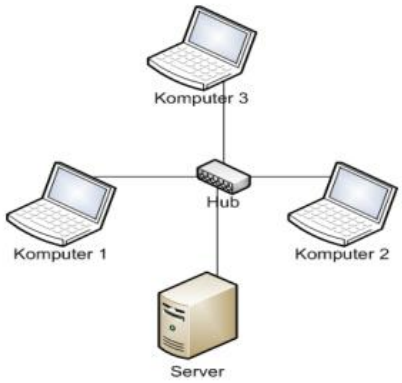
Topologi sebuah bus merupakan garis lurus yang terdiri dari satu jalur kabel utama (*backbone*) dimana pada masing-masing ujungnya diberikan sebuah *terminator*. Semua *nodes* pada jaringan (*file server, workstation*, dan perangkat lainnya) terkoneksi ke sebuah kabel utama. Jaringan-jaringan *Ethernet* dan *Localtalk* menggunakan topologi *linear* ini.



Gambar 2. 2 Topologi Bus

2. Topologi Star

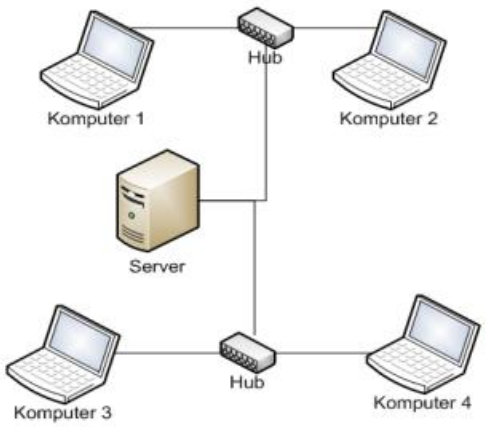
Topologi model ini didesain dimana setap *node* (*file server*, *workstation*, dan perangkat lainnya) terkoneksi ke jaringan melewati sebuah *concentrator* baik berupa *HUB* ataupun *SWITCH*. Data yang terkirim ke jaringan akan melewati *concentrator* sebelum melanjutkan ke tempat tujuannya. *Concentrator* akan mengatur dan mengontrol keseluruhan fungsi jaringan. Dia juga bertindak sebagai *repeater* dalam skala kecil dari aliran data. Konfigurasi pada jaringan model ini menggunakan kabel *Twisted Pair*.



Gambar 2. 3 Topologi star

3. Topologi Tree

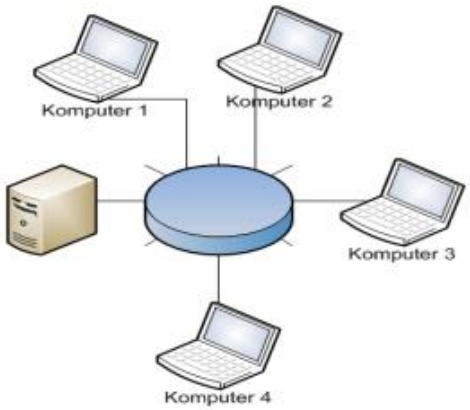
Sebuah topologi model ini merupakan perpaduan antara topologi *Linear BUS* / Garis Lurus dan Bintang, yang terdiri dari kelompok-kelompok dari *workstation* konfigurasi Bintang yang terkoneksi ke kabel utama yang menggunakan topologi *Linear BUS* / Garis Lurus. Topologi ini memungkinkan untuk pengembangan jaringan yang telah ada, dan memungkinkan sebuah perusahaan mengkonfigurasi jaringan sesuai dengan kebutuhannya. Adapun contoh gambarnya seperti berikut:



Gambar 2. 4 Topologi Tree

4. Topologi Ring

Dalam topologi *Ring* semua *workstation* dan *server* dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Tiap *workstation* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain, bila alamat- alamat yang dimaksud sesuai maka informasi diterima dan bila tidak informasi akan dilewatkan. [10]

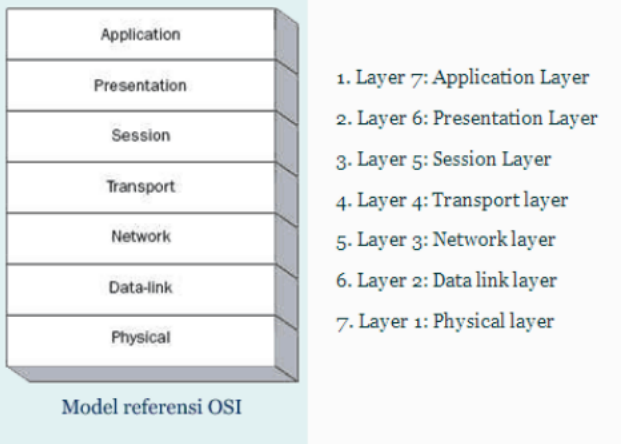


Gambar 2. 5 Topologi Ring

2.2.3 OSI Layer

OSI (Open System Interconeection) model adalah alat referensi untuk memahami komunikasi data antara dua network system. Komunikasi ini dibagi menjadi kedalam 7 layer proses. Setiap layer mempunya tugas masing-masing yang fungsinya untuk mendukung layer diatasnya dan memberikan layanan ke layer dibawahnya. 3 layer terbawah focus untuk mengirimkan traffic melewati jaringan ke *end system* . 4 layer teratas mempunyai peran pada sisi *end system* untuk menyelesaikan proses. [11]

OSI yang merupakan model referensi dan bukan suatu model fisik membagi tugas-tugas jaringan kedalam 7 *layer*.



Gambar 2. 6 Model Referensi OSI

a. Lapisan Fisik

Lapisan fisik (*physical layer*) merupakan dasar semua jaringan di dalam model referensi OSI yang mana merupakan karakteristik perangkat keras yang fungsinya untuk mentransmisikan sinyal data baik itu data analog maupun data digital. Selain itu *physical layer* juga merupakan sarana sistem untuk mengirimkan data ke perangkat lain yang terhubung di dalam suatu jaringan komputer.

Lapisan fisik (*physical layer*) adalah lapisan terbawah dari model referensi OSI, di mana lapisan ini berfungsi untuk menentukan karakteristik dari kabel yang

digunakan untuk menghubungkan komputer dalam jaringan. Pada sisi *transmitter*, lapisan fisik menerapkan fungsi elektris, mekanis dan prosedur untuk membangun, memelihara dan melepaskan sirkuit komunikasi guna mentranmisikan informasi dalam bentuk digit binear ke sisi *receiver*. Sedangkan lapisan fisik pada sisi *receiver* akan menerima data dan mentransmisikan ke lapisan atasnya. [12]

b. Lapisan *Data-link*

Lapisan *data-link* (*data-link layer*) merupakan lapisan kedua dari standar *OSI*. Tugas utama *data-link layer* adalah sebagai fasilitas transmisi *raw* data dan mentransformasi data tersebut ke saluran yang bebas dari kesalahan transmisi. Sebelum diteruskan ke *network* layer, *data-link layer* melaksanakan tugas ini dengan memungkinkan pengirim memecah-mecah data *input* menjadi sejumlah data *frame* (biasanya berjumlah ratusan atau ribuat byte).

Kemudian *data-link layer* mentransmisikan *frame* tersebut secara berurutan dan memproses *acknowledgement* frame yang dikirim kembali oleh penerima. Karena *physical layer* menerima dan mengirim aliran bit tanpa mengindah arti atau arsitektur *frame*, maka tergantung pada *data-link layer*-lah untuk membuat dan mengenali batas-batas frame itu. Hal ini bisa dilakukan dengan cara membubuhkan bit khusus ke awal dan akhir *frame*. [12]

c. Lapisan *Network*

Lapisan jaringan (*Network layer*) merupakan lapisan ketiga dari standar *OSI* yang berfungsi untuk menangani masalah jaringan komunikasi secara rinci. Pada lapisan ini, data yang berupa pesan-pesan (*message*) akan dibagi-bagi dalam bentuk paket-paket data yang dilengkapi dengan *header-header* tertentu pada setiap paket data tersebut.

Network layer ini berfungsi untuk mengambil paket dari sumber dan mengirimkannya ke tujuan. Supaya sampai ditujuan perlu banyak dibuat *hop* pada *Router-Router* perantara di sepanjang lintasannya. Fungsi layer ini sangat kontras dengan fungsi *data-link layer*, yang memiliki tujuan lebih sederhana cukup memindahkan *frame* dari ujung kabel yang satu ke ujung yang lainnya. Jadi

network layer ini merupakan layer *terbawah* yang berkaitan dengan transmisi *end to end*.

Secara umum , lapisan jaringan menyediakan beberapa layanan antara lain : pengendalian operasi subnet , pemilihan rute , dan *internetworking*. [12]

d. Lapisan *Transport*

Transoprt layer merupakan lapisan keempat dari model referensi OSI dan jantung dari hirarki protokol secara keseluruhan. Tugas *layer* ini menyediakan data *trasnport* yang bisa diandalkan dan efektif biayanya dari komputer sumber ke komputer tujuan, yang tidak tergantung pada jaringan fisik atau jaringan-jaringan yang digunakan. Tanpa *transport* layer, seluruh konsep protokol yang menggunakan *layer* tidak akan ada gunanya.

Layer atau lapisan ini yang mengatur koneksi dari satu ujung ke ujung yang lain atau dari komputer pengirim ke komputer penerima dan juga yang membangun koneksi logika antara *host* pengirim dengan penerima dalam jaringan. Layer ini jugalah yang mengatur dan mengimplementasikan layanan *transport* yang handal antar jaringan yang transparan untuk *layer-layer* di atasnya (*upper layer*). Fungsi dari layer ini meliputi *error checking* dan *recovery*. [12]

e. Lapisan Sesi

Lapisan sesi atau *session layer* merupakan lapisan ke lima dari model referensi *OSI* . Lapisan ini menerapkan suatu mekanisme kontrol dialog antara dua aplikasi. Di samping itu, lapisan ini menyediakan sarana untuk membangun hubungan komunikasi antara dua program aplikasi dan menggunakanya.

Beberapa protokol yang terdapat pada layer ini adalah *NETBIOS, NETBEUI* (NETBIOS *Extended User Interface*) dan *PAP* (*Printer Access Protokol*). *NETBIOS* merupakan suatu session interface dan protokol, dikembangkan oleh IBM, yang menyediakan layanan ke *presentation layer* dan *application layer*. *NETBEUI* merupakan suatu pengembangan dari *NETBIOS* yang digunakan pada produk *Microsoft Networking*, seperti Windows NT dan *LAN Manager ADSP*

(*AppleTalk Data Stream Protokol*). Sedangkan *PAP* Terdapat pada printer *Postscript* untuk akses pada jaringan *Apple Talk*. [12]

f. Lapisan Presentasi

Presentation layer merupakan lapisan ke-enam dari model referensi OSI. *Presentation layer* melakukan fungsi-fungsi tertentu yang diminta untuk menjamin pen-muan sebuah penyelesaian umum bagi masalah. Tidak seperti *layer-layer* di bawahnya yang hanya melakukan pemindahan bit dari satu tempat ke tempat lainnya, *presentation layer* memperhatikan sintaks dan semantik informasi yang dikirimkan.

Lapisan ini berhubungan dengan sintaks data yang dipertukarkan diantara entitas aplikasi. Tujuannya adalah untuk mengatasi masalah perbedaan format penyajian data. Lapisan ini mendefinisikan sintaks yang digunakan antar entitas aplikasi. [12]

g. Lapisan Aplikasi

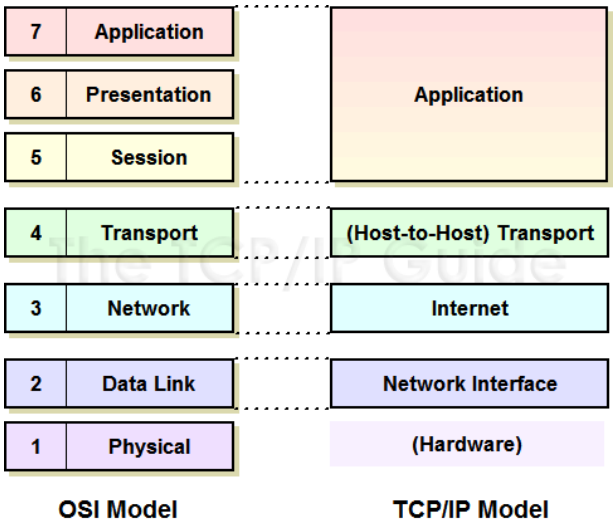
Lapisan paling atas dari lapisan *OSI* yaitu lapisan aplikasi (*Application layer*). Protokol pada lapisan ini secara langsung melayani pemakai dengan memberikan pelayanan informasi yang tersebar yang berhubungan dengan aplikasi-aplikasi dan pengelolaannya. Sering disebut fungsi juga sebagai program aplikasi yang digunakan pada jaringan contohnya *electronic email(SMTP), file transfer program(FTP)* .

Application layer terdiri dari bermacam-macam protokol. Misalnya terdapat ratusan jenis terminal yang tidak kompatibel di seluruh dunia. Ambil keadaan dimana editor layar penuh yang diharapkan bisa bekerja pada jaringan bermacam-macam terminal, yang masing-masing memiliki layout layar yang berlainan, mempunyai cara urutan penekanan tombol yang berbeda untuk penyisipan dan penghapusan teks, memindahkan sensor dan sebagainya. [12]

2.2.4 TCP/IP Layer

Pada tahun 1970 dan 1980 agensi pemerintah U.S menyadari tentang potensial dan pentingnya teknologi internet dan akhirnya membuat pusat research namanya DARPA *(Defanse Advance Research Project Agency).* DARPA membuat standarisasi jaringan yang menspesifikasikan secara detail bagimana sebuah komputer berkomunikasi, mem*forwardkan traffic* yang dinamakan TCP/IP, dengan TCP/IP ini komunikasi dapat dilakukan dengan interkoneksi jaringan, contohnya menghubungkan beberapa gedung, menghubungkan beberapa kampus. [13]

TCP/IP dibagi menjadi beberapa layer untuk mendefenisikan tugasnya sama seperti OSI Layer namun pada TCP/IP layer dipersingkat.



Gambar 2. 7 Perbandingan OSI dan TCP/IP

TCP/IP mempunyai 5 lapisan, yaitu:

a. Lapisan Fisik

Physical Layer (lapisan fisik) merupakan lapisan terbawah yang mendefinisikan besaran fisik seperti media komunikasi, tegangan, arus, dan sebagainya. Lapisan ini dapat bervariasi bergantung pada media komunikasi pada jaringan yang bersangkutan. *TCP/IP* bersifat fleksibel sehingga dapat mengintegralkan mengintegralkan berbagai jaringan dengan media fisik yang berbeda-beda.

b. Lapisan *Network Access*

Network Access Layer mempunyai fungsi yang mirip *dengan Data Link* layer pada *OSI*. Lapisan ini mengatur penyaluran data *frame-frame* data pada media fisik yang digunakan secara handal. Lapisan ini biasanya memberikan servis untuk deteksi dan koreksi kesalahan dari data yang ditransmisikan. Beberapa contoh protokol yang digunakan pada lapisan ini adalah X.25 jaringan publik, Ethernet untuk jaringan Etehernet, AX.25 untuk jaringan Paket Radio dsb.

c. Lapisan *Internet*

Internet Layer mendefinisikan bagaimana hubungan dapat terjadi antara dua pihak yang berada pada jaringan yang berbeda seperti *Network Layer* pada *OSI*. Pada jaringan Internet yang terdiri atas puluhan juta *host* dan ratusan ribu jaringan lokal, lapisan ini bertugas untuk menjamin agar suatu paket yang dikirimkan dapat menemukan tujuannya dimana pun berada. Oleh karena itu, lapisan ini memiliki peranan penting terutama dalam mewujudkan *internetworking* yang meliputi wilayah luas (*worldwide Internet*).

d. Lapisan *Transport*

Transport Layer mendefinisikan cara-cara untuk melakukan pengiriman data antara *end to end host* secara handal. Lapisan ini menjamin bahwa informasi yang diterima pada sisi penerima adalah sama dengan informasi yang dikirimkan pada pengirim. Pada *TCP/IP*, protokol yang dipergunakan adalah *Transmission Control Protocol (TCP)* atau *User Datagram Protocol (UDP). TCP* dipakai untuk aplikasi-aplikasi yang membutuhkan keandalan data, sedangkan *UDP* digunakan untuk aplikasi yang membutuhkan panjang paket yang pendek dan tidak menuntut keandalan yang tinggi.

e. Lapisan Aplikasi

Application Layer merupakan lapisan terakhir dalam arsitektur *TCP/IP* yang berfungsi mendefinisikan aplikasi-aplikasi yang dijalankan pada

jaringan. Karena itu, terdapat banyak protokol pada lapisan ini, sesuai dengan banyaknya aplikasi *TCP/IP* yang dapat dijalankan. [12]

2.2.5 IPv4 *Address*

Tiap komputer dalam TCP/IP diberikan alamat binary yang *uique* yang disebut dengan internet protocol address atau ip address. IPv4 address menggunakan 32-bit address yang dibagi menjadi 2 bagian utama yaitu prefix yang mengidentifikasi komputer tersebut terhubung ke network mana dan suffix yang yang memeberikan unique identifier pada komputer di network tersebut [13] .Dalam perkembangannya ip address ini dibagi menjadi 2 versi yaitu IPv4 dan IPv6 untuk menjamin setiap host yang terhubung ke internet menggunakan *unique address.*

IPv4 merupakan IP *address* yang terdiri dari 32 bit dan memiliki 4 segmen, masing-masing segmen memiliki ukuran sebesar 8 bit menggunakan angka biner dan dipresentasikan dalam notasi desimal bertitik (*dotted-decimal notation*). Namun dalam penulisan alamat IP umumnya, alamat IP dengan angka biner dikonversikan menjadi angka desimal agar memudahkan dalam pengimplementasian. Seperti pada Tabel 2.1 [13].

Tabel 2. 1 Penulisan IP address dengan bilangan biner dan decimal

Bilangan	Oktet ke-1	Oktet ke-2	Oktet ke-3	Oktet ke-4
Biner	01100100	00000011	00000001	01100100
Desimal	100	3	1	100

IPv4 dibagi dalam beberapa kelas yaitu kelas A,B,C,D dan E. Tabel 2.2 menunjukan pembagian kelas dalam IPv4 beserta dengan kegunaan dari setiap kelasnya. Seperti pada Tabel 2.2.

Tabel 2. 2 Pembagian kelas dalam IPv4

Kelas IP	Oktet Pertama (Dalam Desimal)	Digunakan Untuk
A	1-126	Alamat IP untuk jaringan dengan skala besar
B	128-191	Alamat IP untuk jaringan dengan skala menengah hingga skala besar
C	192-223	Alamat untuk jaringan yang kecil
D	224-239	Alamat *multicast*
E	240-255	Direservasikan, umumnya digunakan sebagai alamat percobaan

a. IP *Address* Private

IP *address* privat adalah IP address yang digunakan hanya sebagai identifikasi komputer pada jaringan komputer yang bersifat privat. Terdapat 3 blok IP address yang termasuk kedalam IP address privat. Seperti pada Tabel 2.3.

Tabel 2. 3 IP address privat

Kelas IP	Blok IP	*Range*
A	10.0.0.0/8	10.0.0.0 – 10.255.255.255
B	172.16.0.0/12	172.16.0.0 – 172.31.255.255
C	192.168.0.0/16	192.168.0.0 – 192.168.255.255

b. IP *Address* Publik

IP address publik merupakan alamat-alamat yang dapat diakses melalui jaringan publik atau jaringan internet dan bersifat unik yang berarti tidak ada host yang memiliki IP address publik yang sama. [12]

2.2.6 IPv6 Address

Masalah dengan IP apada modern internetwork lebih kepada masalah kapasitas bukan masalah operasional. Dengan banyakanya perangkat mobile dan perangkat IoT yang terhubung ke internet ketersedian alamat IP habis khususnya alamat IPv4.

Faktanya alamat IPv4 hanya mempunyai panjanga 32 bit dan dibagi menjadi menjadi 4 octet dengan penulisan notasi “dotted decimal”. Artinya kita mempunyai jumlah yang sangat terbatas bila dibandingkan dengan jumlah host atau perangkat yang akan terhubung, ditambah lagi banyak alamat address yang sudah “reserved” untuk special operasional dan pengalokasian yang terbuang percuma disisi pengguna [14].

Singkatnya, kita membutuhkan solusi lain. Solusi tersebut adalah generasi selanjutnya dari IP yang sering kita dengar yaitu IPv6. IP versi 6 dipilih sebagai yang terbaik Karena mempunyai alamat yang luas yaitu 128 bit. IPv6 support maximum 2^128 yaitu: 340,282,366,920,938,463,463,374,607,431,768,211,456 [14].

2.2.6.1 IPv6 Address Format

IPv6 menggunakan 16-byte hexadecimal pada penulisannya dan dibagi oleh kolom (:) untuk penulisan alamat 128-bitnya namun hal ini kurang praktis dan menimbulkan banyak error. Contoh penulisan alamat IPv6: 2001:db8:130F:0000:0000:09C0:876A:130B

Penulisan alamat IPv6 dapat disingkat namun ada aturan yang harus diperhatikan. angka 0 didepan pada field adalah opsional jadi dapat disingkat tidak perlu dituliskan contoh gambar 2.8



Gambar 2. 8 Penulisan IPv6 sebelum disingkat 1

Dan pada gambar 2.9 hasil singkatan penulisan dari gambar 2.8.



Gambar 2. 9 Penulisan IPv6 Sesudah disingkat 1

Aturan penulisan IPv6 selanjutnya yang dapat singkat field yang berisi angka 0 secara berurutan pada octet bisa disingkat menjadi *double colom* “::”. *Double coloum* “::” ini

hanya bisa digunakan sekali pada 1 alamat IPv6 karena jika ada 2 kita tidak akan berapa jumlah octet 0 yang berututan. Contoh gambar 2.10.

001:db8:130F:0000:0000:09C0:876A:130I

Gambar 2. 10 Penulisan IPv6 sebelum disingkat 2

Dan pada gambar 2.11 hasil singkatan penulisan dari gambar 2.10.

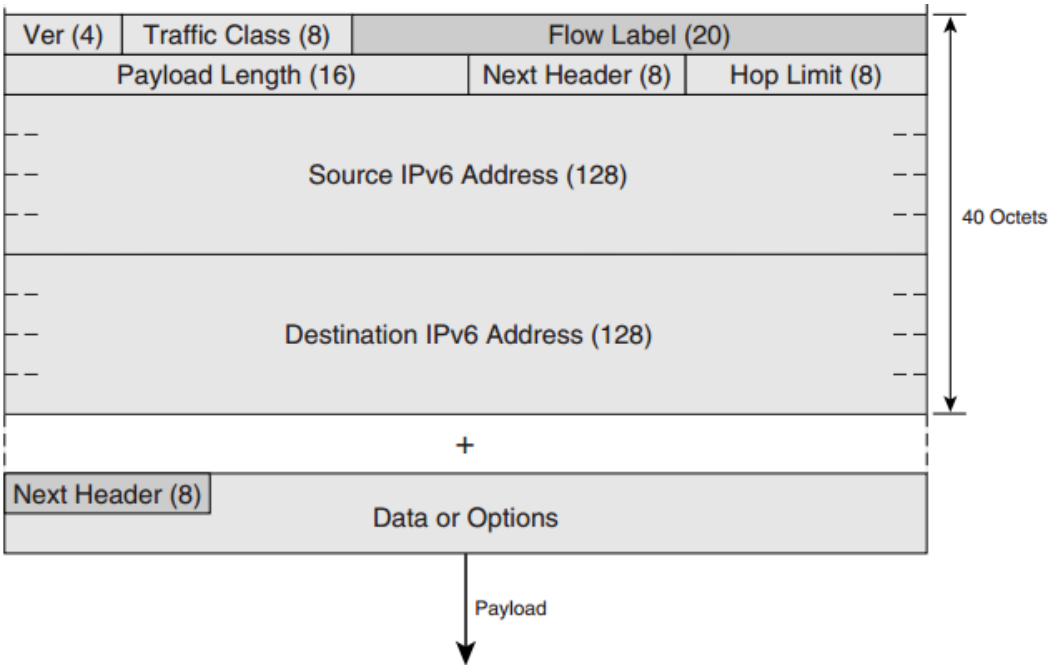
2001:db8:130F::09C0:876A:130B

Gambar 2. 11 Penulisan IPv6 Sesudah disingkat 2

Dengan aturan penulisan IPv6 diatas penulisan menjadi lebih sedikit dan mudah untuk dipahami [14].

2.2.6.2 IPv6 Header Structure

Dalam implementasi IPv6 ada perubahan struktur header adapun panjang header sama dengan IPv4 yaitu 32bit, berikut gambar 2.8 mengenai *struktur header* IPv6.



Gambar 2. 12 Struktur Header IPv6

Berikut ini adalah penjelasan dari header field IPv6:

1.	*Version* (4bit)	:	Digunakan mendefenisikan versi protocol IP.
2.	*Traffic Class* (8bit)	:	Header yang digunakan untuk kepentingan QOS
3.	*Flow Label* (20 bit)	:	Field untuk digunakan untuk kepentingan flow dan field ini diharapkan dapat membuat Router tidak perlu lookup paket lebih dalam untuk memperlakukan sebuah paket.
4.	*Payload Length* (16 bit)	:	Berisi informasi layer 4 keatas dari OSI Layer. Jumlah field ini tetep 40 bytes agar pada saat proses lookup oleh Router lebih cepat, Karena route tidak perlu melakukan pengecekan *variable-length header*
5.	*Next Header* (8bit)	:	Berisi informasi nomor port pada layer atasnya atau layer 4 yaitu transport.
6.	*Hop Limit*(8bit)	:	Field Time To Live (TTL)_untuk mencegah looping pada layer3
7.	*Source Address*(128bit)	:	Berisi informasi alamat IPv6 pengirim.
8.	*Destination Address*(128bit)	:	Berisi informasi alamat IPv6 penerima.
9.	*Extension header*	:	Berisi informasi header tambahan network layer, seperti routing header, encapsulating security payload (ESP) header.

2.2.6.3 IPv6 Address Architecture

Saat kita mengerti penulisan dari IPv6 maka akan memudahkan kita mendiskusikan *address architecture* dari IPv6 yang didefenisikan di RFC 3513: ada 3 address yang didefenisikan.

1. *Unicast* : Digunakan untuk mengidentifikasikan single node, dan taffic yang ditujukan untuk unicast address akan diforwardkan menuju single node.
2. *Multicast* : Digunakan untuk mengidentifikasikan group node, dan traffic yang ditujukan untuk multicast address akan diforwardkan menuju ke semua node yang ada pada group.
3. *Anycast* : Digunakan untuk mengidentifikasikan group node, dan traffic yang ditujukan untuk anycast address akan diforwardkan menuju ke node terdekat yang ada pada group.

2.2.6.4 Management Address dan Alokasi IPv6

IPv6 dalam pengalokasian alamat IPv6 kepada host menggunakan 4 cara.

1. Konfigurasi Statis : Sama seperti IPv4 konfigurasi host address, mask, dan gateway di konfig manual.
2. *Stateless Address Auto Configuration* (SLAAC) : Host secara mandiri mengkonfigurasi alamatnya dengan cara pesan *Router solication* (RS) dikirim untuk mendapatkan pesan *Router Advertisment* (RA) saat konfigurasi interface (RFC2462).
3. *Stateful* DHCPv6 : Host akan menggunakan Dynamic Host Configuration (DHCP) untuk mendapatkan alamat IPv6. Cara ini sama dengan alokasi IPv4 menggunakan DHCP (RFC 3315).
4. *Stateless* DHCP : Host menggunakan SLAAC dan juga menggunakan DHCP untuk mendapatkan informasi tambahan

contohnya (Domain Name Server)DNS, (Trivial File Transfer Protocol) TFTP Server, WINS dan lainnya. [14]

2.2.6.5 Transisi Teknologi IPv6

Adaptasi teknologi IPv6 agar dapat sukses digunakan secara luas membutuhkan suatu metode transisi. Seperti kita tahu kehabisan alamat IPv4 suatu saat pasti akan menggunakan adopsi IPv6. Kunci utama design yang bagus untuk IPv6 yaitu mempunyai kemampuan integrasi dan berjalan secara berdampingan dengan IPv4. [14]. Adapun metode transisi teknologi IPv6.

Teknik *dual stack* adalah teknik yang mengimplementasikan IPv4 dan IPv6 berjalan bersamaan disuatu perangkat jaringan. Metode untuk transisi ke alamat IPv6 dengan cara sebuah device mempunyai alamat IPv4 dan IPv6. Type perangkat ini sering disebut IPv4/IPv6 node. Dengan implementasi ini kita dapat mengaktifkan dan atau mematikan salah satu IP stack tersebut, jadi dengan node type ini ada kemungkinan 3 operasi yang dilakukan. Ketika IPv4 stack di aktifkan dan IPv6 dimatikan node hanya seperti node IPv4 biasa. Ketika IPv6 diaktifkan dan IPv4 diamtikan makan node hanya seperti node IPv6 biasa. Dan ketika node menggunakan stack IPv6 dan IPv4 [15]. Saat host menggunakan *dual-stack* pengiriman pertama akan menggunakan protocol IPv6 dahulu. [13]

Teknik *Tunneling* IPv6 adalah teknik yang mengimplementasikan pengiriman *traffic* diatas infrastruktur jaringan yang IPv4. Teknik *tunneling* ini dapat digunakan untuk percobaan infrastruktur IPv6 ketika semua jaringan yang ada hanya IPv4 dan jaringan IPv4 tidak perlu ada perubahan atau *upgrade. Tunneling* juga sering disebut enkapsulasi, dengan enkapsulasi satu protokol (contohnya IPv6) dapat dienkapsulasi atau dibungkus dengan protokol lain(contohnya IPv4) dan di *forward* diatas jaringan IPv4. [15]

Teknik Transalasi adalah teknik yang mengimplementasikan host atau komputer untuk berkomunikasi hanya dengan host IPv6. Tujuan dari teknik ini untuk menyediakan transparansi routing untuk jaringan IPv6 saat berkomunikasi dengan jaringan IPv4 dan sebaliknya. Perbedaannya tunneling dengan transalasi adalah paket IPv6 pada tunneling tidak akan berubah atau tersentuh tetapi dibungkus dengan paket IPv4 dan dibuka kembali pada saat di ujung tunnel.

2.2.6.5.1 Dual Stack

Host dengan *dual stack* bisa menggunakan teknologi IPv4 dan IPv6 secara bersamaan. Metode migrasi ini sering disebut juga IPv6/IPv4 node, pada saat komunikasi dengan host IPv6 host akan seperti menggunakan alamat IPv6 begitu juga saat berkomunikasi dengan IPv4 host akan menggunakan alamat IPv4. Pada implmetnasi dual-stack ini host akan mencoba menggunakan IPv6 terlebih dahulu kemudian jika tidak bisa maka akan menggunakan alamat IPv4.

2.2.6.5.2 Tunneling 6to4

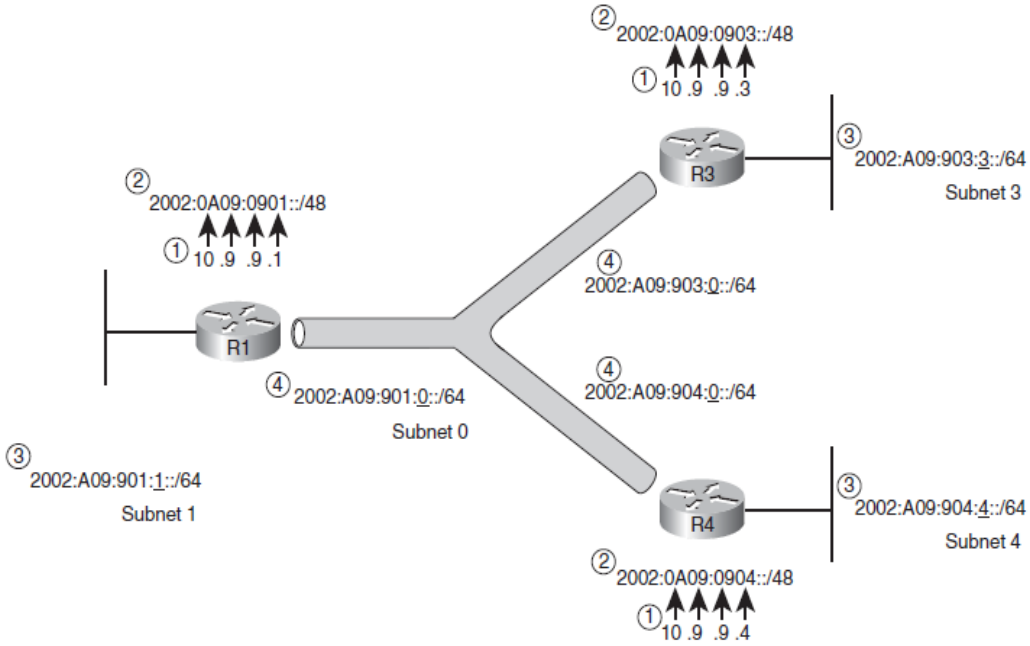
Teknik Tunneling adalah mekanisme yang dapat digunakan jika infarstruktur kita masih menggunakan IPv4 dan infrastruktur IPv4 tidak dapat dirubah atau di modifikasi, dengan metode ini infrastruktur tidak banyak yang berubah. Tunneling sendiri dibagi menjadi 2 kategori manual dan *automatic*. Tunneling dengan manual kita harus mengkonfigurasi tiap *end-point tunnel*. Jika menggunakan automatic tunnel akan dibuat ketika ada komunikasi dalam implmentasinya alamat tujuan IPv4 akan dimasukan dalam IPv6 untuk menentukan *end-point tunnel*. contoh metode tunneling yang popular 6to4 dan ISATAP,6rd(6 radid deployment).

RFC 3056 “Connection of IPv6 Domains via IPv4 Clouds,” mendefenisikan secara detail tentang cara kerja dan implementasi 6to4. Secara garis besar 6to4 sendiri jaringan IPv6 dapat berkomunikasi dengan jaringan IPv6 lainnya diatas jaringan IPv4 tanpa harus mengkonfigurasi tunnel secara manual, tuneel ini akan menentukan tujuan dengan benar dengan cara menggabungkan alamat prefix global IPv6 2002::/16 dengan IPv4. Format alamat addressnya akan menjadi seperti gamber 2.9

2002:*border-router-IPv4-address*::/48

Gambar 2. 13 Prefix 6to4

Engineer mengalokasikan tiap tunnel endpoint Router/host dengan /48 prefix, digunakan untuk semua Router yang terkoneksi di local. Engineer enambahkan versi hexa dari alamat IPv4 Router tersebut (bits 17 sampai 48) atau quertet 2 dan 3. contoh. alamat IP 10.9.9.1 alamat IPv6nya adalah 2002:0A09:0901::/48. Tiap subnet yang akan diimplementasi IPv6 maka akan dialokasikan prefix 2002::/16 dengan octet 2 dan 3 berisi informasi alamat IPv4. Konfigurasi terakhir tambahkan static routing untuk tiap network IPv6 contoh disini site 1 static routingnya. IPv6 route 2002:A09:903:3::/64 2002:A09:903:0::1 Pada gambar 2.10 akan dijelaskan bagaimana ketika ada pesan yang akan dikirimkan lewat 6to4 tunnel.



Gambar 2. 14 Cara Kerja 6to4

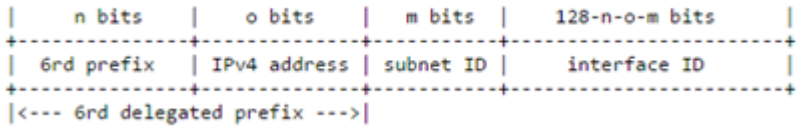
Saat Router menerima paket destination kolom pertama address 2002 makan paket tersebut akan diforwardkan ke tunnel interface, Router kemudian melihat bahwa

tuneel tersebut adalah 6to4 maka Router akan mengirimkan pesan tersebut ke alamat IPv4 pada octet 2 dan 3. [14]

2.2.6.5.3 Tunneling 6rd

Pada jaringan (internet Service Provider) ISP 6to4 ini tidak akan digunakan Karena masalah komunikasi. Paket yang berasal dari 6to4 dapat dengan mudah bekomunikasi dengan host 6to4 diinternet namun itu tidak selalu begitu, alasannya untuk komunikasi antar 6to4 di internet harus menggunakan 6to4 relay Router. pada saat komunikasi antar 6to4 host di internet tidak ada jaminan atau control terhadap route yang dikirim ke Router relay itu terkirim. kemudian selanjutnya walaupun jika ISP mengoperasikan beberapa Router relay 6to4 kemudian diadvertise dengan prefix 2002::/16 bisa saja paket yang diterima dari host yang tidak dikenali, maka dari itu ISP lebih memilih menggunakan alamat *costumer* atau alamat IP yang diberikan oleh (Regional internet Registry)RIR. Service provider juga memerlukan IPv4 yang unique untuk implementasi 6to4. [15]

6rd mengoptimalkan kekurangan yang dimiliki oleh 6to4 dengan cara mengganti 2002::16 menjadi alamat prefix IPv6 service provider, dengan cara ini operasional domain hanya terbatas pada jaringan service provider dan service provider mempunyai control penuh untuk hal tersebut, Service provider juga tidak perlu menggunakan keseluruhuan 32bit address IPv4 untuk alokasi IPv6, IPv4 yang digunakan juga bisa global maupun private. Format penulisan alamat 6rd ada pada gambar 2.11 :



Gambar 2. 15 Format Alamat 6rd

Dari gambar 2.11 dapat dijelaskan nilai 6rd prefix adalah prefix dari alamat IPv6 global yang dipunyai oleh service provider. IPv4 address adalah jumlah bit prefix yang kan

digubungkan dengan 6rd prefix. Dan subnet ID adalah subnet yang akan diberikan ke wilayah pelanggan provider. Untuk mendapatkan 6rd delegated prefix maka n bits + o bits. [15]

2.2.6.5.4 Tunneling ISATAP

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) dibuat untuk menyediakan komunikasi IPv6 metode transisi dual-stack diatas jaringan IPv4. Alamat ISATAP menyimpan alamat IPv4 di EUI-64 *interface identifier*. Pada ISATAP semua komputer atau perangkat jaringan harus sudah support protocol ISATAP yang didefenisikan di RFC 5214. ISATAP menggunakan format alamat seperti berikut gambar 2.12.

[64-bit link-local or global unicast prefix]:0000:5EFE:[IPv4 address of the ISATAP link]

Gambar 2. 16 Format Alamat ISATAP

Identifikasi *interface* ISATAP ada dibagian tengah dari format alamat ISATAP yaitu 0000:5EFE. Contoh kita mempunyai IPv6 prefix 2001:0DB8:0ABC:0DEF::/64 dan tujuan tunnel IPv4 172.20.20.1. Alamat IPv4 akan dirubah menjadi bilangan hexa yaitu AC14:1401 sehingga alamat ISATAP menjadi: 2001:0DB8:0ABC:0DEF:0000:5EFE:AC14:1401. [16]

Dengan menggunakan ISATAP, komputer IPv6 dan IPv4 dapat berkomunikasi dalam intranet, namun jika ingin berkomunikasi dengan internet border Router harus dikonfigurasi sebagai ISATAP Router atau 6to4 gateway. Alamat IPv4 pada ISATAP tidak perlu public, karena prefix yang diberikan sudah unique dan dapat dirouting ke internet. Yang perlu diperhatikan pada tunnel ISATAP ini jika dipasang pada jaringan enterprise atau service provider yang menggunakan NAT itu tidak akan bisa karena alamat private IPv4 pasti akan ditranslasikan. ISATAP sendiri sebenarnya digunakan untuk menyediakan komunikasi antar individu IPv6 pada dual-stack yang terisolasi oleh jaringan IPv4. Pada mode operasinya sendiri ISATAP seperti jaringan ad-hoc dan ini telah terbukti berguna pada jaringan 3GPP.

2.2.6.5.5 NAT64

Address Family Translation atau secara singkatnya translasi memberikan fasilitas komunikasi antara native IPv6 dengan native IPv4 dengan cara melakukan translasi pada header IP, contoh metode translasi yang popular NAT64 yang menggantikan NAT-PT.

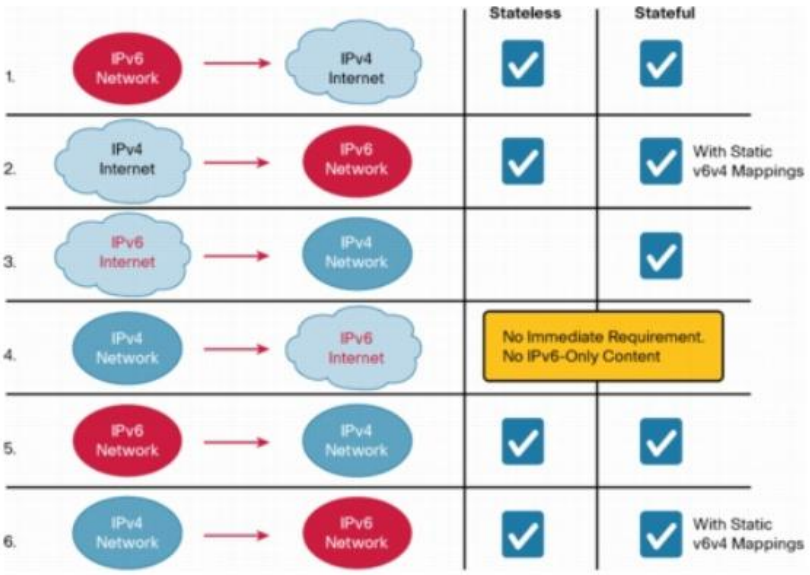
NAT64 memberikan fasilitas komunikasi antara host IPv6 dan IPv6 dengan dukungan teknologi DNS64. NAT64 ada 2 kategori untuk mencapai tujuannya fungsinya yaitu *stateless* dan *stateful*. Nat64 *stateless* didefensikan di RFC 6145 dan NAT64 *stateful* di RFC 6146. Tabel 2.2 menjelaskan perbandingan antara NAT64 *stateless* dan *statefuI*. [17]

Tabel 2. 2 Perbandingan NAT64 Stateless dan Stateful

	NAT64 Stateless	NAT64 Stateful
1.	1:1 translasi ,karena itu terbatas untuk beberap host saja	1:N transalsi, karena itu tidak ada Batasan jumlah host yang harus ditranslasi
2.	Alamat IPv4 yang digunakan cepat habis	Satu alamat IPv4 dapat digunakan banyak host
3.	Tidak ada binding saat translasi	Menggunakan binding setiap transaksi agar unique.
4.	Dibutuhkannya konfigurasi manual ip address atau lewat DHCPv6	Dapat menggunakan berbagai macam alokasi alamat seperti DHCPv6, manual, dan SLAAC
5.	Dibutuhkan transalasi IPv4 ke IPv6 secara	Tidak perlu melakukan translasi antara IPv4 ke IPv6.

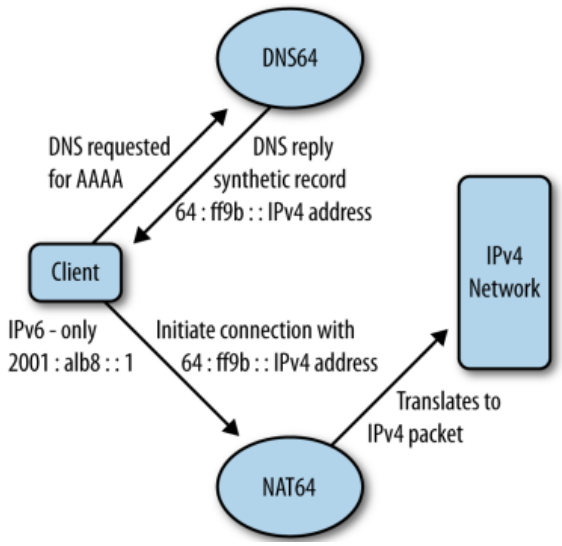
	manual sebagai kebutuhan utama	

Untuk scenario komunikasi antar IPv4 dan IPv6 yang dapat diberikan dari NAT64 dapat dilihat pada gambar 2.17



Gambar 2. 17 Skenario Komunikasi NAT64 IPv6 dan IPv4 [17]

Saat komputer IPv6 dengan NAT64 akan melakukan komunikasi dengan IPv4, komputer IPv6 akan menggunakan alamat 64:ff9b::/96 dan sisa 32 bit adalah alamat tujuan IPv4. Pada gambar 2.18 akan dijelaskan bagaimana cara kerja komputer IPv6 dengan NAT64 berkomunikasi.



Gambar 2. 18 Cara Kerja NAT64

Saat client IPv6 akan berkomunikasi dengan IPv4 akan menanyakan informasi AAAA pada server dns64, jawaban yang diterima adalah alamat prefix nat64 digabungkan dengan alamat IPv4 64:ff9b::IPv4. Saat komputer IPv6 sudah menemukan informasi AAAA tersebut komputer akan mengirimkan paket ke NAT64 dan NAT64 akan mentransalsikan alamat tersebut dan dikirimkan ke host IPv4. [15]

Metode ini sudah di test dan sukses dijaringan internet, tapi masalah muncul jika didalam sebuah aplikasi masih menggunakan format IPv4 tidak menggunakan FQDN, karena saat menanykan record AAAA tidak akan bisa. Pada jaringan mobile mekanisme ini lebih dipilih dibandingkan dengan dual-stack karena meghabiskan baterai.

2.2.7 Plan Design Implement Operate Optimize (PDIOO)

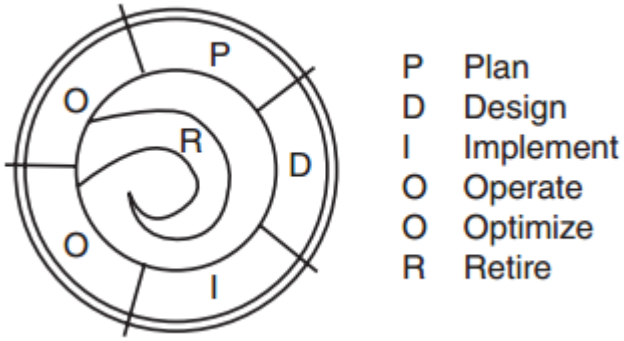
Sistem analis sudah terbiasa dengan istilah *life-cyle* atau proses pembuatan system secara berkala kepada system yang sedang berjalan maupun yang akan dibuat. dalam dunia jaringan *life-cyle* juga digunakan untuk membangun sebuah jaringan atau mengoptimalkan jaringan yang sudah ada [18].

Dokumentasi cisco memilih ke Plan Design Implement Operate Optimize (PDIOO) sebagai *life-cycle* pada jaringan. Tidak jadi masalah kita akan menggunakan life-cyle yang mana selama kita menyadari bahwa perancangan jaringan harus terstruktur, terencana, *modular fashion* dan tanggapan dari pengguna ke pihak operasional jaringan menjadi acuan untuk jaringan baru dalam menambah, mengoptimalkan atau perancangan jaringan. Life-cycle PDIOO terdiri dari beberapa step berikut [18]:

Plan	:	Pada *plan* ini dilakukan pendefenisian kebutuhan network. Menganalisa dimana network akan dipasang atau digunakan, tipe layanan apa yang akan diberikan, dan digunakan oleh siapa. Saat semua sudah terdefenisi maka kebutuhan dasar jaringan sudah teridentifikasi.
Design	:	Kebutuhan jaringan telah didapatkan dari langkah *planning* selanjutnya dibuat langkah *design* dan juga dilakukan koordinasi dengan administrator atau manager. Contoh *design* yang dilakukan logical *design* dan *physical design.*
Implementation	:	Melakukan implementasi sesuai design yang dibuat. Pada langkah ini dilakukan pengetesan design yang dibuat dan pengetesen design.
Operation	:	Operataion adalah test terakhir seberapa efektif design yang dibuat. Jaringan akan dimonitoring pada langkah ini mulai dari peforma dan segala kesalahan yang dibuat yang nantinya akan digunakan sebagai dasar pada langkah *optimize.*
Optimize	:	pada langkah ini akan melakukan identifikasi masalah yang diimplmentasi, dan membuat solusi untuk masalah tersebut. Pada langkah ini juga dilakukan *redesign* jika saat operasi terjadi banyak masalah.

Retire : Ketika jaringan atau bagian dari jaringan sudah *out-of-date* bagian tersebut harus diambil dari jaringan produksi. Walaupun *retire* tidak dimasukan dalam siklus PDIOO namun sangat penting untuk kebutuhan jaringan yang terus berkembang. [18]

Berikut gambar 2. 19 merupaka model dari dari metode PDIOO



Gambar 2. 19 Model Life-Cyle PDIOO

Plan pada metode PDIOO fokus kepada analisa kebutuhan *network analyst* melakukan wawancara kepada pengguna dan orang teknis untuk memahami bisnis dan tujuan teknis pada jaringan baru atau jaringan yang akan dioptimasi. Tugas dari penkarakeristikan pada jaringan yang sudah ada seperti melakukan analisa performa jaringan logic dan fisik. Langkah terakhir pada plan ini adalah menganalisa trafik jaringan yang sudah ada dan yang akan mendatang seperti jalur trafik dan *load*, kebiasaan protokol, dan kebutuhan *quality of service* (QOS). [18]

Design pada metode PDIOO fokus kepada melakukan pembangunan pada rancangan logik seperti pengalamatan logik, penamaan, switching, routing protocol, rancangan keamanan, rancangan manajemen jaringan, dan pemilihan service provider atau WAN sesuai dengan kebutuhan pelanggan. pembangunan pada jaringan fisik melakukan penspesifikasian teknologi dan produk yang sesuai dengan kebutuhan pada rancangan jaringan logik. [18]

Operate dan *Optimize* fokus adalah langkah terakhir dari metode PDIOO pada langkah ini dilakukan rencana implementasi, melakukan *prototype* atau *pilot*,

pengoptimalisasian jaringan dan mendokumentasikan pekerjaan dengan proposal rancangan jaringan. [18].

2.2.8 Border Gateway Protocol (BGP)

Border Gateway protocol (BGP) adalah arsitektur dari routing internet yang digunakan untuk pertukaran informasi route dari Autonomous System (AS) yang berbeda. Perbedaan IGP dan BGP yang paling utama adalah BGP tidak membutuhkan neighbor yang terkoneksi pada subnet yang sama, untuk memilih jalur terbaik BGP membutukan aturan complex yang disebut *path attribute.* BGP sendiri mempunyai 2 kategori neighbor external BGP (eBGP) dan internal BGP (iBGP).

Untuk menghitung best path dalam BGP , menggunakan banyak kemungkinan, tidak seperti RIP dia berdasarkan hop count, EIGRP perhitungan formula berdasarkan bandwidth dan delay, ospf berdasarkan cost yang didapat dari perhitungan bandwidth, berikut adalah urutan BGP *attribute* untuk menentukan jalur terbaik: [16]

0.	*Next hop*	:	Ip next hop harus dapat terhubung, jika tidak terhubung maka route tersebut akan digunakan.
2.	*weight*	:	Diliat dari nilai yang paling tinggi untuk dapat dipilih
3.	*Local preference*	:	Diliat dari nilai yang paling tinggi default nilai 100
4.	*Local originated routes*	:	Attribute utama yang harus dikirimkan saat pengiriman route apakah dari IGP (i), EGP(e), atau incomplete (?).
5.	AS-PATH	:	Dipilih nilai AS-PATH yang terkecil. Nilai ini berisi informasi jalur AS untuk mencapai route.
5.	*Origin*	:	Dipilih nilai yang paling kecil, ada 3 origin code. (i) didapat dari IGP, (e) didapat dari EGP,(?).
6.	*MED(Multi Exit Dicriminator)*	:	Dipilih nilai yang paling kecil.

7. *Neighbor type* : Mengidentifikasikan route tersebut dari iBGP atau eBGP.
8. *IGP metric to next_hop* : Router akan membandingkan metri tersebut untuk tiap alamat *next-hop* dan akan memilih next-hop terendah.

Jika dari 8 attribute diatas masih belum ditemukan jalur tebaik makan Router akan menentukan dengan cara, eBGP route yang paling rendah yang akan disimpan jika tidak makan akan memilih RID paling rendah, jika tidak maka akan memilih alamat *neighbor* paling rendah. [16]

2.2.9 Open Short Path First (OSPF)

Open short path First (OSPF) adalah routing protocol yang digunakan untuk wilayah Interior Gateway Protocol (IGP) atau digunakan hanya untuk autonomous system yang sama. OSPF menggunakan algoritma SPF untuk menentukan jalur terbaik agar mencapai tujuan. Protocol OSPF sendiri *open Standard* artinya spesifikasi protocol dipublish ke umum sehingga semua orang dapat mengimplementasikan tanpa perlu lisensi biaya dan dengan ini juga OSPF banyak disupport vendor. OSPF mempunyai 2 versi OSPFv2 yang dikhusukan untuk pertukaran informasi alamat IPv4 dan OSPFv3 pertukaran informasi alamat IPv6..

Cara kerja OSPF sendiri untuk menentukan route terbaik adalah pertama Router OSPF akan membangun *neighbor* antar OSPF, kemudian antar neighbor akan bertukar informasi tentang route yang dipelajari yang disebut link-state advertisement (LSA), informasi yang telah diterima neighbor lain akan disimpan dalam database link state Database (LSDB). Dengan LSDB Router OSPF akan mengetauhi seluruh informasi route dari semua Router dalam jaringan sehingga nantinya tinggal algoritma SPF yang menentukan jalur terbaik menuju tujuan. Route yang telah dipilih oleh OSPF akan disimpan ke tabel routing.

2.2.10 Multi Protocol Label Switching (MPLS)

Multi protocol Label Switching (MPLS) protocol membuat paradigma baru untuk Router bagaimana cara untuk memforwardkan paket. Dibandingkan harus meneruskan paket berdasarkan IP tujuan yang ada di header, MPLS memforwardkan paket berdasarkan label. Karena menggunakan label pada proses penerusan paket. mpls dapat menentukan suatu tujuan bisa berdasarkan faktor lain seperti kebutuhan QOS, *traffic engineering,* dan kebutuhan privacy untuk tiap pelanggan yang terhubung ke jaringan MPLS, tetapi MPLS tetap masih menggunakan informasi routing protocol IGP atau EGP. [16]

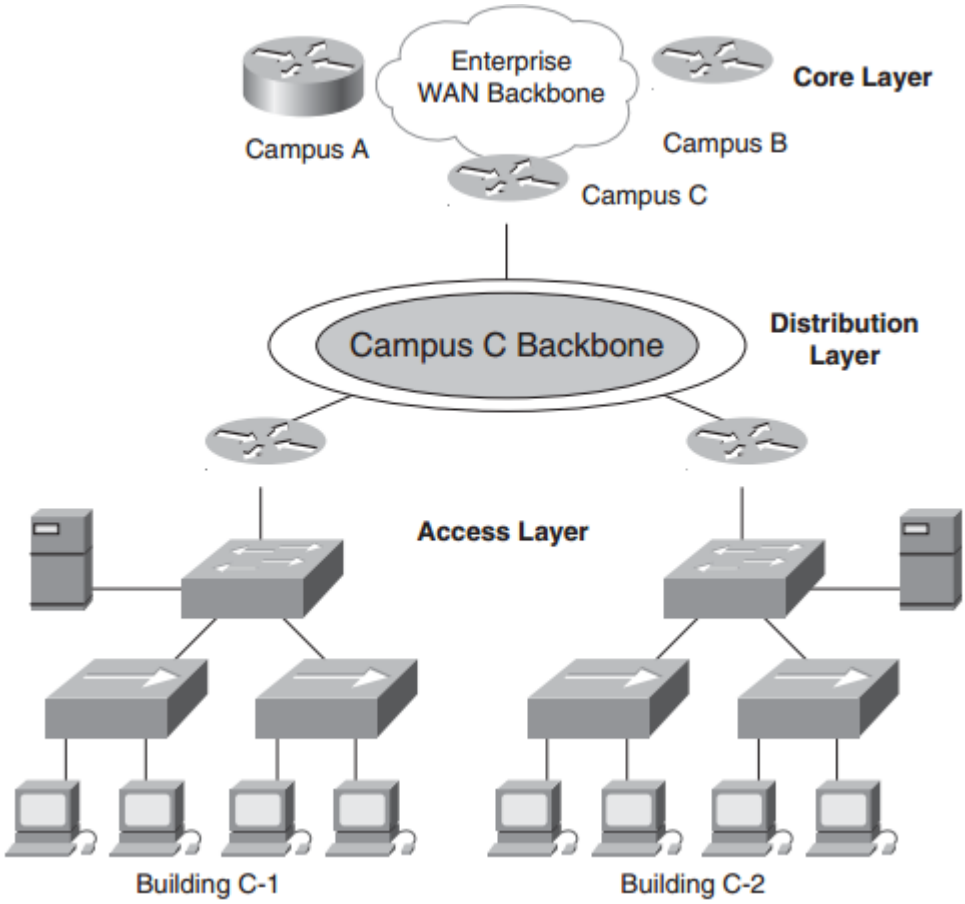
MPLS memiliki banyak variasi dalam implementasinya bisa digunakan untuk MPLS unicast IP atau MPLS VPN. Pada *MPLS unicast IP* mpls akan memforwardkan paket berdasarkan label dan dalam pemilihan interface keluarnya menggunakan route IP pada routing table. Jadi jalur pengiriman MPLS sama dengan jalur pengiriman paket IP. Pertukaran informasi label antar Router pada MPLS menggunakan protocol *Label Distribution Protocol* (LDP) dan Resource Reservation Protocol (RSVP) untuk *traffic engineering* pada MPLS

MPLS VPN adalah pengaplikasian MPLS yang paling populer, dengan ini penyedia layanan atau *enterprise* yang besar dapat menyediakan layanan L3VPN dan L2VPN. Implementasi VPN pada MPLS tidak memerlukan perubahan pada jaringan penyedia layanan, perubahan hanya dilakukan pada perangkat yang mengarah ke pelanggan, karena inilah MPLS banyak diadaptasi dan diimplementasi oleh banyak orang. [13]

Virtual Private LAN Service (VPLS) adalah aplikasi MPLS pada VPN layer 2. Dengan VPLS membuat jaringan Multipoint-to-Multipoint untuk layer 2 antara tempat pelanggan. VPLS ini dapat digunakan sebagai pengganti ethernet over MPLS, L2Pv3 bahkan GRE. Perangkat penyedia layanan yang mengarah deserver akan menjadi seperti switch yang besar karena alamat mac-address yang dibaca banyak dan terhubung ke berbagai pelanggan. [19]

2.2.11 *Hierarchical Network Design*

Hierarchical network design adalah framework yang dibuat oleh perancang jaringan expert untuk membuat topologi jaringan secara baik dan benar. Hierarchical network design ini dibagi menjadi 3 lapisan untuk membangun rancangan topologi tersebut [18]. Tiap lapisan fokus pada spesisfik tujuan dengan ini kita dapat memilih system dan fitur secara benar dan baik pada tiap lapisan. Gambar 2.20 adalah contoh topologi jaringan secara hirarki.



Gambar 2. 20 Hierarchical Network Design

Dari gambar 2.20 layer tersebut dibagi menjadi 3 bagian yaitu lapisan *accees, distribution, core*. Adapun fungsi dari 3 layer tersebut adalah :

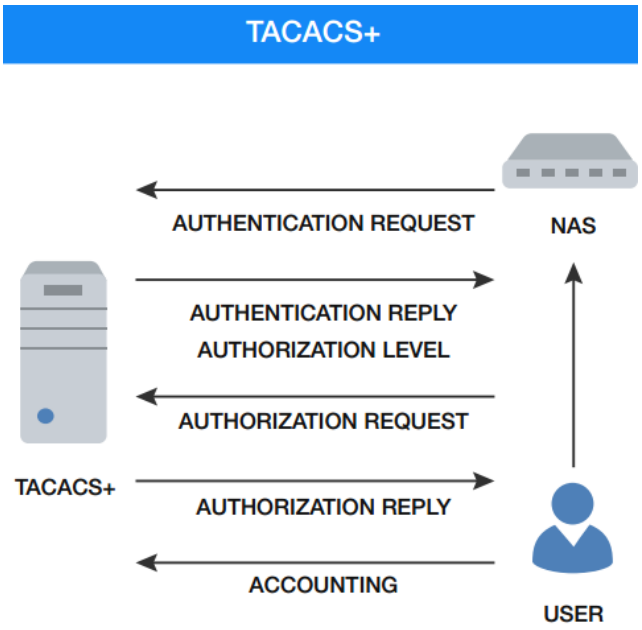
Access : Lapisan yang langsung terhubung ke user via *low-end* switch atau *access-point*.

Distribution	:	Lapisan dengan Router dan switch yang diimplementasikan policies, routing. pada jaringan yang kecil lapisan *core* dan *distribution* digabung.
Core	:	lapisan dengan *high-end* Router dan switch yang mana di optimasikan untuk kebutuhan availibilty dan performance.

2.2.12 Authentication, Authorization, Accounting (AAA)

Protokol AAA adalah protokol yang digunakan dengan tujuan untuk memberikan verifikasi kepada *user* (*authentication*), memberikan kontrol akses kepada pengguna terhadap data di server (*authorization*), dan memberikan monitoring penggunaan informasi untuk kebutuhan layanan billing (*accounting*). Aplikasi yang digunakan untuk implementasi AAA ini contohnya adalah radius dan tacacs. [16]

Terminal Access Controller Access-Control System (TACACS) adalah protokol yang menangani autentikasi remote dan layanan terkait untuk mengakses suatu perangkat jaringan lewat server yang terpusat. Tacacs memisahkan fungsi *authorization,* dengan ini menambahkan kemudahan akses kotrol kepada siapa yang dapat menggunakan perintah pada sebuah perangkat. Setiap perintah yang dimasukan oleh pengguna ke perangkat akan dikirimkan ke tacacs server untuk pengecekan authorization dan nantinya *user* tersebut akan dicek kepemilikan *user group* tersebut.



Gambar 2. 21 Cara Kerja Tacacs

Berdasarkan gambar 2.21 dapat disimpulkan cara bagaimana cara kerja dari tacacs yaitu setiap *user* yang akan melakukan login ke perangkat jaringan, perangkat jaringan akan mengirimkan pesan *authentication request* ke server tacacs apakah *user* tersebut diberikan hak akses login atau tidak. Saat *user* memasukan perintah ke perangkat jaringan maka perintah tersebut akan dicek dengan pesan *authorization request* ke server tacacs apakah user tersebut diberikan hak akses perintah tersebut atau tidak.