BAB II

TINJAUAN PUSTAKA

2.1 Profil Instansi

Balai Besar Keramik adalah unit pelaksana teknis di bawah Badan Penelitian dan Pengembangan Industri, Departemen Perindustrian yang bertanggung jawab kepada Kepala Badan Penelitian dan Pengembangan Industri.

2.1.1 Sejarah Instansi

Pada tahun 1922 didirikan Keramische Laboratorium oleh Pemerintah Kolonial Belanda. Lalu tahun 1942 Keramische Laboratorium diambil alih oeh Jepang. Dan pada 1945 diambil alih kembali oleh Pemerintah Indonesia, namanya diganti menjadi Balai Penyelidikan Keramik. Lalu pada tahun 1980 instansi tersebut direorganisasi dan namanya diganti kembali menjadi Balai Besar Penelitian dan Pengembangan Industri Keramik, dan pada akhirnya namanya menjadi Balai Besar Keramik.

2.1.2 Tempat dan Kedudukan Instansi

Nama : Balai Besar Keramik

Alamat : Jalan Jendral Ahmad Yani No. 392 Bandung

Kode Pos : 40272

2.1.3 Tugas dan Fungsi

Balai Besar Keramik mempunyai tugas dan fungsi untuk melaksanakan dan penelitian, pengembangan, kerjasama, standardisasi, pengujian, sertifikasi, kalibrasi, dan pengembangan kompetensi industri keramik sesuai dengan kebijaksanaan teknis Kepala Badan Penelitian dan Pengembangan Industri.

2.1.4 Visi dan Misi

Visi dari Balai Besar Keramik adalah menjadi lembaga professional dalam memberikan jasa teknologi keramik di Indonesia.

Misi dari balai Besar Keramik adalah :

a. Melaksanakan litbang di bidang teknologi terapan dan standardisasi untuk industry keramik dan industri pengguna keramk.

b. Memberikan pelayanan teknis di bidang litbang, pelatihan, pengujian, konsultasi, sertifikasi dan perekayasaan peralatan industri yang memuaskan pelanggan.

2.1.5 Logo Instansi

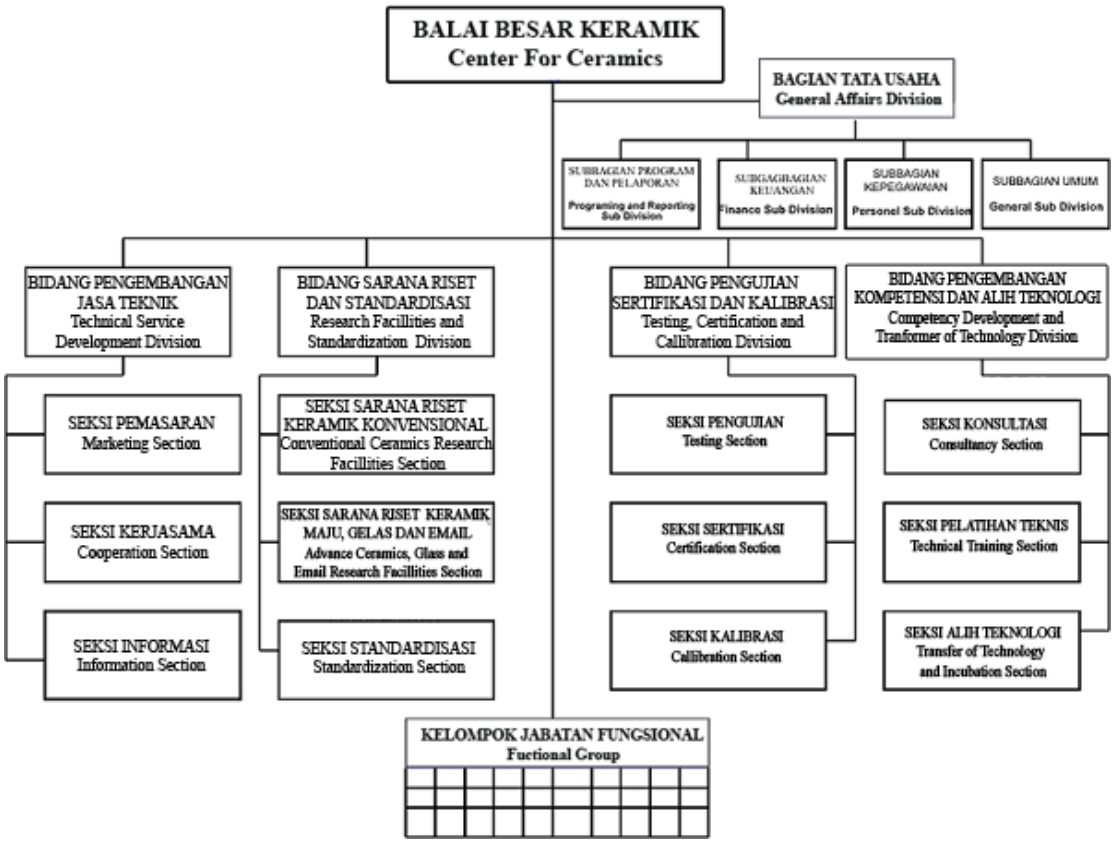
Berikut ini adalah logo dari Balai Besar Keramik :



Gambar 2.1 Logo Balai Besar Keramik

2.1.6 Struktur Organisasi

Berikut ini adalah struktur organisasi dari Balai Besar Keramik :



Gambar 2.2 Stuktur Organisasi

2.2 Jaringan Komputer

Menurut definisi, jaringan komputer merupakan sejumlah komputer yang dapat saling berkomunikasi. Dalam komunikasi ini dapat terjadi perpindahan data ataupun berbagi sumber daya. Dalam skala luas, internet juga merupakan jaringan komputer. Jadi, suatu jaringan komputer tidak hanya terjadi pada sejumlah komputer yang terdapat pada suatu ruangan ataupun suatu gedung atau perusahaan. Pada dasarnya teknologi jaringan komputer itu sendiri merupakan perpaduan antara teknologi komputer dan juga teknologi komunikasi.[1]

Pembangunan jaringan komputer dapat mencegah ketergantungan pada komputer pusat. Setiap proses data tidak harus dilakukan pada satu komputer saja, melainkan dapat didistribusikan ke tempat lainnya. Sehingga dapat terbentuk data yang terintegrasi dengan demikian memudahkan pemakai untuk memperoleh dan mengolah informasi setiap saat. Dengan adanya jaringan komputer ini, maka pengembangan peralatan dapat dilakukan dengan mudah dan menghemat biaya. Jaringan komputer dapat memudahkan pemakai dalam merawat Central Processing Unit (CPU), misalnya untuk memberikan perlindungan terhadap serangan virus, maka pemakai cukup memusatkan perhatian pada CPU yang ada di komputer pusat.

Sistem jaringan komputer memberikan perlindungan terhadap data. Jaminan keamanan data tersebut diberikan melalui pengaturan hak akses para pemakai dan password, serta teknik perlindungan terhadap hardisk sehingga data mendapatkan perlindungan yang efektif. Dengan adanya pemakaian sumber daya secara bersama-sama, maka pemakai bisa mendapatkan hasil dengan maksimal dan kualitas yang tinggi. Selain itu data atau informasi yang diakses selalu terbaru, karena setiap ada perubahan yang terjadi dapat segera lengsung diketahui oleh setiap pemakai.[7]

2.2.1 Jenis Jaringan Komputer

Berdasarkan ruang lingkup geografis terdapat empat jenis jaringan komputer, antara lain :

2.2.1.1 Local Area Network (LAN)

Jarak jangkauan Local Area Network (LAN) tidak terlalu jauh. Biasanya diterapkan pada suatu gedung atau antar gedung dalam suatu kompleks perkantoran atau sekolah. Suatu Local Area Network (LAN), adalah jaringan yang dibatasi oleh area yang lebih kecil, umumnya dibatasi oleh area lingkungan seperti sebuah sekolah dan biasanya dari sekitar 1 kilometer persegi. Beberapa model konfiguarasi LAN biasanya berupa satu komputer yang biasanya dijadikan

sebuah file server, yang digunakan untuk menyimpan perangkat lunak (software yang mengatur aktifitas jaringan), ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer-komputer yang terhubung kedalam jaringan lokal. Komputer-omputer yang terhubung kedalam sebuah file server itu biasanya disebut workstation.[1]

2.2.1.2 Metropolitan Area Network

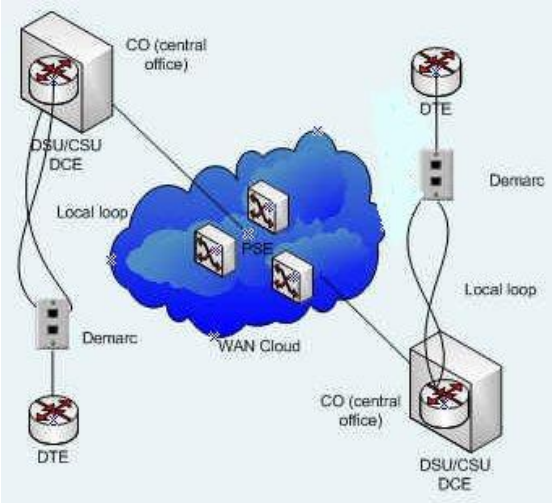
MAN biasanya meliputi area yang lebih besar dari LAN, area yang digunakan adalah dalam sebuah negara.Dalam hal ini jaringan komputer menghubungkan beberapa buah jaringan-jaringan LAN ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu: jaringan pada Bank (sistem Online Perbankan). Setiap bank tentunya memiliki kantor pusat dan kantor cabang. Di setiap kantor baik kantor cabang maupun kantor pusat tentunya memiliki LAN, penggabungan LAN – LAN di setiap kantor ini akan membentuk sebuah MAN. MAN biasanya mampu menunjang data teks dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel atau gelombang radio.[1]

2.2.1.3 Wide Area Network (WAN)

Jaringan Wide Area Network (WAN) mempunyai cakupan terluas, bahkan dapat dikatakan mencakup seluruh dunia. Jaringan ini sendiri dapat dihubungkan dengan menggunakan satelit dan media kabel fiber optic.

Jenis koneksi WAN normalnya tergantung pada layanan yang bisa diberikan oleh penyedia WAN, dan juga berhubungan dengan jenis interface fisik yang dipakai untuk menghubungkan router. Ada banyak sekali jenis koneksi, akan tetapi jika memungkinkan pilihlah jenis koneksi yang teknologinya bisa mendukung data rate yang lebih tinggi dan mendukung konfigurasi yang fleksibel.

Gambar dibawah ini adalah struktur koneksi WAN yang umum dipakai :



Gambar 2.3 Struktur Koneksi WAN

2.3 Arsitektur Jaringan

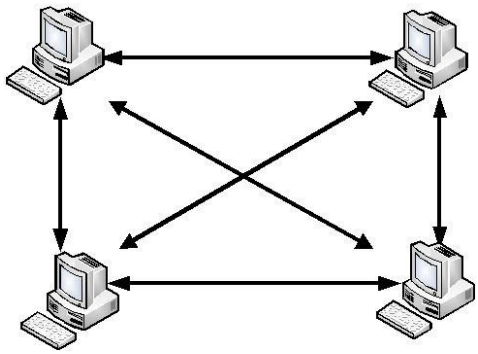
Arsitektur jaringan komputer merupakan tata cara penggunaan perangkat keras dan perangkat lunak dalam jaringan agar satu komputer dengan komputer lainnya dapat melakukan komunikasi dan pertukaran data.

Keamanan sistem jaringan komputer adalah bagian tak terpisahkan dari keamanan sistem komputer sebuah organisasi secara keseluruhan, terutama dengan semakin berkembangnya Internet. Semakin banyak aplikasi pengguna yang berbasiskan pada jaringan komputer. Jika sebuah jaringan komputer tidak aman, maka sistem komputer pada organisasi tersebut juga tidak aman.[1]

2.3.1 Peer-to-Peer Networks

Model hubungan peer-to-peer atau gateway to gateway memungkinkan user membagi sumber dayanya yang ada di komputernya baik itu berupa file, layanan printer dan lain-lain serta mengakses sumber daya yang terdapat pada komputer lain.namun model ini tidak mempunyai sebuah file server atau sumber daya yang terpusat. Didalam model hubungan peer-to-peer ini , seluruh komputer adalah sama, yang mana mempunyai kemampuan yang sama untuk memakai

sumber daya yang tersedia. Model ini di disain untuk jaringan berskala kecil dan menengah.



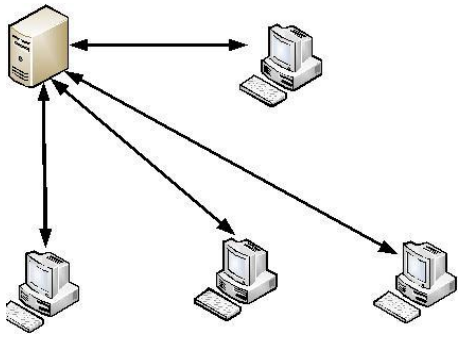
Gambar 2.4 Model hubungan peer-to-peer

Kelebihan dan kekurangan model topologi peer-to-peer:

1. Kelebihan model topologi peer-to-peer :
    a. Tidak terlalu mahal, karena tidak membutuhkan dedicated file server
    b. Mudah dalam konfigurasi programnya, hanya tinggal mengatur untuk operasi model hubungan peer to peer
2. Kekurangan model topologi peer-to-peer :
    a. Tidak terpusat, terutama untuk penyimpanan data dan aplikasi
    b. Tidak aman, karena menyediakan fasilitas untuk keperluan itu.

2.3.2 Client-Server Networks

Model hubungan client server atau host to gateway memungkinkan memungkinkan jaringan untuk mensentralisasi fungsi dan aplikasi kepada satu atau dua dedicated file server. Sebuah file server menjadi jantung dari keseluruhan sisetm, memungkinkan untuk mengakses sumber daya, dan menyediakan keamanan. Workstation yang berdiri sendiri dapat mengambil sumber daya yang ada pada file server. Model hubungan ini, menyediakan mekanisme untuk mrngintegrasikan seluruh kompoen yang ada di jaringan dan memungkinkan banyak pengguna secara bersama-sama memakai server.



Gambar 2.5 Model hubungan Client server

Kelebihan dan kekurangan model topologi client server:

1. Kelebihan model topologi client server :

   a. Terpusat (sumber daya dan keamanan data dikontrol melaui server)

   b. Skalabilitas

   c. Fleksibilitas

   d. Teknologi baru dengan mudah terintegrasi kedalam sistem

   e. Keseluruhan komponen client/network/server dapat bekerja bersama

2. Kekurangan model topologi client server:

   a. Mahal

   b. Membutuhkan investasi untuk dedicated file server

   c. Perbaikan (jaringan besar membutuhkan seorang staf untuk mengatur agar sistem berjalan secara efisien)

   d. Ketika server down, mengakibatkan keseluruhan operasi pada network akan down juga.

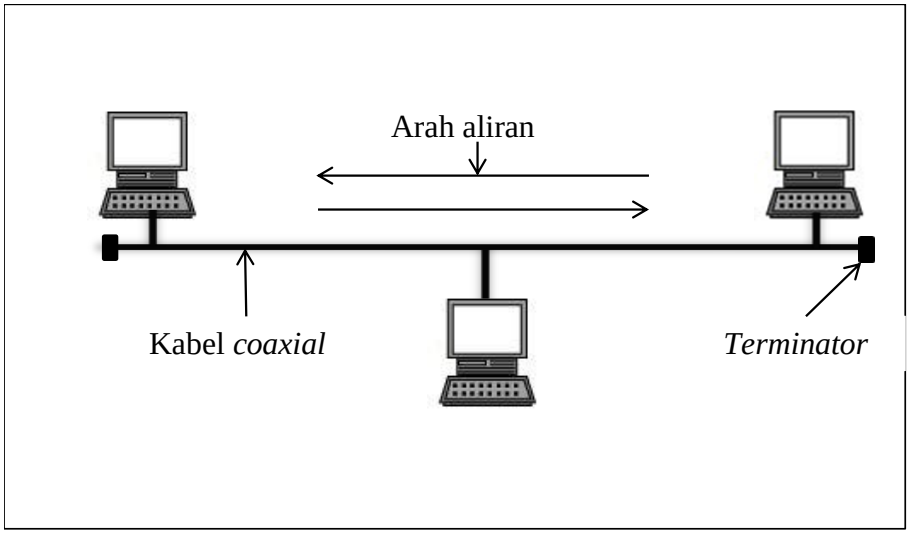
2.4 Topologi Jaringan

Topologi jaringan adalah suatu aturan/rules bagaimana menghubungkan komputer (node) satu sama lain secara fisik dan pola hubungan antara komponen-komponen yang berkomunikasi melalui media/peralatan jaringan, seperti: server, workstation, hub/switch, dan pengabelanya (media transimisi data). Ketika kita memutuskan untuk memilih suatu topologi maka kita perlu mengikuti beberapa spesifikasi tertentu.[1]

Ada dua macam jenis topologi, yaitu physical topology (topologi fisik) dan logical topology (topologi logika). Topologi fisik adalah bentuk jaringan seperti bagaimana memilih perangkat jaringan dan melakukan instalasi perangkat jaringan. Sedangkan topologi logika adalah bagaimana data mengalir di dalam topologi fisik. Ada beberapa macam topologi jaringan berikut penjelasannya:

1) Topologi Bus

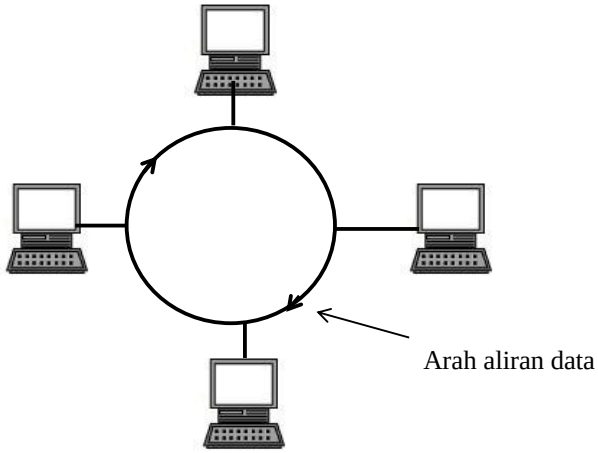
Topologi bus sering disebut daisy chain atau ethernet bus topologies. Sebutan terakhir diberikan karena perangkat jaringan yang digunakan pada topologi ini adalah NIC (Network Interface Card) bernama ethernet. Topologi bus dapat dikenali dari penggunaan sebuah kabel backbone (kabel utama) yang mengghubungkan semua peralatan jaringan. Apabila kabel utama terputus akan menyebabkan jaringan mati total, karena kabel backbone (kabel utama) merupakan satu-satunya jalan bagi lalu lintas data. Artinya, apabila salah satu sambungan terputus maka seluruh sambungan akan ikut terputus juga.



Gambar 2.6 Topologi *Bus*

2) Topologi Ring

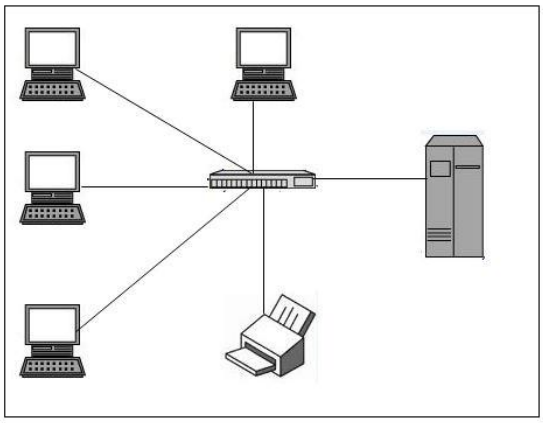
Topologi ring menggunakan kabel backbone (kabel utama) yang berbentuk cincin. Setiap komputer terhubung dengan kabel backbone, pada ujung kabel akan dihubungkan kembali dengan komputer pertama.



Gambar 2.7 Topologi Ring

3) Topologi Star

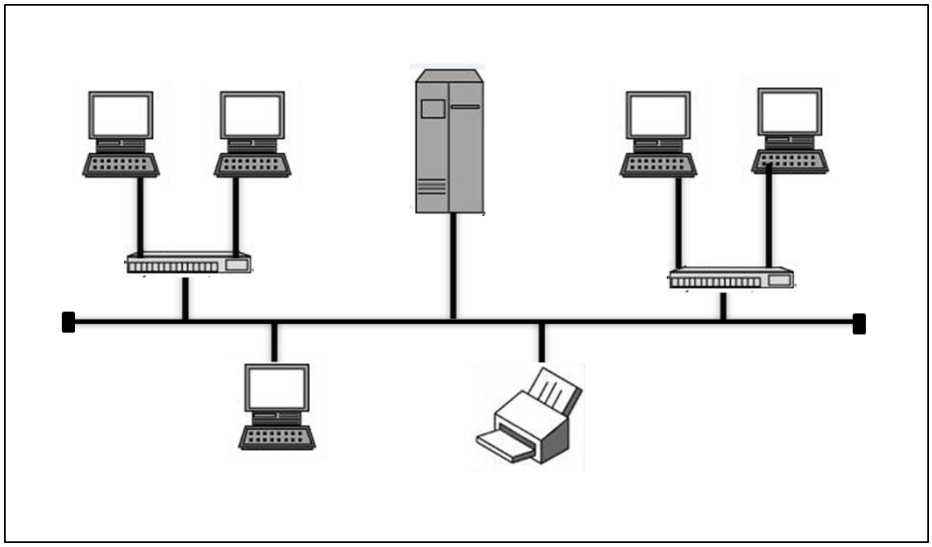
Topologi star menggunakan hub sebagai sebuah sentral yang digunakan untuk menghubungkan semua node. Setiap node menggunakan sebuah kabel UTP atau STP yang dihubungkan dari ethernet card ke hub. Topologi ini banyak digunakan untuk jaringan rumahan, perkantoran, sekolah dan lain-lain.



Gambar 2. 8 Topologi *Star*

4) Topologi Tree

Topologi tree disebut juga sebagai topologi star-bus, topologi ini merupakan penggabungan antara topologi star dan bus. Topologi tree digunakan untuk menghubungkan beberapa LAN dengan LAN lain. Media penghubung antar LAN yaitu menggunakan hub, masing-masing hub merupakan akar dari masing-masing pohon. Topologi ini dapat mengatasi permasalahan pada topologi bus yaitu masalah broadcast traffic, dan permasalahan pada topologi star yaitu keterbatasan kapasitas port hub.[7]



Gambar 2. 9 Topologi *Tree*

2.5 Perangkat Jaringan

Perangkat jaringan adalah sejumlah perangkat yang digunakan dalam jaringan sebagai pemecah jaringan (contoh: hub, bridge, switch), mengatur perutingan jaringan (contoh: router), penguat jaringan (contoh: repeater), pengkonfersi data jaringan (contoh: modem), interface end user dengan jaringan (NIC & wireless adapter).[1]

1. Hub

Hub merupakan perangkat yang dapat menggandakan frame data yang berasal dari salah satu komputer ke semua port yang terdapat pada hub tersebut. Sehingga semua komputer yang terhubung dengan port hub akan menerima data juga.

2. Switch

   Switch bekerja pada lapisan Data Link seperti halnya Bridge. Cara kerja switch sebetulnya mirip dengan Bridge, tetapi switch memiliki sejumlah port sehingga switch sering disebut juga multiport bridge.

3. Reapeter

   Repeater merupakan contoh dari active hub. Repeater merupakan perangkat yang dapat menerima sinyal, kemudian memperkuat dan mengirim kembali sinyal tersebut ke tempat lain. Sehingga sinyal dapat menjangkau area yang lebih jauh.

4. Bridges

   Bridge merupakan peralatan yang dapat menghubungkan beberapa segmen dalam sebuah jaringan. Berbeda dengan hub, bridge dapat mengenalai MAC Address tujuan.

5. Router

   Router adalah peralatan jaringan yang dapat menghubungkan satu jaringan dengan jaringan yang lain. Sepintas lalu, router mirip dengan bridge, namun router lebih “cerdas” dibandingkan dengan bridge. Router bekerja dengan routing table yang disimpan di memorinya untuk membuat keputusan kemana dan bagaimana paket dikirimkan. Router dapat memutuskan route terbaik yang akan ditempuh oleh paket data. Router akan memutuskan media fisik jaringan yang “disukai” dan “tidak disukai”. Protokol routing dapat mengantisipasi berbagai kondisi yang tidak dimiliki oleh peralatan bridge. Router bekerja pada layer network. Router adalah peralatan yang bekerja pada

layer 3 Open System Interconnection (OSI) dan sering digunakan untuk menyambungkan jaringan luas Wide Area Network (WAN) atau untuk melakukan segmentasi layer 3 di LAN. WAN seperti halnya LAN juga beroperasi di layer 1, 2 dan 3 OSI sehingga router yang digunakan untuk menyambungkan LAN dan WAN harus mampu mendukung. Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router-router yang saling terhubung dalam jaringan internet turut serta dalam sebuah algoritma routing terdistribusi untuk menentukan jalur terbaik yang dilalui paket IP dari system ke sistem lain. Proses routing dilakukan secara hop by hop. IP tidak mengetahui jalur keseluruhan menuju tujuan setiap paket. IP routing hanya menyediakan IP address dari router berikutnya yang menurutnya lebih dekat ke host tujuan. Router dapat disetting menjadi gateway dimana ia menjadi penghubung antara jaringan local dengan jaringan luar. Gateway adalah pintu gerbang sebagai keluar-masuknya paket data dari local network menuju outer network. Tujuannya agar client pada local network dapat berkomunikasi dengan internet.

6. NIC

   NIC merupakan peralatan jaringan yang langsung berhubungan dengan komputer dan didesain agar komputer-komputer dalam jaringan dapat saling berkomunikasi. NIC juga menyediakan akses ke media fisik jaringan. NIC bekerja pada layer fisik OSI.

7. Modem

   Modem berasal dari singkatan MOdulator DEModulator. Modulator merupakan bagian yang mengubah sinyal informasi kedalam sinyal pembawa (Carrier) dan siap untuk dikirimkan, sedangkan Demodulator adalah bagian yang memisahkan sinyal informasi (yang berisi data atau pesan) dari sinyal pembawa (carrier) yang diterima sehingga informasi tersebut dapat diterima

dengan baik. Modem merupakan penggabungan kedua-duanya, artinya modem adalah alat komunikasi dua arah.

8. Wireless Adapter

Wireless Adapter pada prinsipnya mirip dengan NIC. Hanya saja wireless adapater merupakan interface end user ke jaringan wireless. Pada laptop-laptop jenis baru, wireless adapter sudah terintegrasi di dalamnya, dan biasa disebut PCMCIA. Untuk laptop dan PC yang belum tersedia, dapat digunakan wireless external.[7]

2.6 Media Transmisi

Media transmisi merupakan media yang digunakan untuk mentransmisikan data dari satu komputer ke komputer lain atau dari server ke client di dalam jaringan. Dalam jaringan komputer, kabel merupakan media penghubung utama. Berikut macam-macam kabel yang sering digunakan pada jaringan LAN.[1]

1. Kabel Coaxial

Kabel coaxial adalah kabel yang memiliki satu copper conductor pada bagian tengahnya. Sebuah lapisan plastik menutupi diantar konduktor dan lapisan pengaman serat besi. Lapisan serat besi tersebut membantu menutupi konduktor dari gangguan seperti dari arus listrik, lalu lintas kendaraan atau mesin dan komputer. Kelemahan kabel coaxial ini yaitu, sulit dalam konfigurasi dan tidak tahan terhadap sinyal-sinyal tertentu seperti sinyal radio. Kelebihannya yaitu dapat memiliki ukuran yang lebih panjang dalam satu jaringan dibandingkan dengan kabel UTP. Ada dua jenis kabel coaxial yaitu thick-coaxial dan thin-coaxial.

2. Kabel UTP (Unshielded Twisted Pair)

Kabel UTP adalah jenis kabel yang paling populer dan umumnya merupakan pilihan terbaik untuk jaringan sederhana. Terdapat empat macam kabel

didalamnya dan konektor yang digunakan untuk kabel UTP ini adalah konektor RJ-45.

3. Kabel STP (Shielded Twisted Pair)

Kabel STP biasa digunakan pada topologi Token Ring, kabel ini sangat sensistif terhadap sinyal radio dan arus listrik. Biasanya kabel jenis ini digunakan pada jaringan yang kurang pengaruh listriknya

4. Kabel Fiber Optic

Kabel jenis ini mempunyai kemampuan mentransmisikan sinyal pada jarak yang relatif lebih jauh dibandingkan dengan kabel coaxial atau kabel UTP. [7]

2.7 Komunikasi Data

Komunikasi data merupakan bagian dari telekomunikasi yang secara khusus berkenaan dengan transmisi atau pemindahan data dan informasi diantara komputer – komputer dan piranti-piranti yang lain dalam bentuk digital yang dikirimkan melalui media komunikasi data. Data berarti informasi yang disajiakan oleh isyarat digital. Komunikasi data merupakan bagian vital dari suatu masyarakat informasi karena sistem ini menyediakan infrastruktur yang memungkinkan komputer-komputer dapat berkomunikasi satu sama lain. Berikut adalah komponen dari komunikasi data:

1. Pengirim, merupakan piranti yang mengirimkan data
2. Penerima, merupakan piranti yang menerima data
3. Data, merupakan informasi yang akan dipindahkan
4. Media pengiriman, merupakan media atau saluran yang digunakan untuk mengirimkan data
5. Protokol, adalah aturan-aturan yang digunakan untuk mengatur jalannya komunikasi data antara beberapa komputer yang terdapat dalam suatu jaringan. Supaya perangkat yang berlainan itu dapat berkomunikasi, mengirim ataupun menerima maka dibutuhkan suatu pengertian. Maka dengan protokol semua itu bisa terjadi [1].

2.8 Keamanan Jaringan

Perkembangan teknologi jaringan komputer menyebabkan terkaitnya satu komputer dengan komputer lainya. Hal ini membuka banyak peluang dalam pengembangan aplikasi komputer tetapi juga mebuat peluang adanya ancaman terhadap pengubahan dan pencurian data. Sebuah aplikasi yang melintasi jaringan publik seperti internet diasumsikan dapat diakses oleh siapapun termasuk orang-orang atau pihak-pihak yang memang berniat untuk mencuri atau mengubah data. Oleh karena itu, untuk melindungi data terhadap akses, pengubahan dan penghalangan yang tidak dilakukan oleh pihak yang berwenang, peranti keamanan data yang melintas di jaringan komputer harus disediakan [2].

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh person yang tidak diijinkan. Sistem jaringan komputer memberikan perlindungan terhadap data. Jaminan keamanan data tersebut diberikan melelui pengaturan hak akses para pemakai dan password, serta teknik perlindungan terhadap hardisk sehingga data mendapatkan perlindungan yang efektif. Dengan adanya pemakaian sumber daya secara bersama-sama, maka pemakai bisa mendapatkan hasil dengan maksimal dan kualitas yang tinggi. Selain itu data atau informasi yang diakses selalu terbaru, karena setiap ada perubahan yang terjadi dapat segera lengsung diketahui oleh setiap pemakai.

Prinsip keamanan jaringan dapat dibedakan menjadi tiga, yaitu :

a. Kerahasiaan

Kerahasiaan berhubungan dengan hak akses untuk membaca data atau informasi dan suatu sistem computer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat dibaca oleh pihak yang telah diberi hak atau wewenang secara legal.

b. Integritas (integrity)

Integrity berhubungan dengan hak akses untuk mengubah data atau informasi dari suatu sistem computer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat diubah oleh pihak yang telah diberi hak.

c. Ketersediaan (availability)

Availability berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi yang terdapat pada sistem komputer dapat diakses dan dimanfaatkan oleh pihak yang berhak.

d. Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli. Untuk membuktikan keaslian dokumen dapat dilakukan dengan teknologi watermarking dan digital signature. Sedangkan untuk menguji keaslian orang atau server yang dimaksud bisa dilakukan dengan menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

e. Akses Kontrol

Aspek kontrol merupakan fitur-fitur keamanan yang mengontrol bagaimana user dan sistem berkomunikasi dan berinteraksi dengan system dan sumberdaya yang lainnya. Akses kontrol melindungi sistem dan sumberdaya dari akses yang tidak berhak dan umumnya menentukan tingkat otorisasi setelah prosedur otentikasi berhasil dilengkapi. Kontrol akses adalah sebuah term luas yang mencakup beberapa tipe mekanisme berbeda yang menjalankan fitur kontrol akses pada sistem komputer, jaringan, dan informasi. Kontrol akses sangatlah penting karena menjadi satu dari garis pertahanan pertama

yang digunakan untuk menghadang akses yang tidak berhak ke dalam sistem dan sumberdaya jaringan.

f. Non-Repudiation

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Penggunaan digital signature, certificates, dan teknologi kriptografi secara umum dapat menjaga aspek ini. Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari digital signature itu jelas legal.

2.8.1 Serangan Terhadap Keamanan Jaringan

Serangan keamanan jaringan yang dioperasionalkan pada jaringan publik rentan terhadap serangan oleh pihak yang tidak berwenang. Serangan terhadap sistem keamanan jaringan bertujuan untuk mengalahkan tujuan layanan keamanan jaringan . misalnya penyerang ingin mengungkap isi teks asli sehingga ia dapat mengungkap teks sandi lainya. Secara umum serangan pada sistem keamanan jaringan dapat dikategorikan menjadi 2 jenis, yaitu serangan pasif dan serangan aktif.[2]

1. Serangan Pasif

Pada seragnan pasif, penyerang hanya mengumpulkan data yang melintas pada jaringan publik (jaringan yang bisa diakses oleh semua orang). Serangan pasif tidak melakukan modifikasi data yang melintas atau merusak sistem, penyerang hanya bisa membaca (read only). Berdasarkan data yang dikumpulkan tadi penyerang melakukan analisis untuk menggagalkan tujuan layanan keamanan jaringan. Karena tidak melakukan modifikasi dan mengganggu sistem, serangan pasif sulit di deteksi, tapi dapat dicegah dengan cara menggunakan sandi pada saat mengirim pesan misalnya. Berikut beberapa jenis serangan pasif:

a. Snooping, merupakan kegiatan yang bermaksud untuk mendapatkan data yang sedang dikirimkan melalui jaringan oleh pihak yang tidak berwenang. Contoh kegiatan snooping yaitu penyadapan email, snooping

ini bisa dicegah dengan cara menyandikan pesan menggunakan mekanisme penyandian (enchiperment)

b. Traffic Analysis, merupakan kegiatan serangan dengan melakukan pemantauan terhadap lalu lintas jaringan untuk kemudian datanya dikumpulkan dan dianalisis untuk mendapatkan informasi dari data – data tersebut.

2. Serangan Aktif

Serangan aktif dapat mengakibatkan perubahan data yang sedang dikirimkan melaui jaringan dan mengganggu sistem. Serangan pasif memungkinkan penyerang untuk mengubah data pada lalu lintas data dijaringan. Jenis – jenis serangan aktif adalah sebagai berikut:

a. Masquerade, merupakan serangan aktif yang dilakukan oleh penyerang dengan cara mengambil alih (menirukan) perilaku pengirim atau penerima. Contohnya pada saat Andi ingi membuat kunci bersama dengan Budi, disaat yang bersamaan secara tidak sadar Rani mengambil alih peran Budi sehingga Andi mengirim pesan ke Rani bukan kepada Budi.
b. Modification, merupakan serangan dengan cara mengambil alih jalur komunikasi untuk mengubah atau menghapus pesan yang sedang dikirimkan untuk keuntungan penyerang. Misalnya pesan “kirim Rp 100.000, 00 ke nomer rekening Andi” dirubah oleh Rani menjadi “kirim Rp 100.000, 00 ke nomer rekening Rani”.
c. Replay, merupakan serangan yang terdiri dari pencatatan secara pasif data dan transmisi ulang untuk menimbullkan efek yang diinginkan oleh penyerang. Misalnya Rani pernah meminta Budi untuk mengirim Rp 100.000, 00 ke Rani, lalu Budi mengirim pesan “kirim Rp 100.000, 00 ke Rani” ke Bank, pada saat pesan dikirimkan Rani mencatat pesan “kirim Rp 100.000, 00 ke Rani” lalu mengirim ulang pesan tersebut ke Bank sehingga Rani mendapat uang dengan jumlah dua kali lebih besar.
d. Denial of Service, merupakan jenis serangan yang bertujuan menyebabkan sistem menjadi tidak dapat bekerja sama sekali sehingga tidak bisa

memeberikan pelayanan yang seharusnya kepada pengguna. Contohnya adalah penyerang membuat permintaan kosong (dummy) sehingga server menjadi overload.

Biasanya sebuah sistem keamanan jaringan dikatakan aman apabila tahan terhadap serangan aktif. Untuk mengembangkan sistem keamanan yang baik, seorang perancang keamanan jaringan harus menganalisis kemungkinan serangan-serangan terhadap layanan keamanan jaringan. [2]

2.8.2 Bentuk Ancaman

1. Brute Force Attack

Jenis ancaman keamanan jaringan ini lebih umum disebut sebagai Brute Force and Dictionary, serangan ini adalah upaya masuk ke dalam jaringan dengan menyerang database password atau menyerang login prompt yang sedang active. Serangan masuk paksa ini adalah suatu upaya untuk menemukan password dari account user dengan cara yang sistematis mencoba berbagai kombinasi angka, huruf, atau symbol. Sementara serangan dengan menggunakan metoda kamus password adalah upaya menemukan password dengan mencoba berbagai kemungkinan password yang biasa dipakai user secara umum dengan menggunakan daftar atau kamus password yang sudah di-definisikan sebelumnya.

Untuk mengatasi serangan keamanan jaringan dari jenis ini anda seharusnya mempunyai suatu policy tentang pemakaian password yang kuat diantaranya untuk tidak memakai password yang dekat dengan kita missal nama, nama anak, tanggal lahir dan sebagainya. Semakin panjang suatu password dan kombinasinya semakin sulit untuk diketemukan. Akan tetapi dengan waktu yang cukup, semua password dapat diketemukan dengan metoda brute force ini.

2. Denial of Services (DoS)

Deniel of Services (DoS) ini adalah salah satu ancaman keamanan jaringan yang membuat suatu layanan jaringan jadi mampet, serangan yang membuat jaringan anda tidak bisa diakses atau serangan yang membuat system anda tidak

bisa memproses atau merespon terhadap traffic yang legitimasi atau permintaan layanan terhadap object dan resource jaringan. Bentuk umum dari serangan Denial of Services ini adalah dengan cara mengirim paket data dalam jumlah yang sangat bersar terhadap suatu server dimana server tersebut tidak bisa memproses semuanya. Bentuk lain dari serangan keamanan jaringan Denial of Services ini adalah memanfaatkan telah diketahuinya celah yang rentan dari suatu operating system, layanan-2, atau applikasi-2. Exploitasi terhadap celah atau titik lemah system ini bisa sering menyebabkan system crash atau pemakaian 100% CPU. Tidak semua Denial of Services ini adalah merupakan akibat dari serangan keamanan jaringan. Error dalam coding suatu program bisa saja mengakibatkan kondisi yang disebut DoS ini. Disamping itu ada beberapa jenis DoS seperti:

3. Spoofing

Spoofing adalah seni untuk menjelma menjadi sesuatu yang lain. Spoofing attack terdiri dari IP address dan node source atau tujuan yang asli atau yang valid diganti dengan IP address atau node source atau tujuan yang lain.

4. Serangan Man-in-the-middle

Serangan keamanan jaringan Man-in-the-middle (serangan pembajakan) terjadi saat user perusak dapat memposisikan diantara dua titik link komunikasi.

a. Dengan jalan mengkopy atau menyusup traffic antara dua party, hal ini pada dasarnya merupakan serangan penyusup.

b. Para penyerang memposisikan dirinya dalam garis komunikasi dimana dia bertindak sebagai proxy atau mekanisme store-and-forwad (simpan dan lepaskan).

5. Spamming

Spam yang umum dijabarkan sebagai email yang tak diundang ini, newsgroup, atau pesan diskusi forum. Spam bisa merupakan iklan dari vendor

atau bisa berisi kuda Trojan. Spam pada umumnya bukan merupakan serangan keamanan jaringan akan tetapi hampir mirip DoS.

6. Sniffer

Suatu serangan keamanan jaringan dalam bentuk Sniffer (atau dikenal sebagai snooping attack) merupakan kegiatan user perusak yang ingin mendapatkan informasi tentang jaringan atau traffic lewat jaringan tersebut. suatu Sniffer sering merupakan program penangkap paket yang bisa menduplikasikan isi paket yang lewat media jaringan kedalam file. Serangan Sniffer sering difokuskan pada koneksi awal antara client dan server untuk mendapatkan logon credensial, kunci rahasia, password dan lainnya.

7. Crackers

Ancaman keamanan jaringan Crackers adalah user perusak yang bermaksud menyerang suatu system atau seseorang. Cracker bisasanya termotivasi oleh ego, power, atau ingin mendapatkan pengakuan. Akibat dari kegiatan hacker bisa berupa pencurian (data, ide, dll), disable system, kompromi keamanan, opini negative public, kehilangan pasar saham, mengurangi keuntungan, dan kehilangan produktifitas.[2]

2.9 Internet

Internet adalah himpunan informasi dan sumber daya komputer yang paling besar di dunia. Internet merupakan koneksi berbagai macam jaringan komputer dengan berbagai jenis hardware dan teknologi yang berbeda. Komunikasi yang dibangun pada jaringan internet menggunakan mekanisme tertentu yang disebut dengan protocol. Protocol yang digunakan untuk menjalankan komunikasi antar jaringan komputer pada internet ini adalah Transmission Control Protocol/ Internet Protocol (TCP/IP).[1]

Proses yang terjadi pada internet mempunyai mekanisme yang telah diatur berdasarkan protokol standar. Proses yang terjadi di internet adalah ada satu program yang meminta kepada program yang lain untuk memberikan suatu

layanan. Dua program tersebut dapat terletak dalam subnet yang sama ataupun berbeda. Komputer dengan program yang meminta layanan disebut dengan client sedangkan yang memberikan layanan disebut server.

2.10 Firewall

Firewall adalah suatu sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Umumnya, sebuah tembok-api diterapkan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dengan jaringan Internet.[1]

Firewall digunakan untuk membatasi atau mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah firewall menjadi istilah lazim yang merujuk pada sistem yang mengatur komunikasi antar dua macam jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke Internet dan juga tentu saja jaringan berbadan hukum di dalamnya, maka perlindungan terhadap perangkat digital perusahaan tersebut dari serangan para peretas, pemata-mata, ataupun pencuri data lainnya, menjadi kenyataan.

Secara mendasar, firewall dapat melakukan hal-hal berikut:

a. Mengatur dan mengontrol lalu lintas jaringan
b. Melakukan autentikasi terhadap akses
c. Melindungi sumber daya dalam jaringan privat
d. Mencatat semua kejadian, dan melaporkan kepada administrator

2.12 Protokol

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras,

perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras.[1]

Protokol perlu diutamakan pada penggunaan standar teknis, untuk menspesifikasi bagaimana membangun komputer atau menghubungkan peralatan perangkat keras. Protokol secara umum digunakan pada komunikasi real-time dimana standar digunakan untuk mengatur struktur dari informasi untuk penyimpanan jangka panjang. Sangat susah untuk menggeneralisir protokol dikarenakan protokol memiliki banyak variasi di dalam tujuan penggunaanya. Kebanyakan protokol memiliki salah satu atau beberapa dari hal berikut:

a. Melakukan deteksi adanya koneksi fisik atau ada tidaknya komputer atau mesin lainnya.

b. Melakukan metode (handshaking).

c. Negosiasi berbagai macam karakteristik hubungan.

d. Bagaimana mengawali dan mengakhiri suatu pesan.

e. Bagaimana format pesan yang digunakan.

f. Yang harus dilakukan saat terjadi kerusakan pesan atau pesan yang tidak sempurna.

g. Mendeteksi rugi-rugi pada hubungan jaringan dan langkah-langkah yang dilakukan selanjutnya

h. Mengakhiri suatu koneksi.

Untuk memudahkan memahami Protokol, kita mesti mengerti Model OSI. Dalam Model OSI terdapat 7 layer dimana masing-masing layer mempunyai jenis protokol sesuai dengan peruntukannya.

2.12 Model OSI

Untuk menyelenggarakan komunikasi berbagai macam vendor komputer diperlukan sebuah aturan baku yang standar dan disetejui berbagai pihak. Seperti halnya dua orang yang berlainan bangsa, maka untuk berkomunikasi memerlukan penerjemah/interpreter atau satu bahasa yang dimengerti kedua belah pihak. Dalam dunia komputer dan telekomunikasi interpreter identik dengan protokol.

Untuk itu maka badan dunia yang menangani masalah standarisasi ISO (International Standardization Organization) membuat aturan baku yang dikenal dengan nama model referensi OSI (Open System Interconnection). Dengan demikian diharapkan semua vendor perangkat telekomunikasi haruslah berpedoman dengan model referensi ini dalam mengembangkan protokolnya.[7]



Gambar 2.10 Model Referensi OSI

Setiap protokol berkomunikasi dengan peer (pasangan) protokol yang sama dalam layer yang sama dalam remote-system misalnya FTP lokal merupakan peer dari FTP remote. Jadi secara abstrak setiap protokol hanya peduli terhadap komunikasi dengan peer-nya, tak perduli dengan layer di bawah dan di atasnya.[1]

Adapun urutan layer dari layer 1 sampai layer 7 sebagai berikut :

1. Lapisan Physical

a. Lapisan ini bertugas mendefinisikan besaran-besaran elektrik yang dipakai untuk berhubungan, misalnya atas tegangan yang benar (Valid) logika 0 dan 1, bentuk konektor yang digunakan, cara penyandian isyarat pada kabel dan lain-lain.

b. Melaksanakan hubungan fisik melalui jalur transmisi.

c. Lapisan Data Link

d. Lapisan ini bertanggung jawab terhadap pengiriman data yang benar (error free) .

e. Mengirim data secara paket dan memeriksa kesalahan pada pengiriman data.

f. Menetapkan prosedur pengaksesan.

2. Lapisan Transport

a. Lapisan ini mengatur bagaimana data atau informasi itu akan dibawa ke tempat tujuan termasuk juga jaminan kualitas dari pelayanan pengiriman data.

b. Lapisan ini pula memilih fasilitas pengiriman yang sebagaimana yang dikehendaki.

3. Lapisan Session

a. Lapisan ini berfungsi menentukan kapan dimulai dan kapan diakhirinya suatu babak atau session komunikasi atau koneksi.

b. Suatu session akan dimulai jika session sebelumnya telah selesai.

c. Melihat data yang sudah dikirim dan diterima oleh proses.

4. Lapisan Presentation

a. Lapisan ini mendefinisikan bagaimana aplikasi dapat memasuki jaringan dan mengatur supaya data yang dipertukarkan atau dikirim ke lapisan aplikasi atau pemakai akhir dapat dimengerti bentuknya.

b. Dalam lapisan ini, peralatan atau sistem yang menggunakan format data yang berlainan dapat saling berkomunikasi .

c. Lapisan ini juga menyediakan enkripsi ataupun kompresi data jika diperlukan.

5. Lapisan Application

a. Lapisan ini berfungsi mengelola interaksi antara program dan pemakai.

b. Lapisan ini juga menerima perintah atau input dari pemakai dan mengembalikan kode error atau pesan kesalahan kepada pemakai jika terjadi error.

Model referensi OSI terdiri dari tujuh lapisan, mulai dari lapisan fisik sampai dengan aplikasi. Model referensi ini tidak hanya berguna untuk produk-produk LAN saja, tetapi dalam membangung jaringan Internet sekalipun sangat diperlukan. Hubungan antara model referensi OSI dengan protokol Internet bisa dilihat dalam Tabel.

Tabel 2.1 Hubungan referensi model OSI dengan Protokol Internet

MODEL OSI		TCP/IP	PROTOKOL TCP/IP	
NO	LAPISAN		PROTOKOL	FUNGSI
7				Distribusi IP pada jaringan dengan jumlah

	Aplication	Aplication	DHCP	IP yang terbatas
			DNS	Database nama domain mesin dan nomer IP
			FTP	Transfer file
			HTTP	Transfer file HTML dan Web
			MIME	Mengirim file binary dalam bentuk tesk
			NNTP	Menerima dan mengirim newsgroup)
			POP	Mengambil mail dari server
			SMB	Transfer berbagai server file DOS dan Windows
6	Presentation		SMTP	Pertukaran mail
			SNMP	Manajemen jaringan

			Telnet	Akses jarak jauh
			TFTP	Transfer file
5	Session		NETBIOS	BIOS jaringan standar
			RPC	Pemanggilan jarak jauh
			SOCKET	Input output nuntuk network jenis BSD-UNIX
4	Transport	Transport	TCP	Pertukaran data berorientasi
			UDP	Pertukaran data non-orientasi (connectonless(
3	Network	Internet	IP	Menetapkan routing
			RIP	Memilih routing
			ARP	Mendapatkan informasi hardware dari nomer IP
				Mendapatkan

			RARP	nomer IP dari hardware
2	Datalink	Network	PPP	Point ke point
			SLIP	Menggunakan sambungan serial
1	Physics	Ethernet, FDDI, ISDN, ATM		

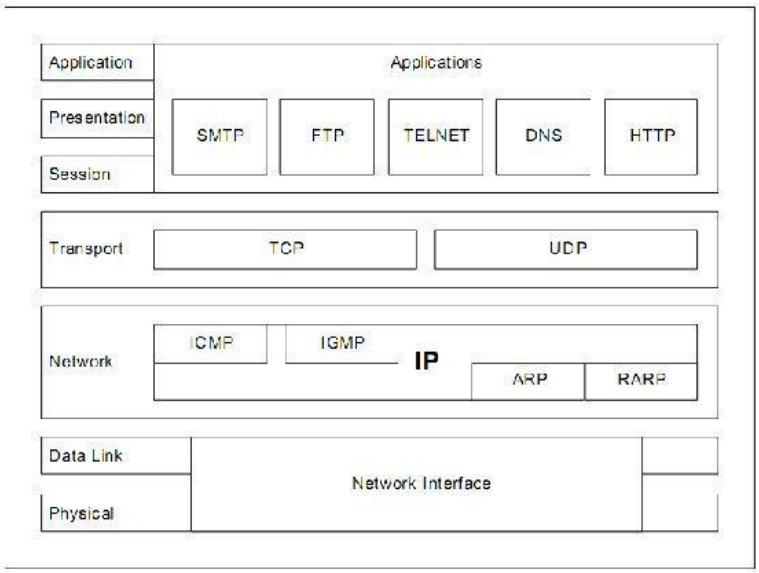
2.13 TCP/IP

TCP/IP dikembangkan mengacu pada model Open System Interconnection (OSI), dimana, layer-layer yang terdapat pada TCP tidak persis sama dengan layer-layer yang terdapat pada model OSI. Dengan menggunakan protokol yang sama yaitu TCP/IP, perbedaan jenis komputer dan sistem operasi tidak menjadi masalah. TCP/IP pada awal perkembangannya digunakan oleh Defense Advanced Research Project Agency (DARPA) untuk membangun jaringan untuk keperluan militer. Nama TCP/IP sendiri diambil dari nama protokol pada layer network yaitu Internet Protocol (IP) dan protokol pada layer transfort yaitu Transmission Control Protocol (TCP). Dengan mengacu pada nama ini, TCP/IP internet kemudian sering disebut sebagai Internet.[1]

TCP/IP(Transmission Control Protocol/Internet Protocol) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar menukar data dari satu komputer ke komputer lain di dalam jaringan internet. TCP/IP merupakan salah satu perangkat lunak jaringan komputer (networking software) yang terdapat dalam sistem, dan dipergunakan dalam komunikasi data dalam local area network (LAN) maupun Internet. TCP/IP dinamakan dari dua protokol yang paling penting di dalamnya yaitu TCP singkatan dari transfer control protocol dan IP singkatan dari Internet Protocol. TCP/IP menjadi satu

nama karena fungsinya selalu bergandengan satu sama lain dalam komunikasi data. TCP/IP saat ini dipergunakan dalam banyak jaringan komputer lokal (LAN) yang terhubung ke Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protocol (protocol suite). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (IP Address) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet.

Arsitektur protokol TCP/IP ini dapat dimodelkan dengan empat layer sebagaimana yang dapat dilihat pada gambar berikut.



Gambar 2.11 Susunan protokol TCP/IP dan model OSI

TCP/IP terdiri dari empat lapis kumpulan protokol yang bertingkat. Empat tingkat itu adalah :

a. Network Interface Layer

Bertanggung jawab mengirim dan menerima data ke dan dari media fisik (berupa kabel, serat optik atau gelombang radio), maka dari itu harus

mampu menerjemahkan sinyal listrik menjadi digital yang dimengerti komputer.

b. Internet Layer

Bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Pada layer ini terdapat tiga macam protokol yaitu:

a) IP (Internet Protocol) berfungsi untuk menyampaikan paket data ke alamat yang tepat, IP memiliki sifat sebagai unrealieble (ketidakandalan: tidak menjamin datagram yang terkirim sampai tujuan), connectionless, datagram delivery service.

b) ARP (Address Resolution Protocol) Protokol yang digunakan untuk nenemukan alamat Hardware dari host/komputer yang terletak pada network yang sama.

c) ICMP (Internet Control message protokol) Protokol yang digunakan untuk mengirimkan pesan dan melapor kegagalan pengiriman data.

c. Internet Layer

Bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Pada layer ini terdapat tiga macam protokol yaitu:

a) IP (Internet Protocol) berfungsi untuk menyampaikan paket data ke alamat yang tepat, IP memiliki sifat sebagai unrealieble (ketidakandalan: tidak menjamin datagram yang terkirim sampai tujuan), connectionless, datagram delivery service.

b) ARP (Address Resolution Protocol) Protokol yang digunakan untuk nenemukan alamat Hardware dari host/komputer yang terletak pada network yang sama.

c) ICMP (Internet Control message protokol) Protokol yang digunakan untuk mengirimkan pesan dan melapor kegagalan pengiriman data.

d. Aplication Layer

Terletak semua aplikasi yang menggunakan protokol TCP/IP.Fungsi masing-masing layer / lapisan protokol serta aliran data pada layer TCP / IP diatas, dapat dicontohkan dengan mengggunakan analogi yang sangat sederhana.

3.13.1 Kelas IP

Alamat IP versi 4 dibagi ke dalam beberapa kelas, dilihat dari oktet pertamanya, seperti terlihat pada tabel. Sebenarnya yang menjadi pembeda kelas IP versi 4 adalah pola biner yang terdapat dalam oktet pertama (utamanya adalah bit-bit awal/*high-order bit*), tapi untuk lebih mudah mengingatnya, akan lebih cepat diingat dengan menggunakan representasi desimal.[1]

Tabel 2.2 Kelas IP

Kelas Alamat IP	**Oktet pertama (desimal)**	**Oktet pertama (biner)**	**Digunakan oleh**
Kelas A	1–126	0xxx xxxx	Alamat *unicast* untuk jaringan skala besar
Kelas B	128–191	10xx xxxx	Alamat *unicast* untuk jaringan skala menengah hingga skala besar
Kelas C	192–223	110x	Alamat *unicast* untuk jaringan skala kecil

		xxxx	
Kelas D	224–239	1110 xxxx	Alamat *multicast* (bukan alamat *unicast*)
Kelas E	240–255	1111 xxxx	Direservasikan;umumnya digunakan sebagai alamat percobaan (eksperimen); (bukan alamat unicast)

a) Kelas A

Alamat-alamat kelas A diberikan untuk jaringan skala besar. Nomor urut bit tertinggi di dalam alamat IP kelas A selalu diset dengan nilai **0** (nol). Tujuh bit berikutnya—untuk melengkapi oktet pertama—akan membuat sebuah *network identifier*. 24 bit sisanya (atau tiga oktet terakhir) merepresentasikan *host identifier*. Ini mengizinkan kelas A memiliki hingga 126 jaringan, dan 16,777,214 host tiap jaringannya. Alamat dengan oktet awal 127 tidak diizinkan, karena digunakan untuk mekanisme Interprocess Communication (IPC) di dalam mesin yang bersangkutan.

b) Kelas B

Alamat-alamat kelas B dikhususkan untuk jaringan skala menengah hingga skala besar. Dua bit pertama di dalam oktet pertama alamat IP kelas B selalu diset ke bilangan biner **10**. 14 bit berikutnya (untuk melengkapi dua oktet pertama), akan membuat sebuah *network identifier*. 16 bit sisanya (dua oktet terakhir) merepresentasikan *host identifier*. Kelas B dapat memiliki 16,384 network, dan 65,534 host untuk setiap network-nya.

c) Kelas C

Alamat IP kelas C digunakan untuk jaringan berskala kecil. Tiga bit pertama di dalam oktet pertama alamat kelas C selalu diset ke nilai biner **110**. 21 bit selanjutnya (untuk melengkapi tiga oktet pertama) akan membentuk sebuah *network identifier*. 8 bit sisanya (sebagai oktet terakhir) akan merepresentasikan *host identifier*. Ini memungkinkan pembuatan total 2,097,152 buah network, dan 254 host untuk setiap network-nya.

d) Kelas D

Alamat IP kelas D disediakan hanya untuk alamat-alamat *IP multicast*, namun berbeda dengan tiga kelas di atas. Empat *bit* pertama di dalam IP kelas D selalu diset ke bilangan biner **1110**. 28*bit* sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali host. Untuk lebih jelas mengenal alamat ini, lihat pada bagian Alamat *Multicast* IPv4.

e) Kelas E

Alamat IP kelas E disediakan sebagai alamat yang bersifat "eksperimental" atau percobaan dan dicadangkan untuk digunakan pada masa depan. Empat bit pertama selalu diset kepada bilanganbiner **1111**. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali host.

2.13.2 Jenis IP Address

Berdasarkan fungsinya IP address dibagi menjadi 2 jenis yaitu :

1. IP Public

IP Public adalah IP address yang telah ditetapkan oleh InterNIC dan berisi beberapa buah network ID yang dijamin unik yang digunakan untuk lingkup internet, host yang menggunakan IP public dapat diakses oleh seluruh user yang tergabung diinternet baik secara langsung maupun tidak langsung (melalui proxy/NAT). IP Addressing juga dikelompokkan berdasarkan negara,

Indonesia umumnya dimulai dengan kepala 202 & 203. Contoh : P Public adalah akses Speedy modem yang merupakan IP Public 125.126.0.1

2. IP Private

IP Private adalah IP address yang digunkan untuk lingkup intranet, host yang menggunakan IP Private hanya bisa diakses di linkup intranet saja. Contoh : IP private akses di LAN modem menggunakan IP Private 192.168.1.1.

2.14 UDP

UDP yang merupakan salah satu protocol utama diatas IP merupakan transport protocol yang lebih sederhana dibandingkan dengan TCP. UDP digunakan untuk situasi yang tidak mementingkan mekanisme reliabilitas. Header UDP hanya berisi empat field yaitu source port, destination port, length dan UDP checksum dimana fungsinya hampir sama dengan TCP, namun fasilitas checksum pada UDP bersifat opsional.[1]

2.14.1 Karakteristik UDP

Berikut ini beberapa karakterisik dari UDP :

a. Connectionless (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak bertukar informasi.

b. Unreliable (tidak nyata): Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan. Protokol lapisan aplikasi yang berjalan di atas UDP harus melakukan pemulihan terhadap pesan-pesan yang hilang selama transmisi. Umumnya, protokol lapisan aplikasi yang berjalan di atas UDP mengimplementasikan layanan keandalan mereka masing-masing, atau mengirim pesan secara periodik atau dengan menggunakan waktu yang telah didefinisikan.

c. UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi atau proses tertentu di dalam sebuah host dalam jaringan yang menggunakan TCP/IP. Header UDP berisi field Source Process Identification dan Destination Process Identification.

d. UDP menyediakan penghitungan checksum berukuran 16-bit.

Secara teknis protokol UDP juga memiliki header yang lebih kecil 8 bytes dibandingkan dengan protokol TCP 20 bytes. Berdasarkan karakterisitik masing-masing protokol inilah yang mengakibatkan protokol UDP akan menggunakan hampir seluruh alokasi bandwidth yang tersedia, sedangkan protokol TCP hampir tidak mendapatkan bandwidth sama sekali, yang bahkan mengakibatkan koneksi TCP terputus.

TCP dan UDP adalah dua protokol koneksi yang paling umum digunakan digunakan untuk data traversal di Internet . Transmission Control Protocol atau TCP berorientasi koneksi , yang berarti bahwa hubungan formal antara dua titik akhir harus ditetapkan sebelum data ditransmisikan . TCP menjamin pengiriman data, dan juga menjamin bahwa paket data akan dikirimkan dalam urutan yang sama di mana mereka dikirim . Proses ini berlangsung seperti ini :

a. Endpoint A mengirimkan paket 1 untuk Endpoint B
b. Endpoint B menerima paket 1 tanpa kesalahan dan mengirimkan paket acknowledgment kembali ke Endpoint A
c. Endpoint A menerima paket pengakuan dan hasil untuk mengirim paket 2 Endpoint B

Jika tidak ada paket pengakuan yang diterima setelah waktu tertentu , paket asli akan dipancarkan kembali . Hal ini menjamin bahwa semua data yang dikirim akan tampil tanpa kesalahan dan dalam urutan yang benar . TCP mengutamakan akurasi atas kecepatan dan efisiensi . Website seperti yang Anda lihat sekarang , pengiriman email , dll menggunakan TCP .

User Datagram Protocol atau UDP sangat berbeda . Tidak seperti TCP , UDP adalah connectionless , yang berarti bahwa paket data dapat dikirim tanpa peringatan , persiapan , atau negosiasi . Tidak ada jabat tangan atau setup, hanya paket-paket data. UDP juga tidak memiliki jenis kontrol kesalahan . Tidak hanya dapat paket disampaikan dalam urutan yang salah , tetapi mereka juga bisa benar-benar ditinggalkan . UDP dimaksudkan untuk aplikasi di mana Anda lebih peduli dengan menjaga aliran informasi akan daripada memastikan Anda menerima setiap paket tunggal . Hal ini membuat UDP ideal untuk layanan real-time seperti Voice over IP . Mengapa UDP ideal untuk layanan real-time dan tidak TCP ? Percaya atau tidak itu sebenarnya sifat ' terpercaya ' dari protokol yang menyakitkan pengalaman pengguna akhir . Dengan TCP , penundaan terjadi setiap kali ada kesalahan seperti packet loss . Penundaan ini, yang disebabkan oleh mentransmisi paket rusak dan setiap paket berikut yang mungkin telah dikirim , diterjemahkan ke dalam tingkat yang tidak dapat diterima jitter bagi pengguna akhir. Real layanan komunikasi time seperti VoIP tidak memerlukan lapisan transport protokol -benar dapat diandalkan . Hal ini memungkinkan UDP untuk bersinar . Kesalahan seperti packet loss biasanya hanya memiliki dampak kecil pada output audio . Adalah jauh lebih baik untuk drop paket dan memiliki beberapa milidetik keheningan daripada memiliki detik lag.

Di bawah ini merupakan tabel perbedaan TCP dan UDP :

Tabel 2.3 Perbedaan TCP dan UDP

No	TCP	UDP
1.	Beroperasi berdasarkan konsep koneksi.	Tidak berdasarkan konsep koneksi, jadi harus membuat kode sendiri.
2.	Jaminan pengiriman-penerimaan	Tidak ada jaminan bahwa pengiriman dan

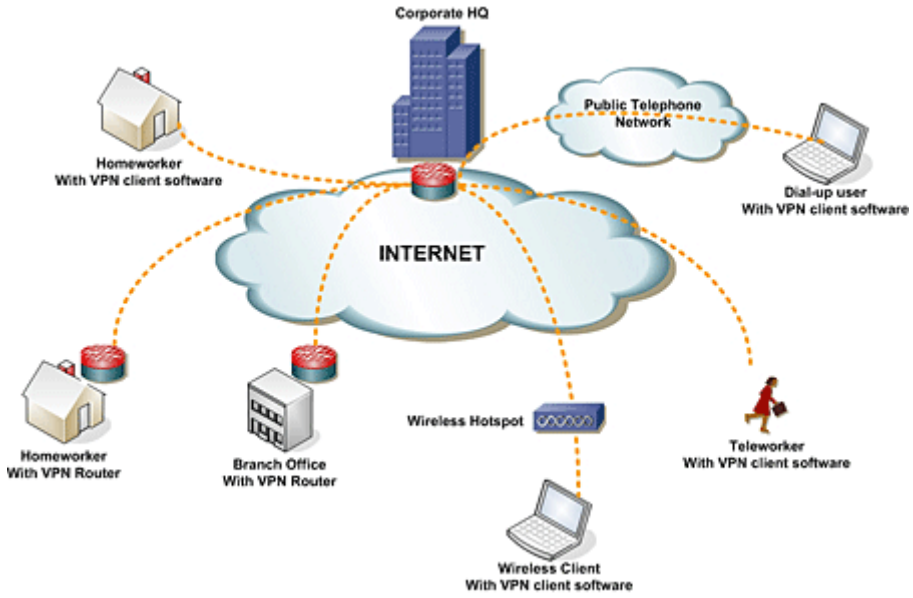
	data akan reliable dan teratur.	penerimaan data akan reliable dan teratur, sehingga paket data mungkin dapat kurang, terduplikat, atau bahkan tidak sampai sama sekali.
3.	Secara otomatis memecah data ke dalam paket-paket.	Pemecahan ke dalam paket-paket dan proses pengirimannya dilakukan secara manual.
4.	Tidak akan mengirimkan data terlalu cepat sehingga memberikan jaminan koneksi internet dapat menanganinya.	Harus membuat kepastian mengenai proses transfer data agar tidak terlalu cepat sehingga internet masih dapat menanganinya.
5.	Mudah untuk digunakan, transfer paket data seperti menulis dan membaca file.	Jika paket ada yang hilang, perlu dipikirkan di mana letak kesalahan yang terjadi dan mengirim ulang data yang diperlukan.
6	Tidak cocok digunakan untuk komunikasi berbasis real time seperti media streaming	cCcok digunakan untuk komunikasi berbasis real time seperti media streaming

2.15 Virtual Private Network

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan pengguna untuk dapat terkoneksi ke jaringan publik 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, walaupaun sebenarnya menggunakan jaringan milik publik.[3]

VPN dapat dibentuk dengan menggunakan teknologi tunneling dan enkripsi. Konkesi VPN juga dapat terjadi pada semual layer pada protocol OSI, sehingga komunikasi menggunakan VPN dapat digunakan untuk berbagai keperluan. VPN dapat terjadi antara dua end-system atau dua komputer atau antara dua atau lebih jaringan yang berbeda. VPN dapat dibentuk dengan menggunakan teknologi tunneling dan enkripsi. Koneksi VPN juga dapat terjadi pada semua layer pada protocol OSI, sehingga komunikasi menggunakan VPN dapat digunakan untuk berbagai keperluan. Dengan demikian, VPN juga dapat dikategorikan sebagai infrastruktur WAN alternatif untuk mendapatkan koneksi point-to-point pribadi antara pengirim dan penerima. Dan dapat dilakukan dengan menggunakan media apa saja, tanpa perlu media leased line atau frame relay.



Gambar 2.12 VPN

Dari gambar tersebut dapat kita lihat bahwa VPN dapat terjadi pada dua end-system. Syarat yang harus terpenuhi adalah kedua system tersebut saling terhubung dengan jaringan public (Internet). Di dalam jaringan public ini kedua system membuat semacam jalur khusus yang biasa disebut tunnel untuk saling

terkoneksi. Jadi tunnel inilah yang membuat seolah-olah kedua system tersebut berada dalam local area yang sama. Analogi dari gambar di atas misalkan bagan system yang kiri adalah suatu jaringan local (LAN) suatu instansi pusat kemudian system yang kanan adalah suatu LAN anak cabang. Kedua LAN ini membangun suatu tunnel pada jaringan public untuk saling terhubung hingga membentuk suatu VPN. Dengan demikian instansi ini tidak perlu lagi membangun suatu jaringan pribadi secara leased line yang memakan banyak biaya.[2]

2.15.1 Fungsi VPN

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

1. Confidentially (Kerahasiaan)

   Dengan digunakannnya 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.

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. [4]

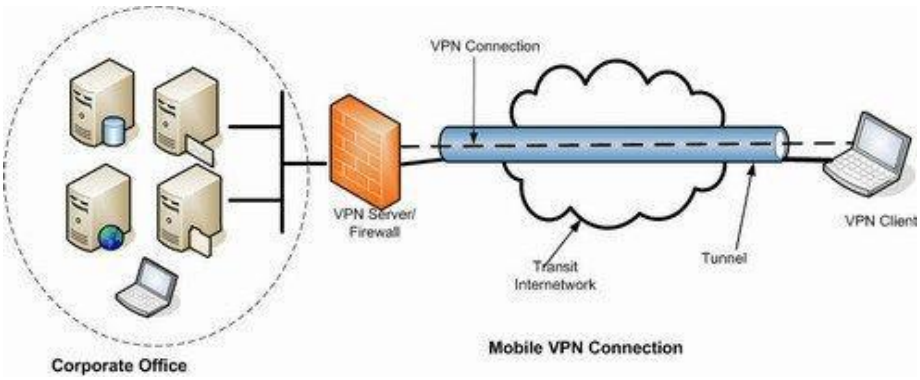
2.15.2 Jenis Implementasi VPN

Di dalam implementasinya VPN dibagi menjadi dua jenis yaitu remote access VPN dan site-to-site VPN :

2.15.2.1 Remote Access

Jenis implementasi yang pertama adalah Remote access yang biasa juga disebut virtual private dial-up network (VPDN), menghubungkan antara pengguna yang mobile dengan local area network (LAN). Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (remote) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan enterprise service provider (ESP). ESP akan memberikan suatu network access server (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan software klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut.[4]

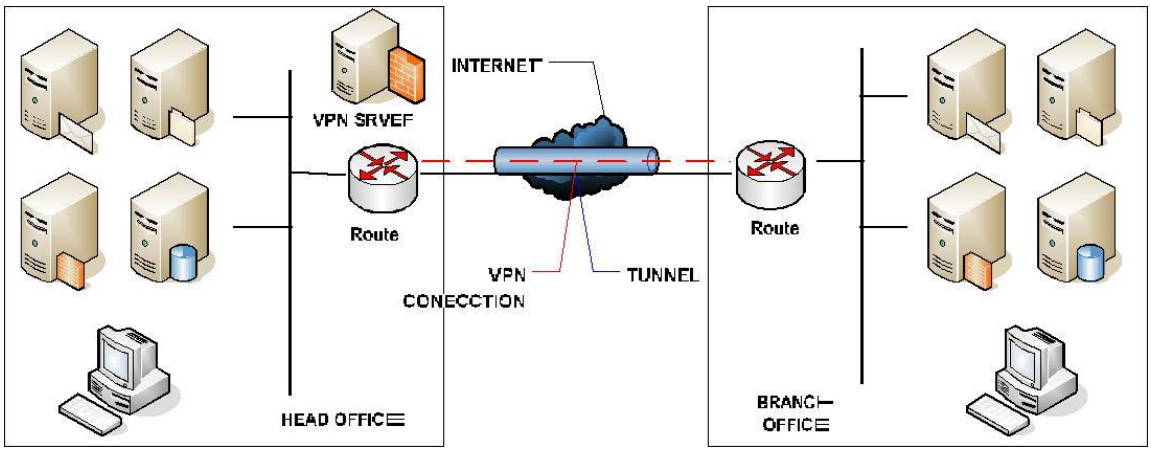
Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-dial nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan sotware klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan. Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan remote access VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.[2]



Gambar 2.13 Remote Access VPN

2.18.2.2 Site-to-Site

Jenis implementasi VPN yang kedua adalah site-to-site VPN. Implementasi jenis ini menghubungkan antara dua tempat yang letaknya berjauhan, seperti halnya kantor pusat dengan kantor cabang atau suatu perusahaan dengan perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, supplier atau pelanggan) disebut ekstranet. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet site-to-site VPN.



Gambar 2.14 Site-to-site VPN

2.16.3 Teknologi VPN

VPN merupakan perpaduan dari teknologi tunneling dengan teknologi enkripsi. Berikut ini akan dijelaskan mengenai teknologi tunneling dan enkripsi tersebut.

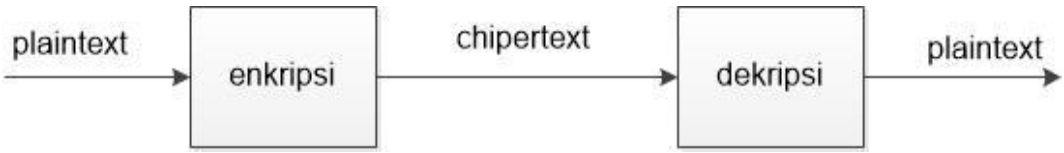
2.16.3.1 Tunneling

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 jaringan umum, namun koneksi tersebut 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 akan terbentuk dan VPN pun tidak dapat dibangun. Apabila tunnel tersebut telah terbentuk, maka koneksi point-to-point 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.[6]

2.8.3.2 Enkripsi

Pesan yang belum disandikan disebut dengan plaintext proses yang digunkaan untuk mengubah plaintext menjadi chipertext disebut enkripsi (encryption) atau enchiperment. Sedangkan proses untuk mengubah chipertext kembali menjadi plaintext disebut dengan dekripsi (decryption). Gambar 2.2 berikut akan menjelaskan istilah-istilah yang dijelaskan diatas.[4]



Gambar 2.15 Enkripsi dan Dekripsi

Kunci-kunci yang digunakan untuk proses enkripsi dan dekripsi tidak harus selalu identik, tergantung pada sistem yang digunakan. Secara umum operasi enkripsi dan dekripsi dapat diterangkan secara matematis sebagai berikut:

$\mathrm{EK}(\mathrm{M}) = \mathrm{C}$ (Proses Enkripsi)

$\mathrm{DK}(\mathrm{C}) = \mathrm{M}$ (Proses Dekripsi)

Pada saat proses enkripsi kita menyandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya. Dengan demikian keamanan suatu pesan bergantung pada kunci ataupun kunci-kunci yang digunakan, bukan pada algoritma yang digunakan. Sehingga algoritma-algortima yang digunakan tersebut dapat dipublikasikan untuk dianalaisis dan produk-produk yang menggunakan algoritma tersebut dapat diproduksi masal.

Berikut ini adalah jenis enkripsi yang biasa digunakan pada VPN :

a. MPPE Windows
b. IPSec encryption: DES atau 3DES
c. VPNd: Blowfish

2.16.4 Jenis Protokol VPN

Jenis protokol yang biasa digunakn dalam VPN sebagai berikut :

1. Point to Point Tunneling Protocol (PPTP)

PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari remote access Point-to-Point protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui intenet. PPTP juga dapat digunakan pada jaringan private LAN-to-LAN. Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya public-switched telephone network (PSTNs) untuk membangun VPN. Pembangunan PPTPyang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk remote users dan mobile users karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.[5]

2. SSTP

Protokol SSTP adalah bentuk tunneling VPN yang menyediakan mekanisme untuk transportasi atau trafik L2TP PPP melalui channel SSL 3.0. SSL menyediakan transport-level security dengan keynegotiation, enkripsi dan memeriksa lalu lintas integritas. Penggunaan SSL melalui TCP port 443 memungkinkan SSTP untuk melewati hampir semua firewall dan server proxy. Hal ini membuat protokol SSTP memberikan akses VPN dengan level penuh pada jaringan.

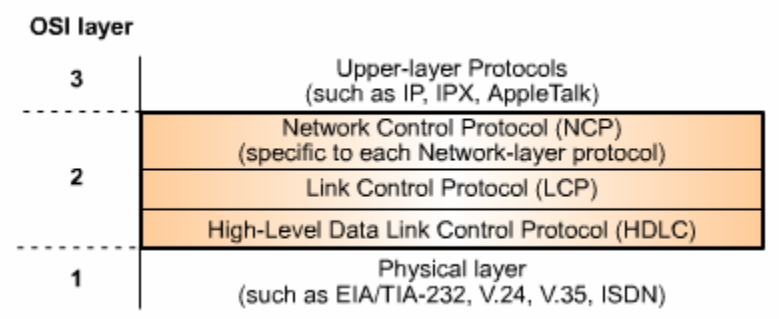
3. Layer 2 Tuneling Protocol (L2TP)

L2TP merupakan pengembangan dari PPTP ditambah L2F. Network security Protocol dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan protocol UDP port 1701. L2TP tidak bisa berdiri sendiri, biasanya untuk keamanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec. Contohnya untuk Operating system Windows, secara default OS Windows menggunakan L2TP/IPSec. Akan tetapi, konsekuensinya tentu saja konfigurasi yang harus dilakukan tidak semudah PPTP. Sisi client pun harus sudah support IPSec ketika menerapkan L2TP/IPSec. Dari segi enkripsi, tentu enkripsi pada L2TP/IPSec memiliki tingkat sekuritas lebih tinggi daripada PPTP yang menggunakan MPPE. [2]

2.17 Protokol L2TP

Perlu diingat, bahwa semakin kita membutuhkan sebuah jaringan yang aman, maka akan semakin kompleks konfigurasi yang perlu diterapkan, begitu juga dengan penggunaan resource hardware, semakin tinggi enkripsi yang digunakan, penggunaan resource, khususnya CPU juga akan naik. Kesimpulan yang bisa kita ambil, jika Anda menginginkan VPN dengan kompatibilitas perangkat client yang baik , maka PPTP bisa menjadi pilihan. Selain itu, PPTP juga bisa menjadi pilihan jika Anda tidak ingin terlalu sulit untuk melakukan konfigurasi. Tetapi jika Anda menginginkan sebuah VPN dengan keamanan lebih bagus, gunakan L2TP/IPsec. Biasanya untuk OS windows, secara default menggunakan L2TP/IPSec, sehingga tinggal diseusuaikan pada sisi server. Jika memang perangkat Anda support dan Anda membutuhkan keamanan yang tinggi pada jalur VPN anda, L2TP/IPSec bisa menjadi pilihan. Satu hal yang menjadi catatan, penggunaan VPN tidak bisa meningkatkan bandwidth (lebih tepatnya mengurangi bandwidth anda karena ada penambahan headernya), tergantung dari besar bandwidth langganan anda. Microsoft mendorong para vendor gateway untuk menerapkan L2TP/IPSec untuk remote akses VPN sehingga sistem operasi

Microsoft yang mendukung L2TP/IPSec dapat terhubung secara langsung ke gateway vendor dan solusi VPN lainnya tanpa harus mengubah kode client-sidenya. Untuk vendor gateway yang mendukung lainnya IPSec berbasis metode akses, Microsoft mendorong vendor untuk menyediakan dukungan untuk L2TP/IPSec sebagai pilihan untuk melengkapi mode multi-protokol dan pertimbangan multicast. User pengguna VPN bisa mengubah secara langsung settingan protokol yang digunakan pada konfigurasi VPNnya. Disitu pengguna bisa mengubah tipe VPN yang digunakan apakah Automatic, PPTP, dan L2TP. Protokol L2TP sering juga disebut sebagai protokol dial-up virtual, karena L2TP memperluas suatu session PPP (Point-to-Point Protocol) dial-up melalui jaringan publik internet, atau sering juga digambarkan seperti koneksi virtual PPP.[4]



Gambar 2.16 Susunan Protokol PPP

PPP terdiri dari 4 komponen utama yaitu :

1. EIA/TIA 232 : Layer fisik untuk komunikasi serial.
2. HDLC : Metode untuk enkapsulasi datagram melalui link serial.
3. LCP : Metode untuk pembentukan, konfigurasi, mempertahankan, dan memutuskan jaringan PPP.
4. NCP : Metode pembentukan dan mengkonfigurasi protokol Network Layer yang berbeda (Layer 3 : misalnya IP, IPX, atau apple talk).

2.17.1 L2TP OVER UDP/IP

L2TP menggunakan port UDP 1701 yang teregister. Inisiator tunnel L2TP akan mengambil satu port UDP source/asal (yang bukan 1701) dan mengirimkan ke tujuan yang dikehendaki dengan alamat port 1701. Demikian pula penerima akan mengambil sebuah port yang bebas (selain 1701) pada sistemnya, dan mengirim balik kepada inisiator dengan alamat port UDP (port 1701). Setiap kali port asal dan tujuan ,dan alamat terbentuk maka alamat port yang digunakan pun akan tetap/static. Jika port yang digunakan berubah-rubah, maka mekanisme L2TP melewati perangkat NAT akan lebih kompleks. Fragmentasi IP dapat terjadi pada L2TP seperti paket L2TP melewati melalui substrat IP. L2TP tidak mempunyai perlakuan khusus untuk mengoptimalkannya. Implementasi LAC dapat menyebabkan LCP bernegoisasi nilai MRU, yang mengoptimalkan lingkungan LAC sehingga paket L2TP dapat dilewatkan dengan nilai MTU yang konsisten. Secara default pada beberapa implementasi L2TP UDP checksum harus digunakan untuk kontol dan data message. UDP checksum pada data message boleh tidak digunakan, tetapi penggunaan checksum pada control message direkomendasikan.[4]

2.18 IP Security (IPSec)

IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, memperkirakan algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec dapat digunakan untuk memproteksi satu atau lebih path antara sepasang Host, antara sepasang security gateway, atau antara security gateway dengan Host (istilah security gateway mengacu pada sistem intermediate yang menggunakan protokol IPSec, misalkan router dan firewall yang mengimplementasikan IPSec). [3]

IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalulintas yaitu Authentication Header (AH) and Encapsulating Security Payload (ESP). Implementasi IPSec harus mendukung ESP dan juga AH.

a. AH (Authentication Header), autentifikasi sumber data dan proteksi terhadap pencurian data. Protocol AH dibuat dengan melakukan enkapsulasi paket IP asli kedalam paket baru yang mengandung IP header yang baru yaitu AH header disertai dengan header asli. Isi data yang dikirimkan melalui protocol AH bersifat clear text sehingga tunnel yang berdasar protocol AH ini tidak menyediakan kepastian data. Kehadiran header AH memungkinkan untuk memverifikasi integritas pesan,. Dengan demikian, AH menyediakan otentikasi tetapi tidak puntuk enkripsi. AH hanya menyediakan algoritma enkripsi sebagai berikut :
b. ESP (Encapsulated Security Payload) dapat menyediakan kepastian data, autentikasi sumber data dan proteksi terhadap gangguan pada data. Protocol ESP dibuat dengan melakukan enkripsi pada paket IP dan membuat paket IP lain yang mengandung header IP asli dan header ESP. Data yang terenkripsi (yang mengandung header IP asli) dan trailer ESP, separuhnya terenkripsi dan sebagian tidak. ESP menyediakan algoritma autentikasi dan juga enkripsi sebagai berikut :

1. Autentikasi

a. SHA1

   SHA1 dikembangkan oleh Institut Nasional Standar dan Teknologi seperti yang dijelaskan di Federal Information Processing Standard (FIPS) 180-1 PUB. Proses SHA erat model setelah MD5. Hasil perhitungan dalam The SHA1 hash 160-bit yang digunakan untuk memeriksa integritas. Karena panjang hash lagi memberikan keamanan yang lebih besar, SHA lebih kuat daripada MD5.
b. MD5

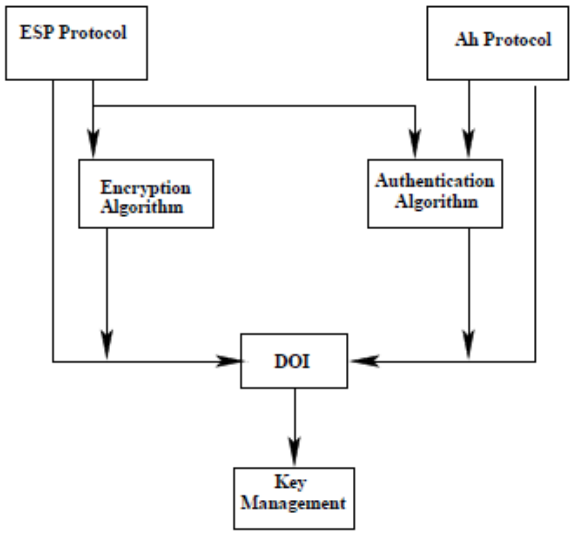
   Pesan Digest 5 (MD5) didasarkan pada RFC 1321. MD5 melengkapi empat lewat di atas blok data, dengan menggunakan sebuah konstanta

numerik yang berbeda untuk setiap kata dalam pesan pada setiap lulus. Jumlah konstanta 32-bit yang digunakan selama perhitungan MD5 akhirnya menghasilkan hash 128-bit yang digunakan untuk memeriksa integritas.

2. Enkripsi

a. DES - 56-bit DES-CBC encryption algorithm;
b. 3DES - 168-bit DES encryption algorithm;
c. AES - 128, 192 and 256-bit key AES-CBC encryption algorithm;
d. Blowfish - added since v4.5
e. Twofish - added since v4.5
f. Camellia - 128, 192 and 256-bit key Camellia encryption algorithm added since v4.5

Kedua protokol ini merupakan pembawa kontrol akses berbasis distribusi kunci kriptografi dan manajemen aliran lalulintas relatif terhadap protokol keamanan.



Gambar 2.18 Arsitektur IPSec

IPSec adalah sekumpulan ekstensi dari keluarga protokol IP. IPSec menyediakan layanan kriptografi untuk keamanan transmisi data. Layanan ini termasuk authenticity, integrity, access control, confidentiality, dab anti replay. Layanan IPSec mirip dengan SSL namun, IPSec melayani lapisan network, dan dilakukan secara transparan. Layanan tersebut dideskripsikan sebagai berikut:

a. Confidentiality, untuk meyakinkan bahwa sulit untuk orang lain tetapi dapat dimengerti oleh penerima yang sah bahwa data telah dikirimkan. Contoh: Kita tidak ingin tahu seseorang dapat melihat password ketika login ke remote server.

b. Integrity, untuk menjamin bahwa data tidak berubah dalam perjalan menuju tujuan.

c. Authenticity, untuk menandai bahwa data yang dikirimkan memang berasal dari pengirim yang benar.

d. Anti Replay, untuk meyakinkan bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan untuk mengulang.

2.18.1 Perlindungan IPSec Terhadap Serangan

IPSec melindungi data sehingga penyerang menemukan sangat sulit atau tidak mungkin untuk menafsirkannya . Tingkat perlindungan yang diberikan ditentukan oleh kekuatan tingkat keamanan yang ditetapkan dalam struktur kebijakan IPSec Anda . IPSec memiliki sejumlah fitur yang secara signifikan mengurangi atau mencegah serangan berikut :

1. Sniffers

   The Encapsulating Security Payload (ESP) protokol di IPSec menyediakan kerahasiaan data dengan enkripsi payload dari paket IP .

2. Data modification

   IPSec menggunakan kunci berbasis kriptografi , bersama hanya oleh komputer pengirim dan penerima , untuk membuat checksum kriptografi untuk setiap paket IP . Setiap modifikasi terhadap paket data mengubah checksum , yang menunjukkan ke komputer penerima bahwa paket itu diubah dalam perjalanan .

3. Spoofing

   IPSec memungkinkan pertukaran dan verifikasi identitas tanpa mengekspos informasi tersebut untuk interpretasi oleh seorang penyerang . Verifikasi Mutual (otentikasi) digunakan untuk membangun kepercayaan antara sistem komunikasi dan sistem hanya dipercaya dapat berkomunikasi satu sama lain . Setelah identitas ditetapkan, IPSec menggunakan kunci berbasis kriptografi , bersama hanya oleh komputer pengirim dan penerima , untuk membuat checksum kriptografi untuk setiap paket IP . Checksum kriptografi memastikan bahwa hanya komputer yang memiliki pengetahuan tentang kunci bisa dikirim setiap paket .

4. Man-in- the-middle attack

   IPSec menggabungkan otentikasi bersama dengan shared , kunci berbasis kriptografi .

5. Denial - of-service

   IPSec menggunakan metodologi packet filtering IP sebagai dasar untuk menentukan apakah komunikasi diperbolehkan , dijamin , atau diblokir , sesuai dengan rentang alamat IP , protokol IP , atau TCP bahkan spesifik dan port UDP. [4]

2.18.2 Security Association

Kombinasi tentang bagaimana melindungi data (ESP dan atau AH termasuk algoritma dan kunci), apa saja data yang dilindungi dan pada saat apa data dilindungi disebut dengan Security Association (SA).[5] SA merupakan identifikasi unik dengan berbasiskan Security Parameter Index (SPI), alamat tujuan IP dan protocol keamanan (AH dan atau ESP) yang diimplementasikan dalam trafik jaringan IPSec. Dua tipe SA yang didefinisikan yaitu

1. Transport Mode

   Protokol menyediakan proteksi terhadap layer di atas IP *layer*. Layanan keamanan pada mode ini dilakukan dengan penambahan sebuah IPsec *header* antara IP *header* dengan *header* protokol *layer* di atas IP yang diproteksi.
2. Tunnel mode

   Protokol diaplikasikan untuk menyediakan proteksi pada paket IP sehingga sekaligus melindungi *layer* di atas IP *layer*. Hal ini dilakukan dengan mengenkapsulasi paket IP yang akan diproteksi pada sebuah IP datagram yang lain.

Tabel 2.4 Transport dan Tunnel Model

	Transport Mode SA	Tunnel Mode SA
AH	Mengotentikasi IP Payload dan memilih bagian-bagian dari IP header dan ekstensi ip	Mengotentikasi bagian dalam paket IP dan bagian luar IP header dan ekstensi header
ESP	Mengenskripsi IP payload dan ekstensi header IP	Mengenkripsi bagian dalam paket IP
ESP dengan otentikasi	Mengenkripsi IP payload dan setiap	Mengenkripsi bagian dalam paket IP

	ektensi header IP setelah ESP header Menotentikasi IP payload tetapi tidak IP header	Mengotentikasi bagian dalam paket IP

2.19 Authentication, Authorization, Accounting (AAA)

Protokol AAA (Authentication, Authorization, Accounting) digunakan untuk mengatur mekanisme bagaimana tata cara berkomunikasi, baik antara client ke domain-domain jaringan maupun antar client dengan domain yang berbeda dengan tetap menjaga keamanan pertukaran data.[4]

Autentikasi (Authentication) yaitu proses pengesahan identitas pengguna (end user) untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik misalnya, username, password, pin, sidik jari) oleh pengguna kepada server. Di sisi server, sistem akan menerima kode unik tersebut, selanjutnya membandingkan dengan kode unik yang disimpan dalam database server. Jika hasilnya sama, maka server akan mengirimkan hak akses kepada pengguna. Namun jika hasilnya tidak sama, maka server akan mengirimkan pesan kegagalan dan menolak hak akses pengguna.[4]

Autorisasi (Authorization) merupakan proses pengecekan wewenang pengguna, mana saja hak-hak akses yang diperbolehkan dan mana saja yang tidak. Pencatatan (Accounting) merupakan proses pengumpulan data informasi seputar berapa lama user melakukan koneksi dan billing time yang telah dilalui selama pemakaian.

Mekanisme jaringan AAA adalah sebagai berikut :

a. User melakukan koneksi ke peralatan NAS point to point sebagai langkah awal koneksi ke jaringan.

b. Network Access Server (NAS) sebagai client AAA kemudian melakukan pengumpulan informasi pengguna dan melanjutkan data pengguna ke server.

c. Server AAA menerima dan memproses data pengguna, kemudian memberikan balasan ke NAS berupa pesan penerima atau penolakan pendaftaran dari pengguna.

d. NAS sebagai client AAA kemudian menyampaikan pesan server AAA tersebut kepada pengguna bahwa pendaftaran ditolak atau diterima beserta layanan yang diperkenankan untuk akses.

2.20 Remote Authentication Dial-In User Service (RADIUS)

Remote Access (pada sebagian literatur Authentication) Dial-In User Service, yang sering disingkat menjadi RADIUS, adalah sebuah protokol keamanan komputer yang digunakan untuk melakukan autentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. RADIUS didefinisikan ddalam RFC 2865 dan RFC 2866, yang pada awalnya digunakan untuk melakukan autentikasi terhadap akses jaringan jarak jauh (remote) dengan menggunakan koneksi dial-up. [4]

RADIUS kini telah diimplementasikan untuk melakukan autentikasi terhadap akses jaringan secara jarak jauh dengan menggunakan koneksi selain dial-up, seperti halnya Virtual Private Networking (VPN), access point nirkabel, switch Ethernet, dan perangkat lainnya. Radius server adalah server Remote Authentikasi Dial-in Service (RADIUS), sebuah protokol keamanan jaringan komputer berbasis server yang sering digunakan untuk melakukan authentikasi dan otorisasi serta pendaftaran akun (account) pengguna secara terpusat untuk mengakses jaringan yang aman.

RADIUS mula-mula dikembangkan oleh perusahan Livingston. Pada awal pengembangannya, RADIUS menggunakan port 1645, yang ternyata bentrok

dengan layanan “datametrics”. Sekarang, port yang dipakai RADIUS adalah port 1812. [5]

1. Proses Authentication

Proses autentikasi diperlukan ketika Anda mempunyai kebutuhan untuk membatasi siapa saja yang diperbolehkan masuk ke dalam jaringan remote access milik Anda. Untuk memenuhi kebutuhan tersebut, pengguna yang ingin mengakses sebuah jaringan secara remote harus diidentifikasi terlebih dahulu. Pengguna yang ingin masuk ke dalam jaringan pribadi tersebut perlu diketahui terlebih dahulu sebelum bebas mengakses jaringan tersebut. Pengenalan ini bertujuan untuk mengetahui apakah pengguna tersebut berhak atau tidak untuk mengakses jaringan.

Proses Autentikasi Terdiri dari 4 tahapan yaitu :

a. Autentikasi untuk mengetahui lokasi dari peralatan pada suatau simpul jaringan (terjadi pada datalink dan network layer)

b. Autentikasi untuk mengenali sitem operasi yang terhubung dengan jaringan (terjadi pada transport layer)

c. Autentikasi untuk mengetahui proses terjadinya kejadian di suatu simpul jaringan (terjadi pada session dan presentation layer)

d. Autentikasi untuk mengenali user dan aplikasi yang digunakan (terjadi pada application layer)

2. Proses Authorization

Proses authorization merupakan langkah selanjutnya setelah proses autentikasi berhasil. Ketika pengguna yang ingin mengakses jaringan Anda telah dikenali dan termasuk dalam daftar yang diperbolehkan membuka akses, langkah berikutnya Anda harus memberikan batasan hak-hak apa saja yang akan diterima oleh pengguna tersebut.

Analogi dari proses ini dapat dimisalkan seperti peraturan-peraturan yang tertempel di dinding-dinding rumah Anda. Isi dari peraturan tersebut biasanya akan membatasi para pengunjung agar mereka tidak dapat dengan bebas berkeliling rumah Anda. Tentu ada bagian yang privasi di rumah Anda, bukan? Misalnya setiap pengunjung rumah Anda tidak diperbolehkan masuk ke ruang kerja Anda. Atau setiap pengunjung harus membuka alas kakinya ketika memasuki ruangan ibadah di rumah Anda. Atau setiap pengunjung hanya diperbolehkan masuk sampai teras rumah.

3. Proses Accounting

Proses accounting dalam layanan koneksi remote access amat sangat penting, apalagi jika Anda membuat jaringan ini untuk kepentingan komersial. Dalam proses accounting ini, perangkat remote access atau server sekuriti akan mengumpulkan informasi seputar berapa lama si pengguna sudah terkoneksi, billing time (waktu start dan waktu stop) yang telah dilaluinya selama pemakaian, sampai berapa besar data yang sudah dilewatkan dalam transaksi komunikasi tersebut. Data dan informasi ini akan berguna sekali untuk pengguna maupun administratornya. Biasanya informasi ini akan digunakan dalam melakukan proses auditing, membuat laporan pemakaian, penganalisisan karakteristik jaringan, pembuatan billing tagihan, dan banyak lagi.

2.21 Mikrotik RouterOS

MikroTik RouterOS™, merupakan sistem operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui Windows Application (WinBox). Selain itu instalasi dapat dilakukan pada Standard komputer PC (Personal Computer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai.[5]

2.22 Tools yang Digunakan

1. Wireshark

   Wireshark merupakan salah satu tools atau aplikasi "Network Analyzer" atau Penganalisa Jaringan. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk sniffing (memperoleh informasi penting seperti password email, dll). Wireshark sendiri merupakan free tools untuk Network Analyzer yang ada saat ini. Dan tampilan dari wireshark ini sendiri terbilang sangat bersahabat dengan user karena menggunakan tampilan grafis atau GUI (Graphical User Interface).

2. WinSCP

   WinSCP adalah sebuah open source file transfer client gratis, dan simple untuk Windows yang mengunakan teknologi Secure Shell (SSH) untuk menyimpan file yang telah disalin antara PC remote dan local dengan menggunakan File Transfer Protocol (FTP), SSH FTP, atau SCP (Secure Copy) protocols dan juga menyediakan beberapa feature pengaturan file dasar.

3. PuTTY

   Putty adalah software remote console/ terminal yang digunakan untuk meremote komp dengan terhubungnya menggunakan port ssh atau sebagainya. Biasanya yang menggunakan software Putty adalah seorang administrator dan seorang Hacker. Putty juga bisa digunakan untuk menjalankan PsyBNC, telnet dan lain-lain.