BAB II

DASAR TEORI

2.1 VPN *(Virtual Private Network)*

VPN (Virtual Private Network) adalah suatu jaringan privat (biasanya untuk instansi atau kelompok tertentu) di dalam jaringan internet (publik), dimana jaringan privat ini seolah-olah sedang mengakses jaringan lokalnya tapi menggunakan jaringan publik.

VPN merupakan salah satu teknik pengamanan jaringan dengan cara membuat suatu *tunne*l, misalkan pada jaringan publik atau internet sehingga bersifat *private* dan aman. VPN dikatakan bersifat *private* karena ketika dibutuhkan sebuah koneksi VPN membutuhkan autentikasi untuk memastikan bahwa kedua ujung dalam koneksi adalah *user* yang sesuai dengan yang diberikan kewenangan untuk mengakses suatu *user*.

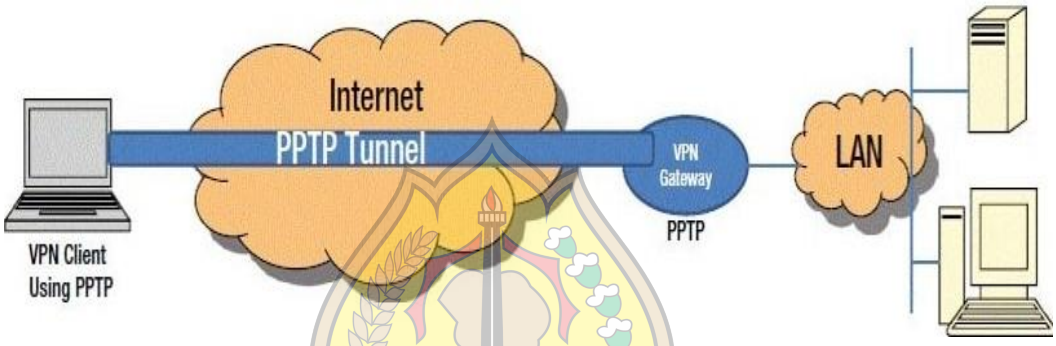
Meningkatnya *prevalensi* koneksi internet *broadband* di kantor dan rumah yang letaknya jauh membuat akses yang lebih murah ke internet menjadi hal yang menarik. VPN memungkinkan masing-masing *remote user* dari jaringan dapat berkomunikasi dalam jalur yang aman dan dapat diandalkan dengan menggunakan internet sebagai perantara untuk terkoneksi ke LAN *(Local Area Network)* pribadi Anda. VPN dapat dikembangkan untuk mengakomodasi lebih banyak pengguna dan tempat-tempat lain secara lebih mudah.

VPN adalah sebuah cara aman untuk mengakses *local area network* yang berada pada jangkauan, dengan menggunakan internet atau jaringan umum lainnya untuk melakukan transmisi data paket secara pribadi, dengan enkripsi perlu

penerapan teknologi tertentu walaupun menggunakan medium yang umum agar *traffic* (lalu lintas) antar *remote-site* tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan *traffic* yang tidak semestinya ke dalam *remote-site*. (Yetti Yuniati, 2014)

2.2 Jenis – Jenis VPN

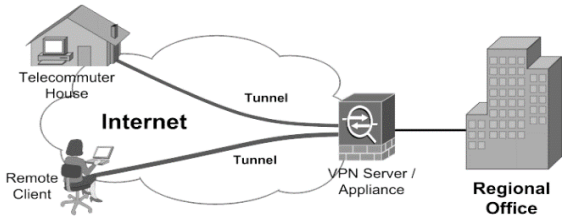
2.2.1 *Point to Point VPN*



Gambar 2.1 Cara kerja *point to point* VPN (Sumber : Citraweb.com, 2019)

Salah satu *service* yang biasa digunakan untuk membangun sebuah jaringan VPN adalah *Point to Point Tunnel Protocol* (PPTP). Sebuah koneksi PPTP terdiri dari *server* dan *client.* Mikrotik Router OS bisa difungsikan baik sebagai server maupun client atau bahkan diaktifkan keduanya bersama dalam satu mesin yang sama. Feature ini sudah termasuk dalam *package* PPTP sehingga perlu cek di menu *system package,* apakah paket tersebut sudah ada di router atau belum. Fungsi PPTP *client* juga sudah ada di hampir semua OS, sehingga bisa menggunakan Laptop/PC sebagai PPTP *client.* Biasanya PPTP ini digunakan untuk jaringan yang sudah melewati *multihop r*outer *(Routed Network).* Jika anda ingin menggunakan PPTP pastikan di *router* tidak ada *rule* yang melakukan *blocking* terhadap *protocol* TCP 1723 dan IP *protocol* 47/GRE karena *service* PPTP menggunakan *protocol* tersebut.

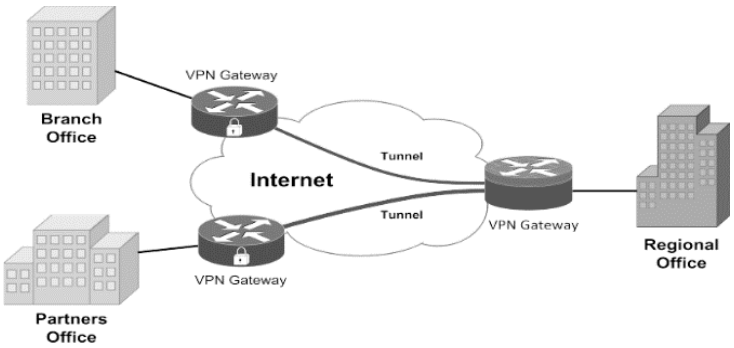
2.2.2 *Remote Access* VPN



Gambar 2.2 Cara kerja remote access VPN (Sumber : Chandra Cahyani, 2020)

Model *Remote Access* VPN banyak digunakan ketika menghubungkan *host* pada jaringan yang tidak aman ke *resource* pada jaringan yang aman, contohnya menghubungkan pegawai yang sedang berada di lokasi *remote* dikantor pusat melalui internet. Salah satu keuntungan yang didapatkan dari *remote access* adalah tidak perlu pergi ke kantor pusat jika ingin mengakses *file* dari komputer di sana. Hal ini tentu membuat kerja semakin produktif serta efektif, karena tidak membuang-buang waktu dalam perjalanan. Selain itu, *remote access* akan membantu dalam keadaan darurat ketika sedang membutuhkan informasi dari kantor.

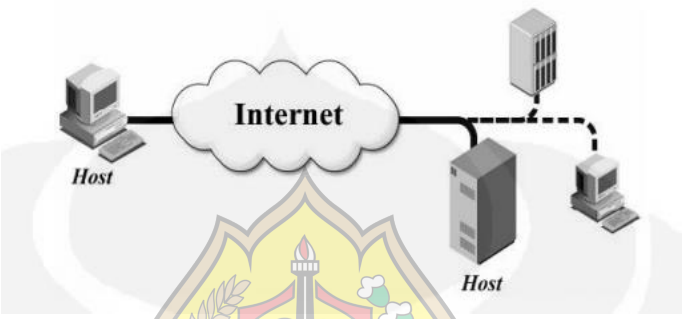
2.2.3 *Site to Site* VPN



Gambar 2.3 Cara kerja *site to site* VPN (Sumber : Chandra Cahyani, 2020)

Arsitektur *Site to Site* biasanya paling banyak digunakan ketika menghubungkan dua jaringan yang aman, seperti menghubungkan sebuah Kantor cabang ke pusat melalui internet. Arsitektur model ini menggantikan *wide area network* (WAN) privat yang *relative* mahal.

2.2.4 *Host to Host* VPN



Gambar 2.4 Cara kerja host to host VPN (Sumber : Chandra Cahyani, 2020)

Model ini biasa digunakan ketika sejumlah kecil user atau administrator pada sistem remote membutuhkan protokol yang tidak aman dan dapat di*update* untuk menyediakan servis VPN. Arsitektur ini tidak transparan terhadap *user* karena harus melakukan otentikasi sebelum menggunakan VPN. Selain itu, semua pihak yang terkait harus meng-instal perangkat lunak VPN client yang telah dikonfigurasi.

2.3 Fungsi Utama VPN

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

2.3.3 *Confidentially* (Kerahasiaan)

Digunakannnya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat

melaluinya. 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.

2.3.4 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.

2.3.5 *Origin Authentication* (Autentikasi Sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang diterimanya. VPN 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 Teknologi VPN

Virtual Private Network adalah perpaduan dari teknologi *tunneling* dengan teknologi enkripsi. Kedua teknologi tersebut saling melengkapi.

a. Teknologi Tunneling

Teknologi *tunneling* merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut *tunnel* karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringa umum, namun koneksi tersbut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya.Hal ini sama dengan seperti penggunaan jalur *busway* yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus. Koneksi *point-to-point* ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat *point-to-point*.

Teknologi ini dapat dibuat di atas jaringan dengan pengaturan *IP Addressing* dan *IP Routing* yang sudah matang. Maksudnya, antara sumber *tunnel* dengan tujuan *tunnel* telah dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak terbentuk dan VPN pun tidak dapat dibangun.

Apabila *tunnel* tersebut telah terbentuk, maka koneksi *point-topoint* palsu tersebut dapat langsung digunakan untuk mengirim dan menerima data. Namun, di dalam teknologi VPN, *tunnel* tidak dibiarkan begitu saja tanpa diberikan sistem

keamanan tambahan. *Tunnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati tunnel tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi aman dan bersifat pribadi.

b. Teknologi Enkripsi

Teknologi enkripsi menjamin data yang berlalu-lalang di dalam tunnel tidak dapat dibaca dengan mudah oleh orang lain yang bukan merupakan komputer tujuannya. Semakin banyak data yang lewat di dalam tunnel yang terbuka di jaringan publik, maka teknologi enkripsi ini semakin dibutuhkan. Enkripsi akan mengubah informasi yang ada dalam tunnel tersebut menjadi sebuah ciphertext atau teks yang dikacaukan dan tidak ada artinya sama sekali apabila dibaca secara langsung. Untuk dapat membuatnya kembali memiliki arti atau dapat dibaca, maka dibutuhkan proses dekripsi. Proses dekripsi terjadi pada ujung-ujung dari hubungan VPN. Pada kedua ujung ini telah menyepakati sebuah algoritma yang aka digunakan untuk melakukan proses enkripsi dan dekripsinya. Dengan demikian, data yang dikirim aman sampai tempat tujuan, karena orang lain di luar tunnel tidak memiliki algoritma untuk membuka data tersebut.

2.5 Mobile VPN

Mobile VPN adalah konfigurasi jaringan di mana perangkat mobile seperti notebook, ponsel maupun Personal Digital Assistant (PDA) dapat mengakses Virtual Private Network (VPN) ketika bergerak dari satu lokasi ke lokasi lainnya. Mobile VPN yang efektif menyediakan pelayanan yang berkesinambungan bagi pengguna dan dapat secara mulus beralih dari teknologi akses dan berbagai jaringan publik. Fungsi mobile VPN yang efektif adalah transparan kepada pengguna akhir tanpa mengorbankan keamanan atau privasi

2.6 *Wireless* LAN *(Local Area Network)*

Wireless LAN (*Local Area Network*) yaitu jaringan komputer yang menggunakan gelombang radio sebagai media transmisi data dimana informasi dari satu komputer ke komputer lainya tanpa menggunakan kabel sebagai media perantara. Dimana ketika sebuah data dikirimkan baik oleh pengirim sinyal Wi-Fi (*Wireless Fidelity*) data biner akan dikodekan menjadi sebuah frekuensi radio kemudian akan transmisikan oleh perangkat *wireless router*. (U. Darmanto Soer,2019).

LAN nirkabel atau yang sering di sebut *wireless* LAN, adalah suatu jaringan area lokal nirkabel yang mengunakan media udara dengan mengunakan frekuensi gelomnang radio dalam mengkomunisikan informasi dari satu point ke point yang lain tanpa mengunakan *physical connection*. *Wireless* LAN merupakan suatu jaringan komputer yang memanfaatkan gelombang radio sebagai media transmisi data. *Wireless* LAN saat ini berkembang dengan sangat pesat karena teknologi ini *relative* murah dan mudah di implementasikan.

Jaringan nirkabel atau WLAN adalah suatu jaringan yang memanfaatkan sinyal gelombang radio sebagai lapisan fisiknya, keuntungan dari teknologi ini adalah mobilitas pengguna yang cukup tinggi karena tidak harus terpaku di satu tempat saja yang menyebabkan kenyamanan dalam pengunanya. Disamping itu, dikarenakan laisan fisiknya tidak berupa benda, seperti kabel, maka perluasan jaringan tidak tergantung pada perangkat fisik yang banyak, namun cukup dengan memberikan satu perangkat yang dapat menjadi akses poin. Dengan tidak bertambahnya perangkat setiap pertambahan pengguna, maka teknologi ini dapat menghemat cukup banyak biaya. (Agus Nur Wicaksono.2016)

Wireless LAN adalah sebuah bentuk komunikasi nirkabel yang memiliki area terbatas seperti dalam suatu ruangan ataupun sebuah gedung (Erick Irawadi Alwi, 2019) yang mengunakan teknologi *Wi-Fi* atau *Wireless Fidelity* adalah satu standar *Wireless Networking* tanpa kabel. Teknologi *Wi-Fi* memiliki standar yang ditetapkan oleh sebuah institusi internasional yang bernama IEEE (*Institute of Electrical and Electronic Engineers*) 802.11.

2.4.3 IEEE 802.11 Standar *Wireless* LAN.

IEEE (*Institute of Electrical and Electronic Engineers*) merupakan institusi yang melakukan diskusi, riset dan pengembangan terhadap perangkat jaringan yang kemudian menjadi standarisasi untuk digunakan sebagai perangkat jaringan.

802.1 = LAN/MAN Management and Media Access Control Bridges

802.2 = Logical Link Control (LLC)

802.3 = CSMA/CD (Standar untuk Ehernet Coaxial atau UTP)

802.4 = Token Bus

802.5 = Token Ring (bisa menggunakan kabel STP)

802.6 = Distributed Queue Dual Bus (DQDB) MAN

802.7 = Broadband LAN

802.8 = Fiber Optic LAN & MAN (Standar FDDI)

802.9 = Integrated services LAN Interface (standar ISDN)

802.10 = LAN/MAN Security (untuk VPN)

802.11 = Wireless LAN (Wi-Fi)

802.12 = Demand Priority Access Method

802.15 = Wireless PAN (Personal Area Network) > IrDA dan Bluetooth

802.16 Broadband Wireless Access (standar untuk WiMAX)

2.6.2 Perkembangan generasi IEEE 802.11

Teknologi jaringan WLAN telah mengalami perkembangan hingga lima generasi. Berikut adalah urutan generasi teknologi WLAN berdasarkan kode IEEE:

1) IEEE 802.11b
2) IEEE 802.11g
3) IEEE 802.11a
4) IEEE 802.11n
5) IEEE 802.11ac

Kode IEEE 802.11 a/b/g/n/ac menyatakan data rate sebuah perangkat WLAN. Data rate sesungguhnya bukanlah kecepatan yang nyata, yang akan di peroleh ketika melakukan transfer suatu data melalui media komunikasi. Kemampuan transfer data dari perangkat telekomunikasi tidak pernah mencapai titik data rate yang tercantum. Tetapi data rate mengambarkan kemampuan sebuah media komunikasi untuk mengirimkan data melalui jalur komunikasi.(Agus Nur Wicaksono,2016). Berikut adalah daftar data rate yang dimiliki oleh masing-masing kode IEEE 802.11 :

1) IEEE 802.11b memiliki data rate sebesar 11 Mbps
2) IEEE 802.11g memiliki data rate sebesar 54 Mbps
3) IEEE 802.11a memiliki data rate sebesar 54 Mbps
4) IEEE 802.11n memiliki data rate lebih dari 100 Mbps hingga 500 Mbps
5) IEEE 802.11ac memiliki data rate mencapai 1300 Mbps

Kode 802.11a/b/g/n/ac menunjukan frekuensi yang digunakan pada perangkat WLAN. Berikut adalah daftar frekuensi berdasarkan kode IEEE 802.11:

1) IEEE 802.11b menggunakan frekuensi 2,4 GHz
2) IEEE 802.11g menggunakan frekuensi 2,4 GHz
3) IEEE 802.11a menggunakan frekuensi 5 GHz
4) IEEE 802.11n menggunakan frekuensi 2,4 GHz dan 5 GHz
5) IEEE 802.11ac menggunakan frekuensi 5 GHz

Tabel 2.1 Perbandingan standar *wireless* 802.11

Spesifikasi	kecepatan	Frekuensi band
802.11b	2 Mbps	2,4 Ghz
802.11g	54 Mbps	2,4 Ghz
802.11a	11 Mbps	5 Ghz
802.11n	100Mbps – 500 Mbps	2,4 Ghz – 5 GHz
802.11ac	1300 Mbps	2,4 Ghz

(Sumber : Agus Nur Wicaksono,2016)

Menurut Agus Nur Wicaksono,2016. Jaringan WLAN harus memiliki kemampuan-kemampuan yang sama dengan yang diwajibkan untuk jaringan LAN pada umumnya. Berikut ini adalah beberapa diantara persyaratan-persyaratan terpenting untuk jaringan WLAN :

a. *Throughtput* : *Medium Access Control* (MAC) jaringan WLAN harus mampu memanfaatkan nirkabel yang ada seefisien mungkin untuk mencapai kapasitas maksimum.
b. Jumlah sel dan terminal : Sebuah jaringan WLAN harus mampu melayani ratusan terminal dan simpul jaringan yang tersebar di dalam banyak sel.

c. Koneksi ke jaringan LAN *backbone* : Dalam sebagian besar kasus, interkoneksi dengan jaringan *backbone* mutlak diperlukan agar hubungan ke terminal –terminal di dalam jaringan tersebut dapat dilakukan.

d. Jangkauan pelayanan : Area layanan tipikal untuk sebuah jaringan WLAN memiliki diameter 100 hingga 300 meter.

e. Daya tahan baterai : Implementasi jaringan WLAN yang tipikal harus menyertakan fitur-fitur yang dapat meminimalkan konsumsi daya, seperti misalnya menempatkan terminal dalam moda “tidur” (*sleep mode*) saat tidak mengakses jaringan.

f. Kehandalan dan kemanan transmisi : Rancang bangun sebuah jaringan WLAN harus mempertimbangkan kehandalan transmisi sebagai salah satu factor terpenting sehingga di dalam suatu ingkungan kerja yang sangat kenta noise pun transimisi masih dapat dilakukan dengan baik dan begitu pula keamanannya terhadap intrusi tetap terjamin.

g. Pengoperasian jaringan secara ko-lokasi : Dua buah jaringan LAN harus dapat di gunakan dalam satu lokasi yang sama tanpa terjadi intrusi-silang secara tidak sengaja oleh para pengguna masing-masing LAN.

h. Pengoperasian tanpa lisensi : Dengan tanpa adanya lisensi penggunan pita frekuensi tertentu untuk jaringan WLAN, maka akan semakin banyak calon pengguna yang berminat menggunakan jaringan WLAN.

i. Handoff / roaming : Protokol MAC yang digunkan di dalam sebuah jaringan WLAN harus memiliki kemampuan untuk mendukung perpindahan terminal terminal dari satu sel ke sel lainnya.

j. Konfigurasi dinamis : Aspek pengalamatan (addressing) dan manajemen jaringan WLAN harus memungkinkan penambahan, penghapusan dan relokasi sistem-sistem (terminal dan simpul) di dalam jaringan secara dinamis tanpa menganggu pengguna lainnya.

2.6.3 Kelebihan jaringan WLAN

Terdapat beberapa keuntungan yang didapat dari penggunaan WLAN, di antaranya:

a. Mobilitas tinggi : WLAN memungkinkan klien untuk mengakses informasi secara *real-time* dimanapun dalam jangkauan WLAN sehinga meningkatkan kualitas layanan dan produktifitas yang tidak mungkin dapat diberikan oleh jaringan LAN biasa.

b. Kemudahan dan kecepatan instalasi : instalasi WLAN sangat mudah dan cepat tanpa harus menarik dan memasang kabel melalui dinding atau atap. Kabel digunakan hanya untuk menghubungkan AP (*access point*) ke jaringan (HUB/*switch*/*router*).

c. *Fleksibel* : dengan teknologi WLAN, memungkinkan untuk membangun jaringan pada area yang tidak mungkin atau sulit untuk dijangkau oleh kabel. Seperti kota-kota besar, di tempat-tempat yang tidak tersedia infrastruktur kabel, WLAN dapat digunakan untuk mengatikan *leased-line*

d. Scalabel : WLAN dapat digunakan dengan berbagai topologi jaringan sesuai dengan kebutuhan instalasi atau spesifikasi, mulai dari jaringan independen

yang hanya terdiri dari beberapa klien saja, sampai jaringan infrastruktur yang terdiri dari beberapa klien saja, sampai jaringan infrastruktur yang terdiri dari ribuan klien.

e. Produktifitas : kapabilitas dalam hal komputasi merupakan syarat mutlak suatu korporasi agar produktifitas karyawannya dapat diandalkan. Dengan dukungan teknologi WLAN maka karyawan dapat selalu tersambung ke internet dalam keadaan mobile.

2.7 TCP/IP *Networking*

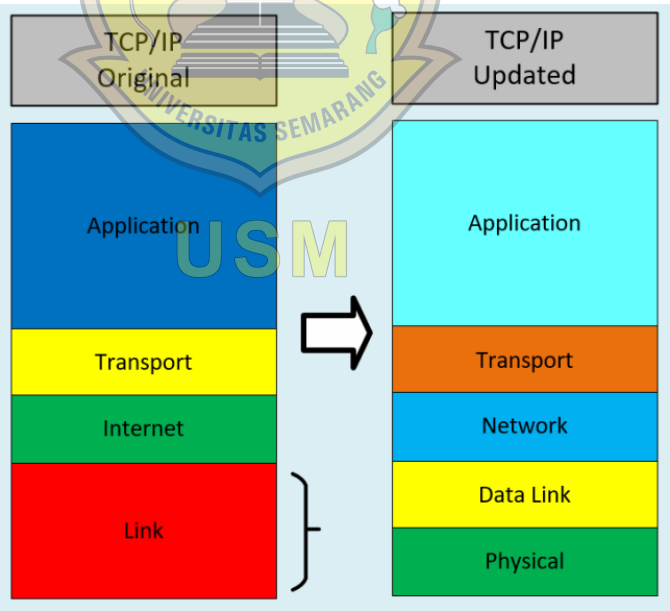
TCP/IP (*Transmission Control Protocol Internet Protokol*) digunakan pertama kali untuk menghubungkan komputer-komputer pemerintah (USA) dan berhubungan dengan kecocokannya dengan berbagai perangkat keras sistem operasi.

TCP/IP merupakan merupakan kurnpulan dari protokol-protokol yang digunakan untuk mengatur komunikasi data di dalarn jaringan Internet atau jaringan yang luas. TCP/IP digunakan untuk komu antarkornputer yang berada pada tempat yang jauh atau komunikasi data *Wide Area Network*, Semua komputer yang berhubungan dengan Internet akan berkomunikasi dengan mengguna protokol ini. Penggunaan protokol ini dapat menghubungkan berbagai jenis kornputer dengan sistern operasi berbeda.

Tujuan digunakannya TCP/IP adalah agar data atau informasi yang dikirimkan dapat sampai ke komputer dengan tepat. Dengan menggunakan protokol ini, data yang dikirimkan dapat terhindar dari kemungkinan hilangnya data tersebut ketika sampai ke komputer tujuan.

2.7.1 Lapisan – Lapisan TCP/IP

Dalam istilah umum komunikasi dapat di katakan melibatkan tiga agen : aplikasi, komputer dan jaringan. Contoh aplikasi termasuk perpindahan berkas dan surat elektronik. Aplikasi-aplikasi yang kita bahas disini adalah aplikasi-aplikasi tersebar melibatkan pertukaran data antara dua sistem komputer. Aplikasi-aplikasi ini dan yang lainnya berjalan pada komputer-komputer yang sering kali dapat mendukung aplikasi berganda secara simultan. Komputer terhubung ke jaringan dan data yang hendak di pertukarkan di pindahkan menggunakan jarinngan dari satu komputer ke komputer yang lain. Maka, perpindahan data dari satu aplikasi ke yang lain pertama-tama melibatkan perpindahan data ke komputer tempat aplikasi berada lalu memindahkan data ke aplikasi tujuan dalam komputer.



Gambar 2.5 TCP/IP *Layer* (Sumber : Wendell Odom, 2011)

Sambil mengingat konsep-konsep ini, kita dapat mengorganisasikan tugas komunikasi ke dalam lima lapisan yang relatif berdiri sendiri :

1. **Lapisan Fisik *(physical layer)***

Mencakup antarmuka fisik antara sebuah perangkat transmisi data (misal workstation, komputer) dan media transmisi atau jaringan. Lapisan ini berurusan menentukan karekteristik media transmisi, sifat sinyal, laju data dan masalah-masalah terkait lainnya.

2. **Lapisan akses jaringan *(network acces layer)***

Berkaitan dengan pertukaran data antara sistem akhir (*server, workstation* dan lain-lain) dan jaringan yang terhubung. Komputer pengirim harus menyediakan alamat komputer tujuan kepada jaringan, sehingga jaringan dapat merutekan data ke tujuan yang sesuai.

3. **Lapisan internet *(internet layer)***

Pada kasus-kasus ketika dua perangkat terhubung ke jaringan-jaringan berbeda diperlukan prosedur-prosedur untuk memungkinkan data melewati banyak jaringan yang saling terhubung. Internet protokol digunakan pada lapisan ini untuk menyediakan fungsi perutean melalui banyak jaringan. Protokol ini diimplementasikan tidak hanya pada sistem akhir tetapi juga dalam router. Router adalah pengolah yang menghubungkan dua jaringan dan fungsi utamanya adalah meneruskan data dari satu jaringan ke jaringan lain dalamm rutenya dari sistem akhir sumber menuju tujuan.

4. **Lapisan *host to host (tranport layer)***

Transport layer betugas untuk mengadakan kontak dan mengatur aliran data antara dua host atau komputer. Pada transport layer terdapat dua protokol, yaku TCP (*Transmosion Control Protocol*) dan UDP (*User Datagram Protocol*.

TCP melakukan pekerjaan pertama kali dengan membentuk hubungan dengan pengguna TCP yang lam. UDP hampir sama dengan TCP hanya dalam UDP tidak adanya pengurutan data yang datang dan tidak adanya pengiriman kembali jika data yang dikirim mengalami masalah di tengah jalan.

5. Lapisan aplikasi

Berisi logika yang diperlukan untuk mendukung berbagai aplikasi penguna. Untuk tiap jenis aplikasi berbeda seperti perpindahan berkas, modul terpisah diperlukan khusus untuk aplikasi tersebut.

2.8 Pengukuran QoS

Quality of Service (QoS) atau Kualitas layanan adalah metode pengukuran yang digunakan untuk menentukan kemampuan sebuah jaringan seperti; aplikasi jaringan, host atau router dengan tujuan memberikan network service yang lebih baik dan terencana sehingga dapat memenuhi kebutuhan suatu layanan.

Quality of Service (QoS) merupakan sebuah arsitektur end-to-end dan bukan merupakan sebuah fitur yang dimiliki oleh jaringan. QoS suatu jaringan merujuk pada tingkat kecepatan dan kehandalan penyampaian berbagai jenis data di dalam suatu komunikasi.

Melalui QoS seorang network administrator dapat memberikan prioritas trafik tertentu. QoS menawarkan kemampuan untuk mendefinisikan atribut-atribut layanan yang disediakan, baik secara kualitatif maupun kuantitatif. Tujuan QoS menyediakan kualitas layanan yang berbeda-beda berdasarkan kebutuhan layanan di dalam jaringan. Menurut Kamarulloh (2009), Quality of Service (QoS) adalah kemampuan memberikan pelayanan berbeda kepada lalu lintas jaringan dengan

kelas-kelas yang berbeda, dengan tujuan memberikan network service yang lebih baik dan terencana dengan dedicated bandwidth, jitter dan latency yang terkontrol dan meningkatkan loss karakteristik.

2.8.1 Manfaat dan Jenis Layanan QoS

Quality of Service (QoS) dalam penggunaanya memiliki beberapa manfaat, yaitu:

1. Memberikan prioritas untuk aplikasi-aplikasi yang kritis pada jaringan.
2. Memaksimalkan penggunaan investasi jaringan yang sudah ada.
3. Meningkatkan performansi untuk aplikasi-aplikasi yang sensitif terhadap delay, seperti Voice dan Video.
4. Merespon terhadap adanya perubahan-perubahan pada aliran trafik di jaringan.

QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. Parameter QoS mengacu pada performansi tingkat kecepatan dan keandalan penyampaian berbagai jenis data dalam komunikasi.

2.8.2 Parameter parameter QoS

Terdapat beberapa parameter Quality of Service (QoS), yaitu sebagai berikut:

2.8.2.1 Throughput

Throughput adalah kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data. Biasanya throughput selalu dikaitkan dengan bandwidth dalam kondisi yang sebenarnya. Bandwidth lebih bersifat tetap, sementara throughput sifatnya adalah dinamis tergantung trafik yang sedang

terjadi. Throughput adalah kecepatan (rate) transfer data efektif yang diukur dalam bps. Throughput merupakan jumlah total kedatangan paket yang sukses yang diamati pada destination selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. Dalam bentuk matematis throughput dapat dirumuskan sebagai berikut :

$$Througtput = \frac{JUMLAH\ \ BIT\ YANG\ DIKIRIM}{TOTAL\ WAKTU\ PENGIRIMAN} \quad \text{.....(2.1)}$$

(Sumber : TIPHON dalam FATONI)

Secara umum terdapat empat kategori penurunan performansi jaringan berdasarkan nilai Throughput sesuai dengan standar TIPHON *(Telecommunications and Internet Protocol Harmonization Over Networks)* yaitu seperti tampak pada tabel berikut:

Tabel 2.2 Standar *Throughput*

KATEGORI THROUGHPUT	**THROUGHPUT (X)**
Buruk	0-338 kbps
Cukup Baik	338-700 kbps
Baik	700-1200 kbps
Lebih Baik	1200 kbps- 2.1 Mbps
Terbaik	>2.1 Mbps

(Sumber : TIPHON, 1999)

2.8.2.2 Packet loss

Packet loss adalah parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang. Paket yang hilang ini dapat terjadi karena collision dan congestion pada jaringan. Packet Loss merupakan kegagalan transmisi paket data mencapai tujuannya yang disebabkan oleh beberapa kemungkinkan, antara lain yaitu:

- Terjadinya overload trafik didalam jaringan.
- Tabrakan (congestion) dalam jaringan.
- Error yang terjadi pada media fisik.
- Kegagalan yang terjadi pada sisi penerima antara lain bisa disebabkan karena Overflow yang terjadi pada buffer.

Packet loss dapat terjadi karena kesalahan yang diperkenalkan oleh medium transmisi fisik. Hal hal yang mempengaruhi terjadinya packet loss juga bisa karena kondisi geografis seperti kabut, hujan, gangguan radio frequensi, sel handoff selama roaming, dan interferensi seperti pohon-pohon, bangunan, dan pegunungan.

Packet Loss dihitung berdasarkan persentase paket yang berhasil dikirim, dirumuskan sebagai berikut:

$$Packet\ Loss = \frac{Data\ Yang\ Dikirim - Data\ Yang\ Diterima}{Paket\ Data\ Yang\ Dikirirm} \text{ x } 100\ \% \quad \text{.....(2.2)}$$

(Sumber : TIPHON dalam FATONI)

Adapun standar packet loss menurut TIPHON adalah sebagai berikut:

Tabel 2.3 Standar *Packet Loss*

KATEGORI PACKET LOSS	PACKET LOSS (%)
Sangat Bagus	0 - 2 %
Bagus	3 - 14 %
Sedang	15 – 25 %
Jelek	>25 %

(Sumber : TIPHON, 1999)

2.8.2.3 Delay / Latency

Delay (*latency*) adalah waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik menuju titik lain yang menjadi tujuannya. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama. Waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. *Delay* diperoleh dari selisih waktu kirim antara satu paket TCP dengan paket lainnya yang direpresentasikan dalam satuan *second*.

Rumus untuk menghitung nilai *delay* adalah :

$$\text{Rata-Rata Delay} = \frac{Total\ Delay}{Total\ Paket\ Yang\ Diterima} \quad \text{.....(2.3)}$$

(Sumber : TIPHON dalam FATONI)

Tabel 2.4 Standar *Delay*

KATEGORI LATENSI	BESAR *DELAY*
Sangat Bagus	< 150 ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Jelek	> 450 ms

(Sumber : TIPHON, 1999)