BAB II

TINJAUAN PUSTAKA

2.1 Konsep Jaringan Komputer

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.

2.2 Jenis-jenis Jaringan Komputer

Adapun jenis-jenis jaringan komputer adalah sebagai berikut :

2.2.1 Berdasarkan Ruang Lingkup Geografis

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

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.

2. *Metropolitan Area Network* (MAN)

   MAN jarak jangkaunya lebih luas dari LAN. Jangkauan MAN dapat mencapai antar kota. Contoh penerapan dari MAN ialah peyediaan layanan internet oleh Internet Service Provider (ISP). Pengguna jasa ISP ini akan tercakup dalam jaringan MAN yang disediakan oleh ISP tersebut.

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.

4. *Global Area Network* (GAN)

   Jaringan *Global Area Network* (GAN) merupakan suatu jaringan yang menghubungkan negara-negara di seluruh dunia. Kecepatan GAN bervariasi mulai dari 1,5 Mbps sampai dengan 100 Gbps dan cakupannya mancapai ribuan kilometer. Contoh yang sangat baik dari GAN ini adalah *internet*.

2.2.2 Berdasarkan *Service*

1. *Intranet*

   Service yang diberikan hanya diberikan kepada pihak-pihak dalam yang mendapat ijin dari otoritas jaringan, dan bukan untuk pihak luar. Terdapat kerahasiaan di dalamnya.

2. *Extranet*

   Terdapat suatu layanan yang juga dapat digunakan oleh pihak luar yang telah memiliki account yang diijinkan. Layanan yang diberikan kepada pihak luar ini bersifat terbatas.

3. *Internet*

   Layanan yang disediakan diberikan secara luas kepada pihak manapun, tanpa harus mendapatkan account terlebih dahulu.

2.3 Definisi *Local Area Network* (LAN)

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.* [BUD3]

2.3.1 Media Transmisi

Media transmisi merupakan jalur yang digunakan untuk dapat melakukan perpindahan data, baik berupa kabel maupun nirkabel (*wireless*). Dalam pemilihan media transmisi perlu mempertimbangkan aspek-aspek sebagai berikut.

1. *Resistance*

   Resistance adalah ketahanan terhadap pengaruh *Electrical Magentic Interface* (EMI). Data yang dialirkan melalui kabel akan berupa gelombang elektromagnetik, sehingga apabila terdapat gelombang elektromagnetik lain di sekitar kabel dapat mengganggu atau merusak data yang berjalan di dalam kabel.

2. *Bandwith*

   Bandwith adalah jumlah frekuensi yang dapat diakomodasi oleh media transmisi. Dengan media yang dapat mengakomodasi jumlah frekuensi lebih banyak, jumlah data yang dikirim atau diterima akan lebih banyak dan dengan waktu pengiriman yang lebih cepat.

3. *Attenuation*

   Attenuation adalah luas jangkauan yang dapat diberikan oleh media transimsi. Luas jangkau ini sendiri dikarenakan adanya hambatan yang dimiliki media transmisi itu sendiri.

4. *Cost*

   Cost adalah dana yang dipunyai dan biaya yang harus dikeluarkan untuk instalasi jaringan tetap harus dibandingkan dengan kebutuhan yang ada.

2.3.1.1 Kabel *Coaxcial*

Kabel koaksial adalah kabel yang memiliki satu *Copper Conductor* dibagian tengahnya. Sebuah lapisan plastik menutupi diantara konduktor dan lapisan

pengaman serat besi. Lapisan serat besi tersebut membantu menutupi gangguan dari arus listrik, lalulintas kendaraan atau mesin dan komputer.



Gambar 2.1 Kabel *Coaxial*

Kelebihan dari kabel koaksial yaitu dapat mendukung penggunaan kabel yang panjang diantara jaringan daripada kabel *Twisted Pair.* Namun, kabel koaksial memiliki kelemahan yaitu sangat sulit untuk proses konfigurasi, kabel ini juga sangat tidak tahan terhadap serangan dari sinyal-sinyal tertentu.

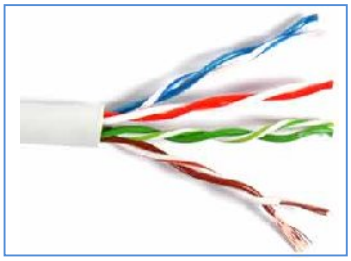
Ada dua jenis tipe kabel koaksial, yaitu kabel *thin coaxial* dan kabel *thick coaxial*. Kabel *thin coaxial* disebut juga dengan 10base2 *(thinnet),* dimana angka 2 menunjuk pada panjang maksimum untuk setiap segmen kabel tersebut yaitu 200 meter, namun kenyataanya hanya dapat menjangkau 185 meter. Kabel ini sangat populer terutama pada penggunaan jaringan yang *linear*. Sedangkan kabel *thick coaxial* disebut juga dengan 10base5 (*thicket*), dimana angka 5 menunjuk pada panjang maksimum untuk setiap segmen kabel tersebut yaitu 500 meter, dan satu kekurangan dari kabel jenis ini adalah tidak lentur dan sangat relatif sulit untuk mengkonfigurasinya. Tipe konektor untuk kabel jenis ini adalah konektor *Bayone-Neill-Concelman* (BNC).

2.3.1.2 *Twisted Pair*

Kabel *twisted pair* terdiri dari dua tipe yaitu sebagai berikut :

1. *Unshielded twisted pair* (UTP)

   Kabel UTP memiliki dua lapisan tembaga, selain itu kabel ini berpilin (*twist*) yang bertujuan untuk mengurangi *crosstalk* antar kabel yang berdekatan dan mengurangi gangguan akibat interferensi elektromagnetik. Kabel UTP memiliki kecepatan transfer data dapat mencapai 10-100 Mbps dan jarak jangkaunya berkisar hingga 100 meter dan kabel ini adalah yang paling populer dan umumnya merupakan pilihan yang terbaik untuk jaringan sederhana.



Gambar 2.2 Kabel UTP

2. *Shielded twisted pair* (STP)

   Karateristik dari kabel STP hampir sama dengan kabel UTP, akan tetapi kabel STP memiliki lapisan tambahan diantara jaket terluar dan pelindung tembaganya, sehingga sesuai untuk digunakan pada instalasi *outdoor*. Kecepatan transfer dan jarak jangkaunya sama dengan kabel UTP yaitu 10-100 Mbps dan 100 meter.



Gambar 2.3 Kabel *twisted pair*

2.3.1.3 *Fiber Optic*

Kabel fiber optic menggunakan cahaya sebagai media untuk mentransmisikan data. Cahaya tersebut dialirkan melalui kaca atau serat plastic tipis yang berada di dalamnya. Kecepatan transfer kabel fiber optic jauh lebih tinggi daripada jenis kabel lainnya. Jarak jangkaunya pun lebih jauh, yaitu mencapai 2500 meter walaupun tanpa menggunakan repeater. Untuk itu kabel ini digunakan untuk jaringan WAN.



Gambar 2.4 *Fiber optic*

2.3.1.4 Wireless

Teknologi komunikasi data yang menggunakan *wireless* antara lain sebagai berikut.

1. *Mobile radio*

   Mobile radio menggunakan gelombang radio sebagai media transmisinya. Pada radio mobil terdapat suatu sentral dari komunikasi dan frekuensi yang telah ditentukan. Contoh penggunaan dari teknologi ini ialah penggunaan *Hand Talk* (HT).

2. *Microwave*

   Microwave merupakan gelombnag dengan frekuansi tinggi yang digunakan untuk point-to-point audio sinyal data. Frekuensi microwave memerlukan garis arah langsung antara pengirim dan penerima. Contoh penggunaannya ialah Access point dan wifi.

3. *Very Small Aperture Terminal* (VSAT)

   Very Small Aperture Terminal merupakan bagian dari satelit.. VSAT dapat mengirim dan menerima suara, data, dan sinyal video. Setiap data yang dikirim dari VSAT ke bagian lain di bumi akan diteruskan oleh transmitter ke satelit yang berfungsi *concentrator*. VSAT mampu menangani data sampai dengan 56 Kbps.

4. *Mobile Satellite Communication*

   Contoh paling dekat *mobile Satellite Communication* adalah ponsel yang dikhususkan untuk berkomunikasi melalui sebuah pemancar yang berada di

bumi dan kemudian diteruskan menuju satelit untuk dipancarkan kembali ke stasiun bumi yang lain dan diteruskan ke user yang dituju.

2.3.2 Topologi Jaringan

Topologi jaringan diklasifikasikan menjadi dua, yaitu topologi fisik dan topologi logik. Topologi fisik merupakan *map* (peta) dari jaringan atau merupakan *layout* dari pengkabelan dan workstation jaringan yang mendeskripsikan lokasi semua komponen jaringan, sedangkan topologi logik mendefinisikan mekanisme aliran data atau informasi dalam jaringan.

Terdapat beberapa macam topologi fisik yang sering digunakan, antara lain sebagai berikut.

1. Bus
2. Ring
3. Star
4. Mesh
5. Wireless

Selain topologi fisik, berikut merupakan beberapa macam topologi logik yang biasa digunakan :

1. Topologi logik Bus
2. Topologi logik Token Ring

2.3.2.1 Topologi *Bus*

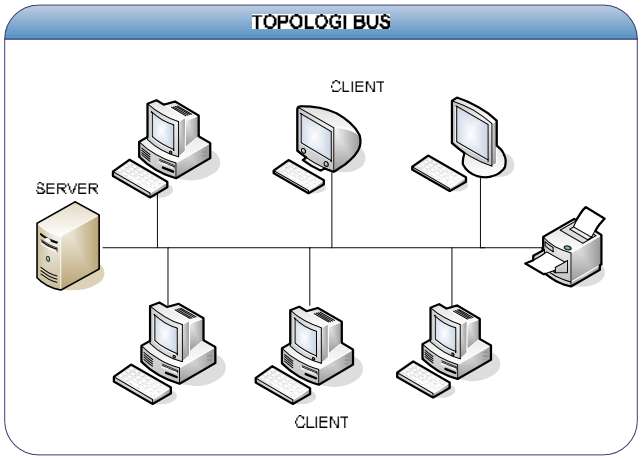
Topologi bus menggunakan satu jalur data utama (*backbone*) sebagai jalur utama komunikasi. Apabila pesan dikirim, tidak hanya komputer tujuan yang menerima data, akan tetapi semua komputer yang tergabung di dalam jaringan tersebut akan mendapatkan pesan yang sama. Bila terjadi komunikasi data yang sangat padat, kemungkinan terjadinya tabrakan (*collusion*) akan semakin besar dan membuat kinerja jaringan menurun.

Kabel yang digunakan pada jaringan ini ialah kabel coaxial 50 ohm dan dengan konektor RG58 untuk disambungkan dengan LAN Card di komputer. Dan untuk menyambung dari kabel utama (*backbone*) ke kabel yang dihubungkan ke komputer diperlukan konektor BNC. Setiap kabel ini mempunyai jarak jangkau (*atteniation*) sejauh 185 meter. Bila ingin menggunakan dengan jarak yang lebih dari itu, maka diperlukan repeater.

Kelebihan dan kekurangan dari topologi *Bus* :

1. Kelebihan Topologi Fisik *Bus*:
    a. Kemudahan untuk instalasi
    b. Relatif lebih murah
    c. Memerlukan kabel yang lebih pendek dibanding topologi fisik lain
2. Kekurangan Topologi Fisik *Bus*:
    a. Kesulitan untuk dipindahkan atau dirubah
    b. *Fault tolerance* yang kecil

c. Kesulitan untuk troubleshooting jika terdapat masalah jaringan



Gambar 2.5 Topologi Bus

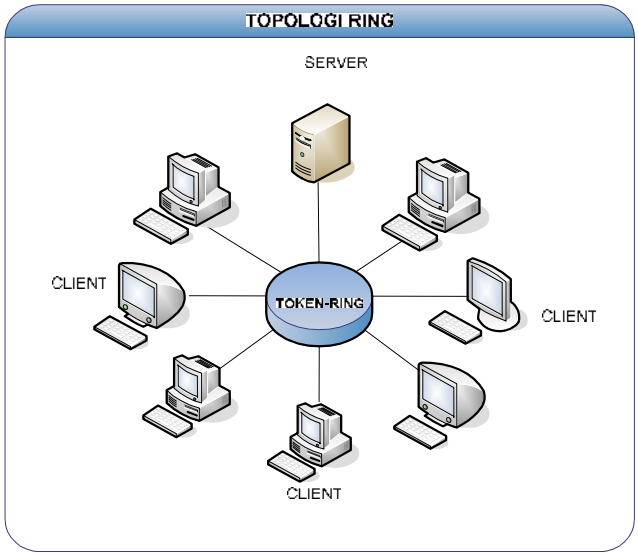
2.3.2.2 Topologi *Ring*

Seluruh komputer dalam jaringan terhubung pada sebuah jalur data yang sambung menyambung sehingga berbentuk menyerupai cincin. Setiap komputer akan berfungsi sebagai repeater yang menerima sinyal dari komputer sebelumnya, memperkuatnya, dan kemudian meneruskan ke komputer berikutnya. Sehingga, topologi ring memberikan jarak jangkau yang lebih jauh.

Kelebihan dan kekurangan dari topologi *Ring* :

1. Kelebihan Topologi *Ring* :
    a. Kemudahan dalam desain kabel.
    b. Mudah melakukan *troubleshoot*.
2. Kekurangan Topologi *Ring*:
    a. Kesulitan untuk rekonfigurasi.

b. *Fault Tolerance* kecil, sehingga kerusakan pada satu jalur kabel membuat keseluruhan jaringan *down*.



Gambar 2.6 Topologi *Ring*

2.3.2.3 Topologi *Star*

Ciri utama dari jaringan ini ialah adanya *concentrator*. Seluruh komputer dalam jaringan dihubungkan ke pusat secara langsung tanpa melalui komputer yang lain, sehingga setiap komputer akan memiliki jalur sendiri untuk sampai ke pusat (*concentrator*). *Concentrator* dapat berupa hub, switch, router, ataupun multi point repeater.

Kelebihan dan kekurangan dari topologi *Star* :

1. Kelebihan Topologi *Star* :
   a. Lebih *Fault Tolerance* dibanding *Bus*.

b. Komponen baru jaringan lebih mudah ditambahkan.

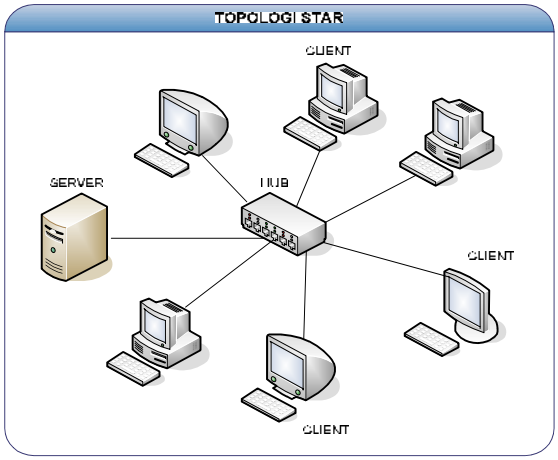
c. Kerusakan pada satu kabel tidak akan membuat *down* keseluruhan jaringan.

d. Mudah melakukan *troubleshoot*.

2. Kekurangan Topologi *Star*:

a. Jika *node* tengah mengalami kerusakan, maka seluruh jaringan akan terhenti

b. Relatif mahal, karena membutuhkan pengkabelan yang lebih panjang.



Gambar 2.7 Topologi *Star*

2.3.2.4 Topologi *Mesh*

Topologi *Mesh* adalah suatu topologi yang memang didisain untuk memiliki tingkat restorasi dengan berbagai alternatif rute atau penjaluran yang biasanya disiapkan dengan dukungan perangkat lunak atau *software*. Komponen utama yang digunakan dalam topologi mesh ini adalah *Digital Cross Connect* (DXC) dengan satu atau lebih dari dua sinyal *aggregate*, dan tingkat *cross connect*

(koneksi persilangan) yang beragam pada level sinyal SDH. Topologi jaringan mesh ini menerapkan hubungan antar sentral secara penuh. Jumlah saluran ini harus disediakan untuk membentuk suatu jaringan topologi *mesh* adalah jumlah sentral dikurangi 1 (n-1, dengan n adalah jumlah sentral).

Kelebihan dan kekurangan dari topologi *Mesh* :

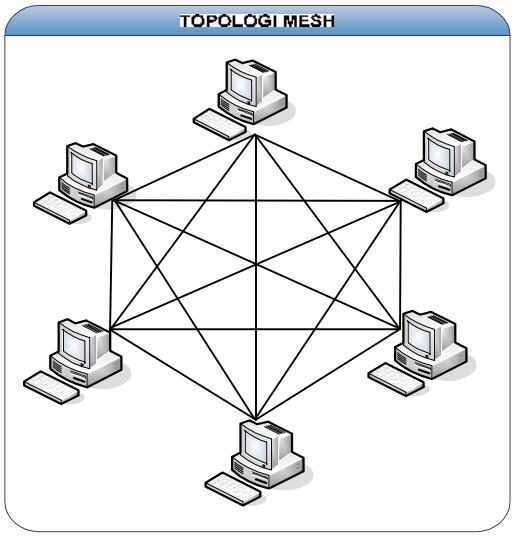
1. Kelebihan Topologi *Mesh*:

   Apabila ada salah satu jalur pada komputer putus, komputer masih dapat berhubungan dengan jalur yang lain.

2. Kekurangan Topologi *Mesh*:

   a. Mahal.

   b. Penggunaan ethernet dan kabel yang banyak sehingga dibutuhkan dana yang besar



Gambar 2.8 Topologi *Mesh*

2.3.2.5 Topologi *Wireless (AdHoc Network)*

Topologi *wireless* akan terbentuk jika terdapat 2 atau lebih entity jaringan yang mempunyai RF transceiver dan mensuport *AdHoc Networking*, berada pada jarak yang memungkinkan untuk berkomunikasi. *AdHoc network* memungkinkan pemakai untuk saling berkomunikasi dan saling tukar menukar data secara langsung.

2.3.3 Faktor-faktor dalam pemilihan topologi

Berikut adalah beberapa faktor yang harus dipertimbangkan dalam pemilihan topologi yang akan digunakan untuk jaringan komputer :

1. Biaya
2. Kecepatan
3. Lingkungan
4. Ukuran
5. Konektivitas

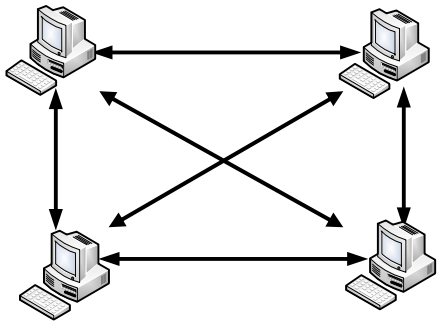
2.3.4 Model Hubungan Pada LAN

Model hubungan pada LAN terbagi menjadi dua, yaitu :

2.3.4.1 *Peer-to-peer*

Model hubungan *peer-to-peer* memungkinkan user membagi sumber dayanya yang ada dikomputernya 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.



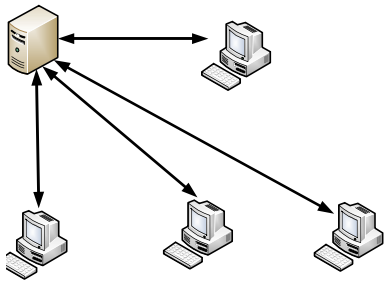
Gambar 2.9 Model hubungan *peer-to-peer*

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.

2.3.4.2 *Client Server*

Model hubungan *client server* 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 sumber daya pada *file server*.



Gambar 2.10 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*

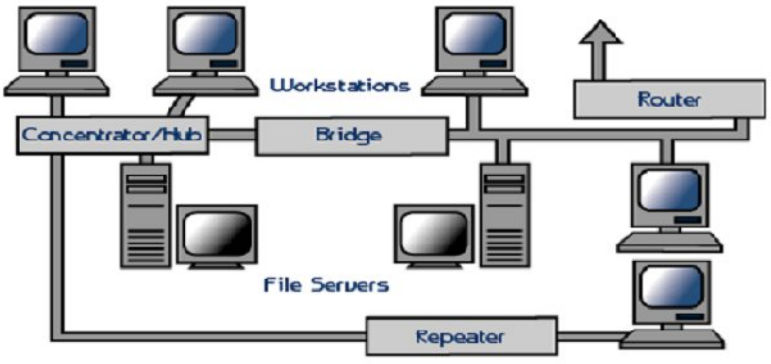
    c. Perbaikan (jaringan besar membutuhkan seorang staf untuk mengatur agar sistem berjalan secara efisien)

    d. Berketergantungan

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

2.3.5 Perangkat Keras Pada LAN

Perangkat keras yang dibutuhkan untuk membangun sebuah jaringan komputer yaitu : Komputer, Card Network, Hub, dan segala sesuatu yang berhubungan dengan koneksi jaringan seperti: Printer, CDROM, Scanner, Bridges, Router dan lainnya yang dibutuhkan untuk process transformasi data didalam jaringan.



Gambar 2.11 Perangkat keras pada LAN

1. File Servers

2. Workstations

3. Network Interface Cards

4. Concentrators/Hubs

5. Repeaters

6. Bridges

7. Routers

2.3.5.1 *File Server*

Sebuah file server merupakan jantungnya kebayakan Jaringan, merupakan komputer yang sangat cepat, mempunyai memori yang besar, harddisk yang memiliki kapasitas besar, dengan kartu jaringan yang cepat. Sistem operasi jaringan tersimpan disini, juga termasuk didalamnya beberapa aplikasi dan data yang dibutuhkan untuk jaringan.

Sebuah file server bertugas mengontrol komunikasi dan informasi diantara node/komponen dalam suatu jaringan. Sebagai contoh mengelola pengiriman file database atau pengolah kata dari workstation atau salah satu node, ke node yang lain, atau menerima email pada saat yang bersamaan dengan tugas yang lain terlihat bahwa tugas file server sangat kompleks, dia juga harus menyimpan informasi dan membaginya secara cepat.

Minimal sebuah file server mempunyai beberpa karakter seperti tersebut di bawah ini :

a. Processor minimal 166 megahertz atau processor yang lebih cepat lagi (Pentium Pro, Pentium II, PowerPC).
b. Sebuah Harddisk yang cepat dan berkapasitas besar atau kurang lebih 10 GB
c. Sebuah RAID (Redundant Array of Inexpensive Disks).Sebuah tape untuk back up data (contohnya . DAT, JAZ, Zip, atau CD-RW)
d. Mempunyai banyak port network
e. Kartu jaringan yang cepat dan Reliabilitas
f. Kurang lebih 32 MB memori

2.3.5.2 *Workstations*

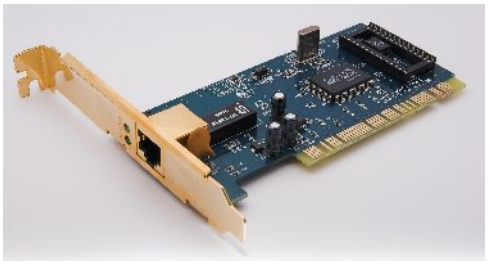
Keseluruhan komputer yang terhubung ke file server dalam jaringan disebut sebagai workstation. Sebuah workstation minimal mempunyai ; Kartu jaringan, Aplikasi jaringan (sofware jaringan), kabel untuk menghubungkan ke jaringan, biasanya sebuah workstation tidak begitu membutuhkan Floppy karena data yang ingin di simpan bisa dan dapat diletakkan di file server. Hampir semua jenis komputer dapat digunakan sebagai komputer workstation.

2.3.5.3 *Network Interface Cards* (NIC) atau Kartu Jaringan

Kartu Jaringan (NIC) merupakan perangkat yang menyediakan media untuk menghubungkan antara komputer, kebanyakan kartu jaringan adalah kartu inernal, yaitu kartu jaringan yang di pasang pada slot ekspansi di dalam komputer.

Berdasarkan tipe bus, ada beberapa tipe *Network Interface Card* (NIC) atau *Network Card*, yaitu ISA dan PCI. Saat ini terdapat jenis *network card* yang banyak digunakan, yaitu PCI.

Kartu jaringan yang banyak terpakai saat ini adalah : kartu jaringan Ethernet, LocalTalk konektor, dan kartu jaringan Token Ring. Yang saat ini populer digunakan adalah Ethernet, lalu diikuti oleh Token Ring, dan LocalTalk.



Gambar 2.12 *Network Interface Cards* (NIC)

2.3.5.4 *Ethernet Card* (Kartu Jaringan *Ethernet*)

Kartu Jaringan *ethernet* umumnya telah menyediakan port koneksi untuk kabel Koaksial ataupun kabel twisted pair, jika didesain untuk kabel koaksial

konenektorya adalah BNC, dan apabila didesain untuk kabel twisted pair maka akan punya konektor RJ-45. Beberapa kartu jaringan ethernet kadang juga punya konektor AUI. Semua itu di koneksikan dengan koaksial, twisted pair,ataupun dengan kabel fiber optik. Kartu Jaringan *ethernet* biasanya dibeli terpisah dengan komputer, kecuali seperti komputer Macintosh yang sudah mengikutkan kartu jaringan ethernet didalamnya.

2.3.5.5 *LocalTalk Connectors*

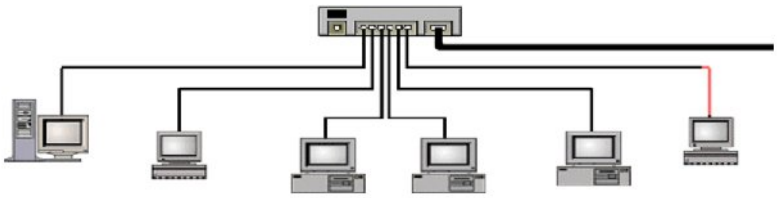
LocalTalk adalah kartu jaringan buat komputer macintosh, ini menggunakan sebuah kotak adapter khusus dan kabel yang terpasang ke Port untuk printer. Kekurangan dari LocalTalk dibandingkan Ethernet adalah kecepatan laju transfer datanya, Ethernet bi Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir di setiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi di dalam perudahaan tersebut. Internet yang mulai populer saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan jaringan komputer yang terhubungan dan dapat saling berinteraksi. Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat, sehingga dalam beberapa tahun saja jumlah pengguna jaringan komputer yang tergabung dalam Internet berlipat ganda.asanya dapat sampai 10 Mbps, sedangkan LocalTalk hanya dapat beroperasi pada kecepatan 230 Kbps atau setara dengan 0.23 Mps

2.3.5.6 *Token Ring Cards*

Kartu jaringan Token Ring terlihat hampir sama dengan Kartu jaringan Ethernet. Satu perbedaannya adalah tipe konektor di belakang KArtu jaringannya, Token Ring umumnya mempunyai tipe konektor 9 Pin DIN yang menyambung Kartu jaringan ke Kabel Network.

2.3.5.7 *Hub* atau Konsentrator

Sebuah Konsentrator/Hub adalah sebuah perangkat yang menyatukan kabel-kabel network dari tiap-tiap workstation, server atau perangkat lain. Dalam topologi Star, kabel twisted pair datang dari sebuah workstation masuk kedalam hub. Hub mempunyai banyak slot concentrator yang mana dapat dipasang menurut nomor port dari card yang dituju.



Gambar 2.13 *Hub* atau Konsentrator

Ciri-ciri yang dimiliki Konsentrator adalah :

a. Biasanya terdiri dari 8, 12, atau 24 port RJ-45
b. Digunakan pada topologi Star/Star
c. Biasanya di jual dengan aplikasi khusus yaitu aplikasi yang mengatur manjemen port tersebut.

d. Biasanya disebut hub

e. Biasanya di pasang pada rak khusus, yang didalamnya ada Bridges, router

2.3.5.8 *Repeaters*

Contoh yang paling mudah adalah pada sebuah LAN menggunakan topologi Topologi Star dengan menggunakan kabel unshielded twisted pair. Dimana diketahui panjang maksimal untuk sebuah kabel unshileded twisted pair adalah 100 meter, maka untuk menguatkan sinyal dari kabel tersebut dipasanglah sebuah repeater pada jaringan tersebut.



Gambar 2.14 *Repeater*

2.3.5.9 *Bridges* (Jembatan)

Bridge Adalah sebuah perangkat yang membagi satu buah jaringan kedalam dua buah jaringan, ini digunakan untuk mendapatkan jaringan yang efisien, dimana kadang pertumbuhan network sangat cepat makanya di perlukan jembatan untuk itu. Kebanyakan Bridges dapat mengetahui masing-masing alamat dari tiap-tiap segmen komputer pada jaringan sebelahnya dan juga pada jaringan yang lain di sebelahnya pula. Diibaratkan bahwa Bridges ini seperti polisi lalu lintas yang mengatur di persimpangan jalan pada saat jam-jam sibuk. Dia mengatur agar informasi di antara kedua sisi network tetap jalan dengan baik dan teratur. Bridges

juga dapat di gunakan untuk mengkoneksi diantara network yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula.

2.3.5.10 *Routers*

Sebuah Router mengartikan informaari dari satu jaringan ke jaringan yang lain, dia hampir sama dengan Bridge namun agak pintar sedikit, router akan mencari jalur yang terbaik untuk mengirimkan sebuah pesan yang berdasakan atas alamat tujuan dan alamat asal.

Sementara Bridges dapat mengetahui alamat masing-masing komputer di masing-masing sisi jaringan, router mengetahui alamat komputerr, bridges dan router lainnya. router dapat mengetahui keseluruhan jaringan melihat sisi mana yang paling sibuk dan dia bisa menarik data dari sisi yang sibuk tersebut sampai sisi tersebut bersih.

Jika sebuah perusahaan mempunyai LAN dan menginginkan terkoneksi ke Internet, mereka harus membeli router. Ini berarti sebuah router dapat menterjemahkan informasi diantara LAN anda dan Internet. ini juga berarti mencarikan alternatif jalur yang terbaik untuk mengirimkan data melewati internet.

Ini berarti Router itu :

a. Mengatur jalur sinyal secara effisien
b. Mengatur Pesan diantara dua buah protocol
c. Mengatur Pesan diantara topologi jaringan linear Bus dan Star

d. Mengatur Pesan diantara melewati Kabel *Fiber optic*, kabel koaksial atau kabel *twisted pair*

2.4 Protokol Pada *Local Area Network* (LAN)

Protokol adalah aturan-aturan main yang mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan, aturan itu termasuk di dalamnya petunjuk yang berlaku bagi cara-cara atau metode mengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan transfer data.

Protokol-Protokol yang dikenal adalah sebagai berikut :

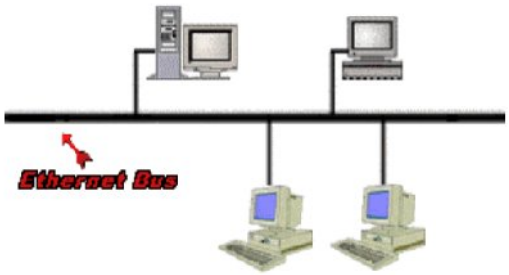
1. Ethernet
2. Local Talk
3. Token Ring
4. FDDI
5. ATM

2.4.1 *Ethernet*

Protocol Ethernet sejauh ini adalah yang paling banyak digunakan, Ethernet menggunakan metode akses yang disebut CSMA/CD *(Carrier Sense Multiple Access/Collision Detection)*. Sistem ini menjelaskan bahwa setiap komputer memperhatikan ke dalam kabel dari network sebelum mengirimkan sesuatu ke dalamnya. Jika dalam jaringan tidak ada aktifitas atau bersih komputer akan mentransmisikan data, jika ada transmisi lain di dalam kabel, komputer akan

menunggu dan akan mencoba kembali transmisi jika jaringan telah bersih. kadangkala dua buah komputer melakukan transmisi pada saat yang sama, ketika hal ini terjadi, masing-masing komputer akan mundur dan akan menunggu kesempatan secara acak untuk mentransmisikan data kembali. metode ini dikenal dengan koalisi, dan tidak akan berpengaruh pada kecepatan transmisi dari *network*.

Protokol *Ethernet* dapat digunakan untuk pada model jaringan *bus*, *star*, atau tree . Data dapat ditransmisikan melewati kabel *twisted pair*, koaksial, ataupun kabel *fiber optic* pada kecepatan 10 Mbps.



Gambar 2.15 *Ethernet*

2.4.2 *LocalTalk*

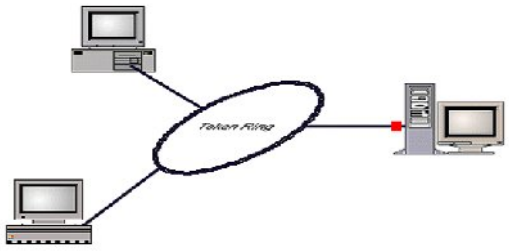
LocalTalk adalah sebuh protokol network yang di kembangkan oleh Apple Computer, Inc. untuk mesin-mesin komputer Macintosh . Metode yang digunakan oleh *LocalTalk* adalah CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance)*. Hampir sama dengan CSMA/CD.. Adapter *LocalTalk* dan kabel *twisted pair* khusus dapat digunakan untuk menghubungkan beberapa komputer

melewati port serial. Sistem Operasi Macintosh memungkinkan koneksi secara jaringan *peer-to-peer* tanpa membutuhkan tambahan aplikasi khusus

Protokol *LocalTalk* dapat digunakan untuk model jaringan *bus*, *star*, ataupun model *tree* dengan menggunakan kabel *twisted pair*. Kekurangan yang paling mencolok yaitu kecepatan transmisinya. Kecepatan transmisinya hanya 230 Kbps.

2.4.3 *Token Ring*

Protokol Token di kembangkan oleh IBM pada pertengahan tahun 1980. Metode Aksesnya melalui lewatnya sebuah token dalam sebuah lingkaran seperti Cincin . Dalam lingkaran token, komputer-komputer dihubungkan satu dengan yang lainnya seperti sebuah cincin. Sebuah Sinyal token bergerak berputar dalam sebuah lingkaran (cincin) dalam sebuah jaringan dan bergerak dari sebuah komputer-menuju ke komputer berikutnya, jika pada persinggahan di salah satu komputer ternyata ada data yang ingin ditransmisikan, token akan mengangkutnya ke tempat dimana data itu ingin ditujukan, token bergerak terus untuk saling mengkoneksikan diantara masing-masing komputer.

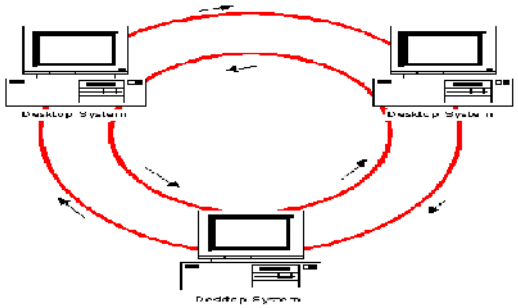


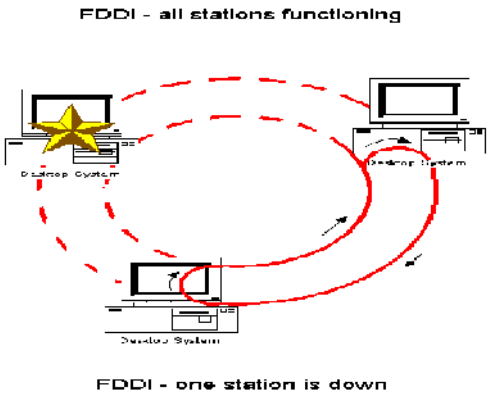
Gambar 2.16 *Token Ring*

Protokol *token ring* membutuhkan model jaringan *star* dengan menggunakan kabel *twisted pair* atau kabel *fiber optic* . Dan dapat melakukan kecepatan transmisi 4 Mbps atau 16 Mbps. Sejalan dengan perkembangan Ethernet, penggunaan *token ring* makin berkurang sampai sekarang.

2.4.4 *Fiber Distributed Data Interface* (FDDI)

Fiber Distributed Data Interface (FDDI) adalah sebuah protokol jaringan yang menghubungkan antara dua atau lebih jaringan bahkan pada jarak yang jauh . Metode aksesnya yang digunakan oleh FDDI adalah model token . FDDI menggunakan dua buah topologi *ring* secara fisik. Proses transmisi baiasanya menggunakan satu buah *ring*, namun jika ada masalah ditemukan akan secara otomatis menggunakan *ring* yang kedua.





Gambar 2.17 FDDI *All station dan One station*

Sebuah keuntungan dari FDDI adalah pada kecepatannya, karena menggunakan *fiber optic cable* pada kecepatan 100 Mbps.

2.4.5 *Asynchronous Transfer Mode* (ATM)

ATM adalah singkatan dari *Asynchronous Transfer Mode* (ATM) yaitu sebuah protokol jaringan yang mentransmisikan pada kecepatan 155 Mbps atau lebih. ATM mentarnsmisikan data kedalam satu paket dimana pada protokol yang lain mentransfer pada besar-kecilnya paket. ATM mendukung variasi media seperti video, CD-audio, dan gambar. ATM bekerja pada model topologi star dengan menggunakan kabel *fiber optic* ataupun kabel *twisted pair*. ATM pada umumnya digunakan untuk menghubungkan dua atau lebih LAN. ATM juga banyak dipakai oleh *Internet Service Providers* (ISP) untuk meningkatkan kecepatan akses *internet* untuk klien mereka.

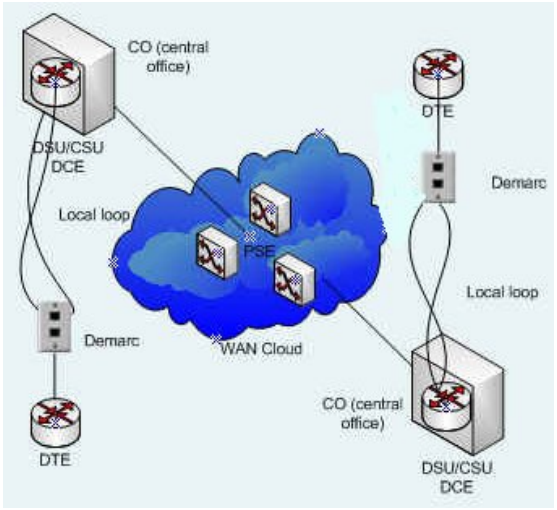
Tabel 2.1 Perbandingan Protokol pada LAN

Protokol yang dipakai	Kabel yang digunakan	Kecepatan transfer	Topologi Fisik
Ethernet	Twisted Pair, Coaxial, Fibre	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fibre	100 Mbps	Star
Local Talk	Twisted Pair	0, 23 Mbps	Linear Bus, Star
Token Ring	Twisted Pair	4 Mbps – 16 Mbps	Star – Wired Ring
FDDI	Fiber	100 Mbps	Dual Ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

2.5 Koneksi WAN

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.

Diagram dibawah ini adalah struktur koneksi WAN yang umum dipakai.



Gambar 2.18 Struktur Koneksi WAN

DTE adalah Data Terminal Equipment yang berada pada sisi koneksi link WAN yang mengirim dan menerima data. DTE ini berada pada sisi bangunan si pelanggan dan sebagai titik tanda masuk antara jaringan WAN dan LAN. DTE ini biasanya berupa router, akan tetapi computer dan multiplexer juga bisa bertindak sebagai DTE. Secara luas, DTE adalah semua equipment yang berada pada sisi tempat si pelanggan yang berkomunikasi dengan DCE pada sisi yang lain.

Demarc adalah titik demarkasi dimana perkabelan dari perusahaan telpon terhubung ke perkabelan di sisi rumah pelanggan. Umumnya pelanggan bertanggung jawab terhadap semua *equipment* disisi demark dan pihak Telkom bertanggung jawab semua *equipment* disisi lain dari demark.

Local loop adalah kabel ekstensi ke kantor central telephone.

Central office adalah fasilitas *switching* dan juga memberikan *entry* WAN *cloud* dan juga *exit points* untuk panggilan masuk dan keluar, dan juga bertindak sebagai *switching point* untuk meneruskan data ke *central office* lainnya. *Central office* juga memberikan layanan seperti *switching* sinyal telpon masuk menuju *trunk line*. CO juga berfungsi memberikan catu daya DC ke *local loop* untuk membentuk *circuit electric*.

DCE adalah peralatan data circuit terminating yang berkomunikasi dengan DTE dan juga WAN cloud. DCE pada umumnya berupa router disisi penyedia jasa yang merelay data pesan antara *customer* dan WAN *cloud*. DCE adalah piranti yang mensuplay *signal clocking* ke DTE. Suatu modem atau CSU/DSU disisi pelanggan sering diklasifikasikan sebagai DCE. DCE bisa serupa DTE seperti router akan tetapi masing-2 mempunyai perannya sendiri.

PSE adalah *packet switching exchange*, suatu *switch* pada jaringan pembawa *packet-switched*. PSE merupakan titik perantara di WAN *cloud*.

WAN *cloud* adalah hirarkhi dari *trunk, switch,* dan *central office* yang membentuk jaringan sambungan telpon. Kenapa di presentasikan dengan Cloud karena struktur fisik bermacam-2 dan jaringan-2 dengan titik koneksi bersama bisa saling timpang tindih.

2.5.1 Standar koneksi WAN

Koneksi standard WAN yang direkomendasikan adalah sebagai berikut.

a Untuk layanan WAN menggunakan koneksi serial, gunakanlah kabel serial V.35

b Untuk koneksi WAN berkecepatan rendah (dibawah 64Kbps) yang biasa diasosiasikan dengan PSTN analog, gunakanlah kebel serial RS-232.

c Untuk koneksi ISDN BRI, kabel UTP (Cat5) yang digunakan seharusnya memakai kabel dengan warna yang berbeda (putih atau kuning) dari kabel UTP yang umum dipakai untuk menunjukkan bahwa kabel tersebut adalah koneksi WAN. Perlu diperhatikan bahwa peralatan ISDN yang disambungkan pada piranti yang buksan ISDN bisa menyebabkan kerusakan.

d Untuk koneksi WAN ISDN, terminal adapter (TA) haruslah dihindari; sebaiknya gunakan router ISDN native.

e Semua perkabelan haruslah di dokumentasikan dan diberi label dengan jelas.

2.5.2 Kategori Koneksi WAN

Adapaun WAN dikategorikan sebagai berikut

a Dedicated *point-to-point* atau *leased line* (serial *synchronous*) seperti T1, T3

b Jaringan *circuit-switched* (asynchronous serial) seperti ISDN

c Jaringan *packet-switched* (synchronous serial) seperti frame relay, x.25

2.5.2.1 *Dedicated connection* atau *leased line*

Dedicated connection atau *leased line* adalah koneksi sambungan permanen *point-to-point* antara dua piranti yang mempunyai karakteristik berikut ini:

a *Dedicated point-to-point* – serial *synchronous*

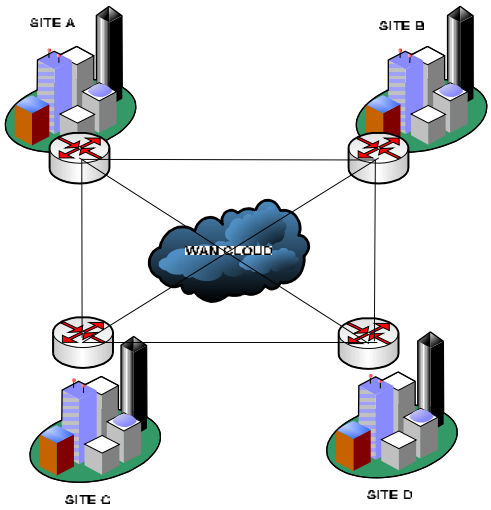
b Koneksi permanen, seperti T1, T3

c Ketersediannya tinggi

d Sambungan biasanya disewa dari penyedia layanan WAN

e *Leased line* lebih mahal dibanding solusi WAN lainnya

f Menggunakan koneksi terpisah di masing-2 titik



Gambar 2.19 Koneksi WAN *Point to Point*

2.5.2.1.1 Penggunaan Sambungan WAN jenis leased line

Biasanya *leased line* digunakan apabila dalam kondisi seperti berikut :

a Jika jaringan kita mempunyai trafik yang sangat tinggi melalui jaringan WAN

b Jika memerlukan sambungan konstan antar *site*

c Hanya mempunyai beberapa interkoneksi *site* saja

2.5.2.2 Jaringan *circuit-switched*

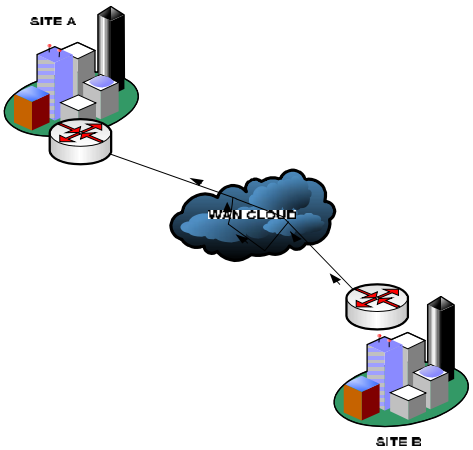
Jenis koneksi jaringan *circuit-switched* memberikan alternative dari sambungan *leased line*, memungkinkan kita menggunakan sambungan bersama (*share line*). Koneksi WAN jenis ini bekerja dua arah, koneksi WAN *dial-in* dan *dial-out*. Saat kita memakai koneksi WAN *circuit-switched*, maka:

a Komputer pengirim *dial-in* ke sambungan dan terbentuklah koneksi WAN

b Komputer penerima mengirim pemberitahuan dan mengunci sambungan

c Komputer pengirim mentransmisikan data melalui koneksi WAN ini

d Setelah transmisi selesai, koneksi dilepas agar user yang lain bisa memakai



Gambar 2.20 Koneksi WAN *Circuit Switched*

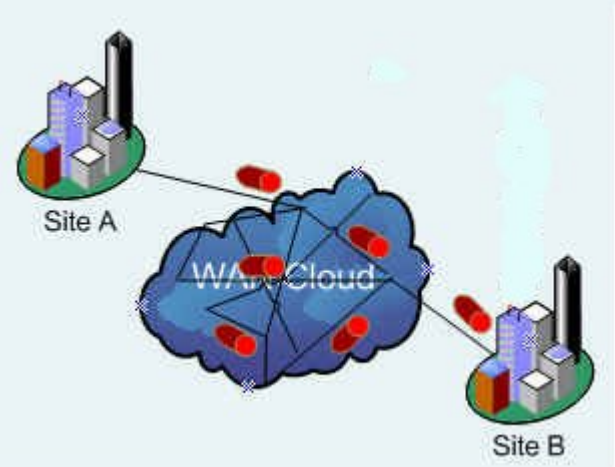
Jaringan *cisrcuit-switched* menggunakan *switch virtual circuit* (SVC). Suatu jalur *dedicated* transmisi data terbentuk sebelum komunikasi dimulai dengan cara melepas *switch electric*. Jalur ini akan tetap terbentuk sampai komunikasi berakhir.

2.5.2.3 Jaringan *Packet-switched*

Jaringan *packet-switched* tidak memerlukan sambungan tersendiri atau sambungan cadangan sementara. Sebaliknya jenis jaringan *packet-switched* ini memungkinkan jalur paket data di set secara dinamis ketika data mengalir melalui jaringan. Jenis koneksi jaringan ini mempunyai karakteristik sebagai berikut:

a *Message* dipecah kedalam paket-2
b Paket-2 menjelajah secara independen melalui inter-jaringan (yaitu mengambil jalur yang berbeda)
c Pada sisi penerima paket-2 di *assembling* ulang pada urutan yang tepat
d Piranti pengirim dan penerima mengasumsikan suatu koneksi yang ’selalu on’ (tidak memerlukan *dial-up*)

Jenis koneksi jaringan WAN ini menggunakan permanent virtual circuit (PVC). Walaupun suatu PVC terlihat terhubung langsung – jalur WAN tersendiri, jalur yang diambil setiap paket melalui inter-jaringan dapat berbeda



Gambar 2.21 Koneksi WAN *paket switched*

Jaringan *dedicated* dan *packet-switched* mempunyai sambungan koneksi WAN yang selalu tersedia ke dalam jaringan, sementara jaringan *circuit-switched* pertama harus membuat jalur koeksi WAN terbentuk terlebih dahulu antar piranti (melalui *dial-up*). Dial-on-demand routing (DDR) dapat mensimulasikan koneksi WAN yang selalu on. Dengan DDR router secara automatis membuka koneksi WAN baru jika data perlu dikirim, dan kemudian menutup sendiri saat sambungan jadi idle. Teknologi WAN terbaru memperbaiki proses koneksi WAN menjadi lebih pendek.

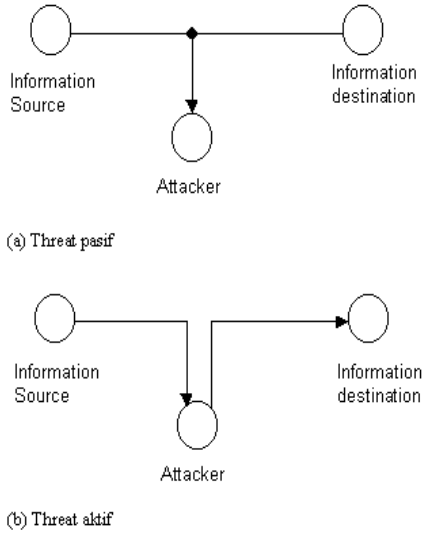
2.6 Keamanan Jaringan Komputer

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh person yang tidak diijinkan.

Terdapat dua kategori threat yaitu *threat* pasif dan *threat* aktif.

a. *Threat* pasif melakukan pemantauan dan atau perekaman data selama data ditranmisikan lewat fasilitas komunikasi. Tujuan penyerang adalah untuk mendapatkan informasi yang sedang dikirimkan.

b. *Threat* aktif merupakan pengguna gelap suatu peralatan terhubung fasilitas komunikasi untuk mengubah transmisi data atau mengubah isyarat kendali atau memunculkan data atau isyarat kendali palsu.



Gambar 2.22 *Thread* aktif dan *thread* pasif

Seberapa besar tingkat ancaman dapat diukur dengan melihat beberapa faktor, antara lain :

a. Kegunaan sistem

b. Kerahasiaan data dalam sistem.

c. Tingkat kepetingan dari integritas data

d. Kepentingan untuk menjaga akses yang tidak boleh terputus

e. Profil pengguna

f. Hubungan antara sistem dengan sistem yang lain.

Suatu cara untuk pengamanan data adalah dengan enkripsi. Dalam hal ini terdapat tiga kategori enkripsi antara lain :

a. Kunci enkripsi rahasia, dalam hal ini terdapat sebuah kunci yang digunakan untuk meng-enkripsi dan juga sekaligus men-dekripsi informasi.

b. Kunci enksripsi public, dalam hal ini dua kunci digunakan, satu untuk proses enkripsi dan yang lain untuk proses dekripsi.

c. Fungsi one-way, di mana informasi di-enkripsi untuk menciptakan "signature" dari informasi asli yang bisa digunakan untuk keperluan autentifikasi.

Enkripsi dibentuk dengan berdasarkan suatu algoritma yang akan mengacak suatu informasi menjadi bentuk yang tidak bisa dibaca atau tak bisa dilihat. Dekripsi adalah proses dengan algoritma yang sama untuk mengembalikan informasi teracak menjadi bentuk aslinya. Algoritma yang digunakan harus terdiri dari susunan prosedur yang direncanakan secara hati-hati yang harus secara

efektif menghasilkan sebuah bentuk terenkripsi yang tidak bisa dikembalikan oleh seseorang bahkan sekalipun mereka memiliki algoritma yang sama.

Tujuan dari sistem kriptografi adalah :

a. *Confidentiality* : memberikan kerahasiaan pesan dan menyimpan data dengan menyembuyikan informasi lewat teknik-teknik enkripsi.

b. *Message Integrity* : memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat ia dibuat samapai saat ia dibuka.

c. *Non-repudiation* : memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut.

d. *Authentication* : Memberikan dua layanan. Pertama mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikannya. Kedua untuk menguji identitas seseorang apabila ia kan memasuki sebuah sistem.

1. Beberapa contoh algoritma yang menggunakan kunci-simetris:
   a. DES - Data Encryption Standard
   b. blowfish
   c. twofish
   d. MARS

e. IDEA

f. 3DES - DES diaplikasikan 3 kali

g. AES - Advanced Encryption Standard, yang bernama asli rijndael

2. Beberapa contoh algoritma yang menggunakan kunci-Asimetris:

a. Knapsack

b. RSA - Rivert-Shamir-Adelman

c. Diffie-Hellman

3. Beberapa contoh algoritma fungsi hash Kriptografi :

a. MD4

b. MD5

c. SHA-0

d. SHA-1

e. SHA-256

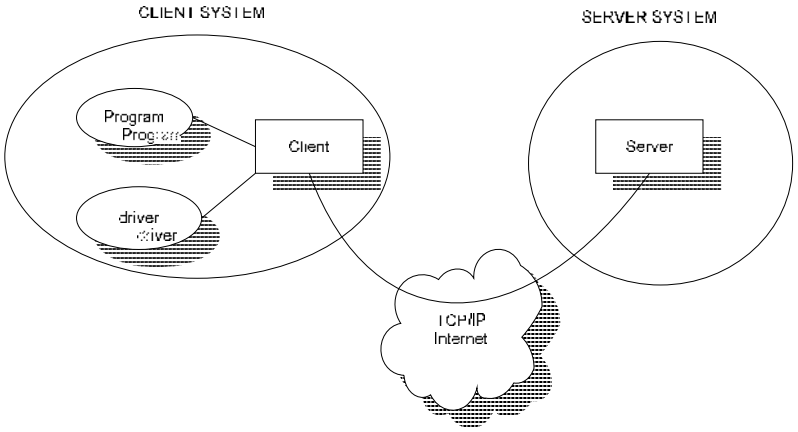
f. SHA-512

2.7 Definisi *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).*

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*.

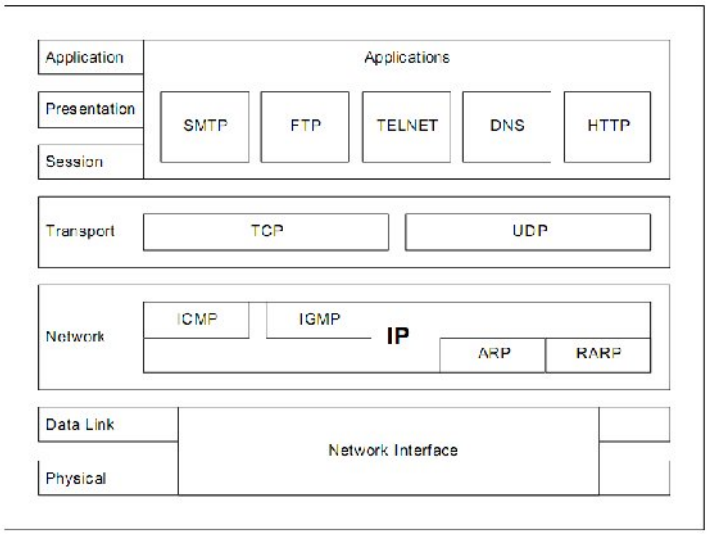


Gambar 2.23 Model *Client Server Internet*

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



Gambar 2.24 Susunan protokol TCP/IP dan model OSI

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

1. *Application Layer*, yaitu layer yang bertanggung jawab terhadap aplikasi-aplikasi yang menggunakan TCP/IP.

2. *Transport Layer*, yaitu layer yang bertanggung jawab memberikan layanan pengiriman data dari satu node ke node yang lain.
3. *Internet Layer*, yaitu layer yang menentukan jenis datagram dan menangani perutean data yang dikirim.
4. *Network Interface Layer*, yaitu layer yang bertanggung jawab untuk mengirim dan menerima data pada media fisik transmisi yang digunakan.

2.9 *Domain Name Server* (DNS)

Untuk mengidentifikasi suatu entitas, protokol TCP/IP menggunakan alamat IP. Namun apabila dalam aplikasi setiap orang harus menghafal alamat IP untuk melakukan komunikasi bisa berakibat timbulnya kesulitan untuk mengingat. Apalagi jika perkembangan internet sudah demikian pesat. Untuk itu protokol TCP/IP memiliki suatu metode untuk membuat suatu map yang menterjemahkan nama kepada alamat IP atau sebaliknya. Metode ini disebut juga sebagai *Domain Name System* (DNS).

Domain Name System (DNS) adalah distribute database system yang digunakan untuk pencarian nama komputer (*name resolution*) di jaringan yang mengunakan TCP/IP (*Transmission Control Protocol/Internet Protocol*). DNS biasa digunakan pada aplikasi yang terhubung ke Internet seperti web browser atau e-mail, dimana DNS membantu memetakan host name sebuah komputer ke IP address. Selain digunakan di Internet, DNS juga dapat di implementasikan ke private network atau intranet dimana DNS memiliki keunggulan seperti [5]

1. Mudah, DNS sangat mudah karena user tidak lagi direpotkan untuk mengingat IP address sebuah komputer cukup host name (nama Komputer).
2. Konsisten, IP address sebuah komputer bisa berubah tapi host name tidak berubah.
3. Simpel, user hanya menggunakan satu nama domain untuk mencari baik di Internet maupun di Intranet.

2.10 *Internet Protocol Version* 4 (IPv4)

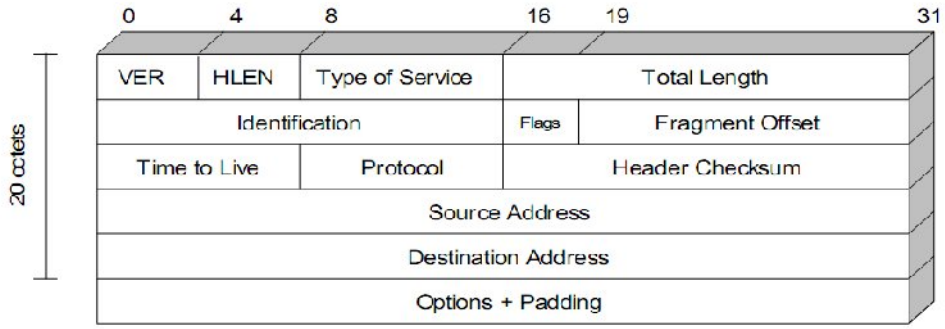
IP merupakan suatu mekanisme transmisi yang digunakan oleh protokol-protokol TCP/IP, dimana IP bersifat *unreliable, connectionless* dan *datagram delivery service*.

Unreliable berarti bahwa protokol IP tidak menjamin datagram (Paket yang terdapat di dalam IP *layer*) yang dikirim pasti sampai ke tempat tujuan. Protokol IP hanya berusaha sebaik-baiknya agar paket yang dikirim tersebut sampai ke tujuan. Jika dalam perjalanan, paket tersebut mengalami gangguan seperti jalur putus, kongesti pada *router* atau target *host down*, protokol IP hanya bisa menginformasikan kepada pengirim paket melalui protokol ICMP bahwa terjadi masalah dalam pengiriman paket IP. Jika diinginkan keandalan yang lebih baik, keandalan itu harus disediakan oleh protokol yang berada di atas IP *layer* misalnya TCP dan aplikasi pengguna.

Connectionless berarti bahwa dalam mengirim paket dari tempat asal ke tujuan, baik pihak pengirim dan penerima paket IP sama sekali tidak mengadakan perjanjian terlebih dahulu (*handshake*).

Datagram delivery service berarti bahwa setiap paket yang dikirimkan tidak tergantung pada paket data yang lain. Akibatnya jalur yang ditempuh oleh masing-mading paket data bisa jadi berbeda satu dengan yang lainnya.

Pada saat ini secara umum *internet* masih menggunakan IP *version* 4, dimana pemakaiannya sudah semakin terbatas mengingat jumlah pengguna internet yang berkembang dengan cepat. Hal ini disebabkan oleh panjang alamat yang dimiliki IPv4 yaitu 32 bit. Pada gambar di bawah ini ditunjukkan format *header* dari IPv4.



Gambar 2.25 IPv4 *Header*

Informasi yang terdapat pada *header* IP :

1. *Version* (VER), berisi tentang versi protokol IP yang dipakai.
2. *Header Length* (HLEN), berisi panjang *header* IP bernilai 32 bit.
3. *Type of Service* (TOS), berisi kualitas *service* cara penanganan paket IP.
4. *Total Length of Datagram*, total panjang datagram IP dalam ukuran *byte*.

5. *Identification*, *Flags*, dan *Fragment Offset*, berisi tentang data yang berhubungan dengan fragmentasi paket.
6. *Time to Live* (TTL), berisi jumlah *router/hop* maksimal yang boleh dilewati paket IP. Setiap kali paket IP melewati *router*, isi *field* akan dikurangi satu. Jika TTL telah habis dan paket belum sampai ke tujuan, paket akan dibuang dan *router* terakhir akan mengirimkan paket ICMP *time exceeded*.
7. *Protocol*, berisi angka yang mengidentifikasikan protokol *layer* atas, yang menggunakan isi data dari paket IP ini.
8. *Header Checksum*, berisi nilai *checksum* yang dihitung dari seluruh *field* dari *header* paket IP. Sebelum dikirimkan, protokol IP terlebih dahulu menghitung *checksum* dari *header* paket IP tersebut untuk nantinya dihitung kembali di sisi penerima. Jika terjadi perbedaan maka paket dianggap rusak dan dibuang.
9. *Source IP Address*, alamat asal/sumber.
10. *Destination IP Address*, alamat tujuan.
11. *Option*, mengkodekan pilihan-pilihan yang diminta oleh pengirim seperti *security label*, *source routing*, *record routing*, dan *time stamping*.
12. *Padding*, digunakan untuk meyakinkan bahwa *header* paket bernilai kelipatan dari 32 bit.

2.11 Kelas-kelas IP address

IP address dibagi menjadi lima kelas, A sampai E. IP address yang dipakai secara umum dibagi dalam 3 kelas, sementara 2 kelas lainnya dipakai untuk kepentingan khusus. Ini untuk memudahkan pendistribusian IP address ke seluruh dunia.

1. Kelas A

Karakteristik :

a. Format : 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

b. Bit pertama : 0

c. Panjang Network ID : 8 bit

d. Panjang Host ID : 24 bit

e. Byte pertama : 0 – 127

f. Jumlah : 126 kelas A (0 dan 127 dicadangkan)

g. Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx

h. Jumlah IP : 16.777.214 IP address pada tiap kelas A

IP address kelas ini diberikan kepada suatu jaringan yang berukuran sangat besar, yang pada tiap jaringannya terdapat sekitar 16 juta host.

2. Kelas B

Karakteristik :

a. Format : 10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

b. 2 bit pertama : 10

c. Panjang Network ID : 16 bit

d. Panjang Host ID : 16 bit

e. Byte pertama : 128 – 191

f. Jumlah : 16.384 kelas B

g. Range IP : 128.0.xxx.xxx sampai 191.155.xxx.xxx

h. Jumlah IP : 65.535 IP address pada tiap kelas B

IP address kelas ini diberikan kepada jaringan dengan ukuran sedang-besar.

3. Kelas C

Karakteristik :

a. Format : 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

b. Bit pertama : 110

c. Panjang Network ID : 24 bit

d. Panjang Host ID : 8 bit

e. Byte pertama : 192 – 223

f. Jumlah : 2.097.152 kelas C

g. Range IP : 192.0.0.xxx sampai 223.255.255.xxx

h. Jumlah IP : 254 IP address pada tiap kelas C

IP kelas ini dialokasikan untuk jaringan berukuran kecil.

4. Kelas D

Karakteristik :

a. Format : 1110mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm

b. 4 bit pertama : 1110

c. Bit Multicast : 28 bit

d. Byte Inisial : 8 bit

e. Byte pertama : 224-247

f. Deskripsi : Kelas D adalah ruang alamat Multicast (RFC 1112)

IP kelas D digunakan sebagai alamat multicast yaitu sejumlah komputer memakai bersama suatu aplikasi. 4 bit pertama IP address kelas D di set 1110. Dalam multicasting tidak dikenal network bit dan host bit.

5. Kelas E

Karakteristik :

a. Format : 1111rrrr.rrrrrrrr.rrrrrrrr.rrrrrrrr

b. 4 bit pertama : 1111

c. Bit Multicast : 28 bit

d. Byte Inisial : 248-255

e. Deskripsi : Kelas E adalah ruang alamat untuk keperluan eksperimental.

IP address kelas E tidak digunakan untuk umum. 4 bit pertama IP address ini di set 1111.

2.12 *Subnetting*

Konsep *subnetting* dari IP address merupakan teknik yang umum digunakan di internet untuk mengefisiensikan alokasi IP address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP address.

Untuk beberapa alasan yang menyangkut efisiensi IP address, mengatasi masalah topologi *network* dan organisasi, *network* administrator biasanya melakukan *subnetting*. Esensi dari *subnetting* adalah "memindahkan" garis pemisah antara bagian *network* dan bagian host dari suatu IP address. Beberapa bit dari bagian host dialokasikan menjadi bit tambahan pada bagian *network*. Address suatu *network* menurut struktur baku dipecah menjadi beberapa sub- network. Cara ini menciptakan sejumlah *network* tambahan dengan mengurangi jumlah maksimum *host* yang ada dalam tiap *network* tersebut.

Jadi intinya, *Subnetting* adalah metode untuk membagi suatu network yang besar menjadi sub network-sub *network* yang lebih kecil, dengan cara mengorbankan sebagian host ID atau dengan cara meminjam bagian dari IP Address yang merupakan bagian host menjadi bagian network, agar bisa digunakan untuk membuat *network* ID tambahan.

Tujuan lain yang tidak kalah pentinganya dari subnetting adalah untuk mengurangi tingkat kongesti dalam suatu *network*. Untuk menghindari terjadinya kongesti akibat terlalu banyak host dalam suatu *physical network,* dilakukan segmentasi jaringan.

2.13 *Virtual Private Network* (VPN)

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.

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.

2.13.1 Fungsi Utama Teknologi 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 Intergrity* (Keutuhan Data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

3. *Origin Authentication* (Autentikasi Sumber)

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

2.13.2 Teknologi VPN

VPN merupakan perpaduan dari teknologi tunneling dengan teknologi enkripsi.

2.13.2.1 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 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.

2.13.2.2 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.

2.13.3 Jenis implementasi VPN

Didalam implementasinya VPN dibagi menjadi dua jenis yaitu *remote access* VPN dan s*ite-to-site* VPN :

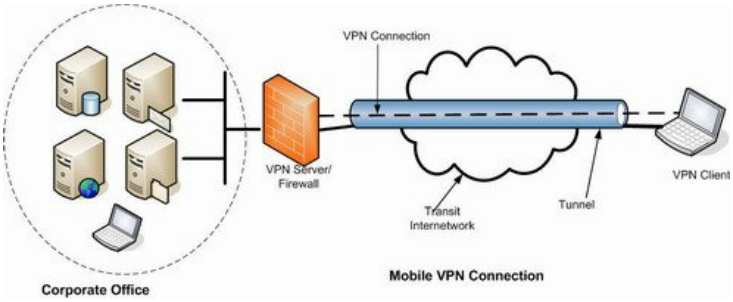
2.13.3.1 *Remote Access* VPN

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.

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.

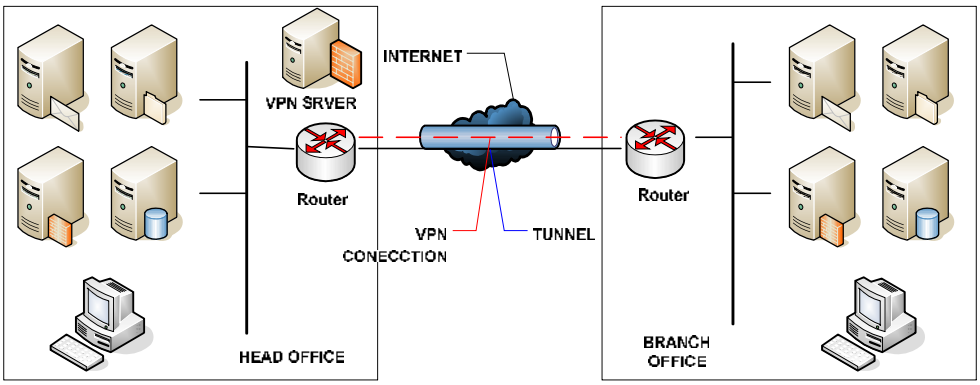
Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.



Gambar 2.26 *Remote Access* VPN

2.13.3.2 *Site-to*-site VPN

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 2.27 *Site-to-site* VPN

2.13.4 Protokol pada VPN

Terdapat lima protokol yang hingga saat ini paling banyak digunakan untuk VPN. Kelima protokol tersebut antara lain sebagai berikut.

1. *Point to Point Tunneling Protocol* (PPTP)
2. *Layer 2 Tunneling Protocol* (L2TP)
3. SOCKS
4. *Cryptographic IP Encapsulation* (CIPE)
5. *Generic Routing Encapsulation* (GRE)
6. *Internet Protocol Securuty* (IPSec)

Protokol-protokol di atas menekankan pada authentikasi dan enkripsi dalam VPN. Adanya sistem authentikasi akan mengijinkan klien dan *server* untuk menempatkan identitas orang yang berbeda di dalam jaringan secara benar. Enkripsi mengijinkan data yang dikirim dan diterima tersembunyi dari publik saat melewati jaringan publik.

2.13.4.1 *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 *internet*. PPTP juga dapat digunakan pada jaringan private LAN-to-LAN.

PPTP terdapat sejak dalam sistem operasi Windows NT server dan Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol PPTP dengan aman untuk terhubung dengan *private network* sebagai *klien* dengan *remote access* melalui internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya *public-switched telephone network* (PSTNs) untuk membangun VPN. Pembangunan PPTP yang 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.

Umumnya terdapat tiga komputer yang diperlukan untuk membangun PPTP, yaitu sebagai berikut.

1. Klien PPTP
2. *Network access server* (NAS)
3. *Server* PPTP

Akan tetapi tidak diperlukan *network access server* dalam membuat PPTP tunnel saat menggunakan klien PPTP yang terhubung dengan LAN untuk dapat terhubung dengan *server* PPTP yang terhubung pada LAN yang sama.

2.13.4.2 *Layer 2 Tunneling Protocol* (L2TP)

L2TP adalah *tunneling protocol* yang memadukan dua buah *tunneling protokol* yaitu L2F (Layer 2 Forwarding) milik cisco dan PPTP milik Microsoft. L2TP biasa digunakan dalam membuat *Virtual Private Dial Network* (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. Umunnya L2TP menggunakan port 1702 dengan protocol UDP untuk mengirimkan L2TP *encapsulated* PPP frames sebagai data yang di tunnel.

Terdapat dua model tunnel yang dikenal, yaitu *compulsory* dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint* tunnel-nya. Pada *compulsory tunnel*, ujung *tunnel* berada pada ISP, sedangkan pada voluntary ujung tunnel berada pada *client remote*. L2TP murni hanya membentuk jaringan *tunnel*, oleh karena itu L2TP sering dikombinasi dengan IPSec sebagai metode enkripsi.

2.13.4.3 SOCKS

SOCKS adalah suatu protokol proxy untuk lingkungan *client/server*. SOCKS meliputi dua komponen utama, yaitu *library server* SOCKS dan *client* SOCKS. Implementasi *server* SOCKS dilakukan pada layer application dan library client

SOCKS terletak di antara layer aplikasi *client* dan layer transport . Saat ini ada dua versi protokol SOCKS, yaitu SOCKS versi 4 dan SOCKS versi 5.

2.13.4.4 *Crypthography Ip Encapsulation* (CIPE)

CIPE adalah merupakan suatu paket dalam enkripsi IP *tunnel device*. Dimana dapat dipergunakan untuk membangun suatu enkripsi router untuk VPN (*Virtual Private Network*) dan aplikasi lain yang sejenis.

CIPE menggunakan algoritma *cryptographic Blowfish* Dan *IDEA* dengan panjang 128 bit (seperti kebanyakan aplikasi cryptographic umum lainnya, e.g. SSL). Protokol secara khusus dirancang serta didokumentasikan secara terbuka sehingga dapat mengalami peningkatkan didasarkan masukan serta tinjauan ulang dari kalayak umum. Hal ini dipercaya sebagai hal yang paling menjamin atau aman didalam pendekatan pengembangan *cryptographi protocol*.

2.13.4.5 *Generic Routing Encapsulation* (GRE)

GRE memiliki kemampuan membawa lebih dari satu jenis protokol pengalamatan komunikasi. Bukan hanya paket beralamat IP saja yang dapat dibawanya, melainkan banyak paket protokol lain seperti CNLP, IPX, dan banyak lagi. Namun, semua itu dibungkus atau dienkapsulasi menjadi sebuah paket yang bersistem pengalamatan IP. Kemudian paket tersebut didistribusikan melalui sistem *tunnel* yang juga bekerja di atas protokol komunikasi IP.

Dengan menggunakan tunneling GRE, router yang ada pada ujung-ujung *tunnel* melakukan enkapsulasi paket-paket protokol lain di dalam header dari protokol IP. Hal ini akan membuat paket-paket tadi dapat dibawa ke manapun dengan cara dan metode yang terdapat pada teknologi IP. Dengan adanya kemampuan ini, maka protokol-protokol yang dibawa oleh paket IP tersebut dapat lebih bebas bergerak ke manapun lokasi yang dituju, asalkan terjangkau secara pengalamatan IP.

Aplikasi yang cukup banyak menggunakan bantuan protokol tunneling ini adalah menggabungkan jaringan-jaringan lokal yang terpisah secara jarak kembali dapat berkomunikasi. Atau dengan kata lain, GRE banyak digunakan untuk memperpanjang dan mengekspansi jaringan lokal yang dimiliki si penggunanya. Meski cukup banyak digunakan, GRE juga tidak menyediakan sistem enkripsi data yang lalu-lalang di tunnel-nya, sehingga semua aktivitas datanya dapat dimonitor menggunakan *protocol analyzer*.

2.13.4.6 *Internet Protocol Security* (IPSec)

IPsec merupakan suatu set ektensi protokol dari *Internet Protocol* (IP) yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). IPSec didesain untuk menyediakan interoperabilitas, kualitas yang baik dan sekuriti berbasis kriptografi untuk IPv4 dan IPv6. layanan yang disediakan meliputi kontrol akses, integritas hubungan, otentifikasi data asal, proteksi jawaban lawan, kerahasiaan (enkripsi),

dan pembatasan aliran lalulintas kerahasiaan. Layanan ini tersedia dalam IP layer, memberi perlindungan pada IP dan layer protokol berikutnya

IPsec merupakan tunneling protokol yang bekerja pada layer 3. 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 menyediakan layanan-layanan keamanan tersebut dengan menggunakan sebuah metode pengamanan yang bernama *Internet Key Exchange* (IKE). IKE bertugas untuk menangani protokol yang bernegosiasi dan algoritma pengamanan yang diciptakan berdasarkan dari *policy* yang diterapkan. Dan pada akhirnya IKE akan menghasilkan sebuah system enkripsi dan kunci pengamanannya yang akan digunakan untuk otentikasi yang digunakan pada system IPSec ini.

IPSec bekerja dengan tiga cara, yaitu:

1. Network-to-network
2. Host-to-network
3. Host-to-host

Protokol yang berjalan dibelakang IPSec adalah:

1. AH (Authentication Header), menyediakan layanan authentication (menyatakan bahwa data yang dikirim berasal dari pengirim yang benar),

intregrity (keaslian data), dan replay protection (transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan), juga melakukan pengamanan terhadap IP header (header compression).

2. ESP (Encapsulated Security Payload), menyediakan layanan authentication, intregity, replay protection, dan confidentiality (keamanan terjaga) terhadap data. ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah header.

IPsec merupakan suatu set ektensi protokol dari *Internet Protocol* (IP) yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). Istilah dari IPsec mengacu pada suatu set dari mekanisme yang didesain untuk mengamankan trafik pada level IP atau pada *network layer*. Teknologi dari IPsec ini didasari oleh teknologi modern dari kriptografi, dimana layanan keamanan yang disediakan antara lain yaitu:

1. ***Confidentiality*** :

   Untuk mejamin kerahasiaan dimana sulit bagi pihak yang tidak berwenang untuk dapat melihat atau mengerti kecuali oleh penerima yang sah bahwa data telah dikirimkan.

2. ***Integrity*** :

   Untuk menjamin bahwa data tidak berubah dalam perjalanan menuju tujuan.

3. ***Authenticity*** :

   Untuk menjamin bahwa data yang dikirimkan memang berasal dari pengirim yang benar.

4. ***Anti Reply*** :

   Untuk menjamin bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengijinkan untuk mengulang transaksi.

2.14 Perangkat Lunak yang digunakan pada penelitian:

2.14.1 Mikrotik *Router Operatng System*

MikroTik RouterOS™ adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi *router network* yang handal, mencakup berbagai fitur yang dibuat untuk IP *Network* dan jaringan *wireless*, cocok digunakan oleh ISP dan provider hotspot.

2.14.2 Fitur – fitur Mikrotik Router OS

Adapun fitur-fitur daari mikrotik adalah sebagai berikut :

1. *Address list*

   Pengelompokan IP Addresss berdasarkan nama.

2. *Asynchronous*

   Mendukung serial PPP dial-in/dial-out, dengan autentifiasi CHAP, PAP,

MSCHAPv,1 dan MSCHAP v.2, radius, dial on demand, modem pool hingga 128 ports.

3. *Bonding*

   Mendukung dalam pengkombinasian beberapa antarmuka Ethernet ke dalam 1 pipa pada koneksi yang cepat.

4. *Bridge*

   Mendukung fungsi bridge spanning tree, multiple bridge interface, bridge firewalling.

5. *Data Rate Management*.

   Qos berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO quaeue, CIR, MIR, limit antar peer to peer.

6. DHCP *(Domain Host Configuration's Protocol).*

   Mendukung DHCP tiap antarmuka, DHCP Realy, DHCP Client, multiple network DHCP, static and dynamic DHCP leases.

7. Fierwall dan NAT.

   Mendukung pemfilteran koneksi peer to peer, source NAT, dan destination NAT. mampu memfilter berdasarkan MAC, IP Address, range port, protocol IP, pemilihan opsi protocol seperti, ICMP, TCPFlags, dan MSS.

8. Hotspot

   Hotspot Gateway dengan outentifikasi RADIUS. Mendukung limit data rate, SSL, HTTPS.

9. IPsec

   Protocol AH dan ESP untuk Ipsec. MOD differ-hellman groups 1, 2, 5, MD5 dan Algoritma SHA1 hashing, algoritma enkripsi menggunakan DES, 3DES, AES-128, AES-192, AES-128K. perfect Forwarding Secresy (PFS) MODP group1,2,5.

10. ISDN *(Integrated Services Digital Network)*

    Mendukung ISDN Dial-in/Dial-out.

11. M3P *(Mikrotik Protokol packet Packer)*

    Mikrotik Protokol packet Packer untuk wireless links dan Ethernet.

12. MNDP *(Mikrotik Discovery Neighbor Protocol)*.

    Mikrotik Discovery Neighbor Protocol, juga mendukung Cisco Discovery Protokol (CDP).

13. Monitoring / Accounting.

    Laporan traffic IP, log, statistic graphs yang dapat diakses melalui HTTP.

14. NTP *(Network Time Protocol)*.

    Network Time Protocol untuk server dan client. Singkronisasi menggunakan system GPS.

15. *Point to Point tunneling Protocol*.

    PPTP, PPPoE dan L2TP Access Concentrators.

16. Proxy.

    Cache untuk FTP dan HTTPproxy server,HTTPS proxy, transparent proxy untuk DNS dan HTTP, mendukung protocol SOKCS, mendukung parent proxy, static DNS.

16. Routing.

    Routing static dan dinamik.

17. SDSL (single line DSL).

    Mendukung single line DSL, mode pemutusan jalur koneksi dan jaringan.

18. Simple Tunnels.

    Tunnel IPIP dan EoIP (Ethernet Over IP)

19. SNMP *(Simple Network Management Protocol)*.

    Mode akses read-only

21. *Synchronous*

22. *Tool*

    Ping, traceroute, bandwith test, ping flood, telnet, SSH, packet sniffer, dinamik DNS Update.

23. UPnP *(universal Plug n Play)*.

    Mendukung antarmuka universal Plug n Play

24. VLAN *(Virtual Local Area Network)*.

    Mendukung Virtual LAN IEEE802.1q untuk jaringan Ethernet dan wireless multiple VLAN, VLAN bridge.

25. VOIP *(voice over IP)*.

    Mendukunbg aplikasi voice over IP.

26. VRRP *(Virtual Router Redudant Protocol)*.

    Mendukung Virtual Router Redudant Protocol

27. WinBox.

    Aplikasi mode GUI untuk meremote dan mengkonfigurasi Mikrotik Router OS.

2.15 *Network Protocol Analyzer* (Wireshark -win 32- 1.2.9)

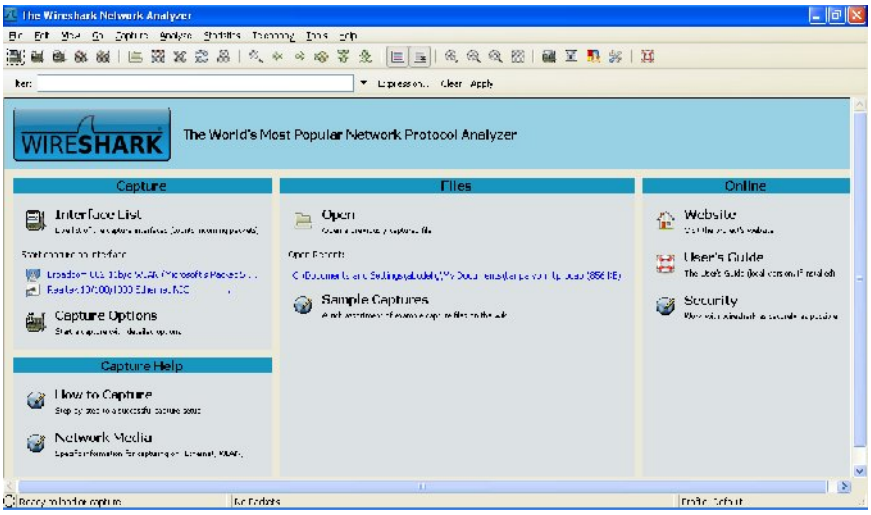
Wireshark adalah *tool* atau program yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan *Graphical User Interface* (GUI) atau tampilan grafis.

Wireshark mampu menangkap paket-paket data atau informasi yang berjalan dalam jaringan yang kita monitor. Semua jenis paket informasi dalam berbagai

format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang *tool* ini juga dapat dipakai untuk *sniffing* (memperoleh informasi penting seperti *password* email atau *account* lain) dengan menangkap paket-paket yang berjalan di dalam jaringan dan menganalisanya.

Wireshark merupakan sebuah *tool* yang cukup mudah dalam penggunaanya. Kita cukup memasukkan perintah untuk mendapatkan informasi yang ingin kita *capture* (yang ingin diperoleh) dari jaringan kita.

Berikut tampilan interface Wireshark dan Dialog Capture Option:



Gambar 2.28 Tampilan *interface* Wireshark

2.16 RaidenDNSD 1.3 RTM

RaidenDNSD adalah sebuah perangkat lunak yang berfungsi sebagai DNS *server* untuk sistem operasi windows. Adapun beberapa fitur yang dimiliki raidenDNSD adalah :

1. RM :

   Memungkinkan pengguna melakukan *remote* atau kontrol dan mengelola RaidenDNSD.

2. DNSD:

   Menyediakan klien AP untuk pengguna, sehingga pengguna dapat dengan mudah melakukan *update* IP yang dinamis

3. Wizard:

   Wizard memungkinkan pengguna untuk dapat mengetahui daftar domain dengan mudah

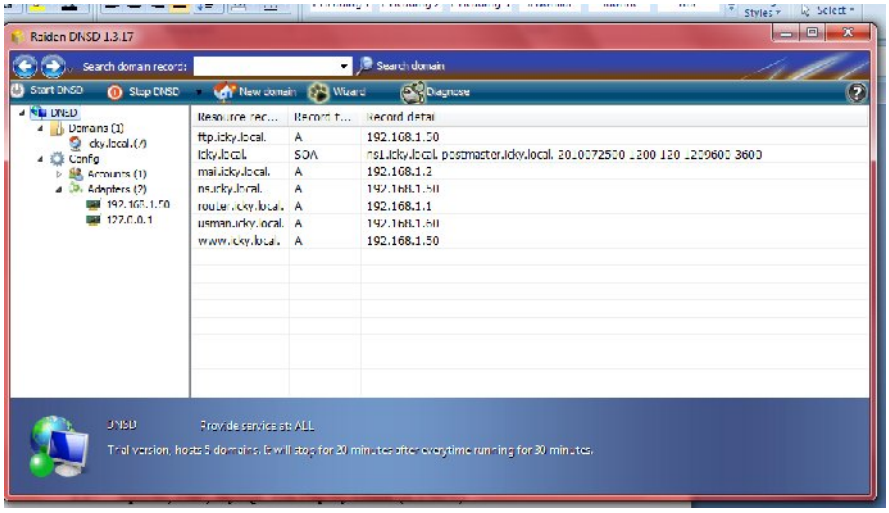
4. Security :

   Melindungi dari *DOS attact*

Kelebihan RaidenDNSD :

1. Performa tinggi
2. Stabil
3. Aman
4. Mudah digunakan

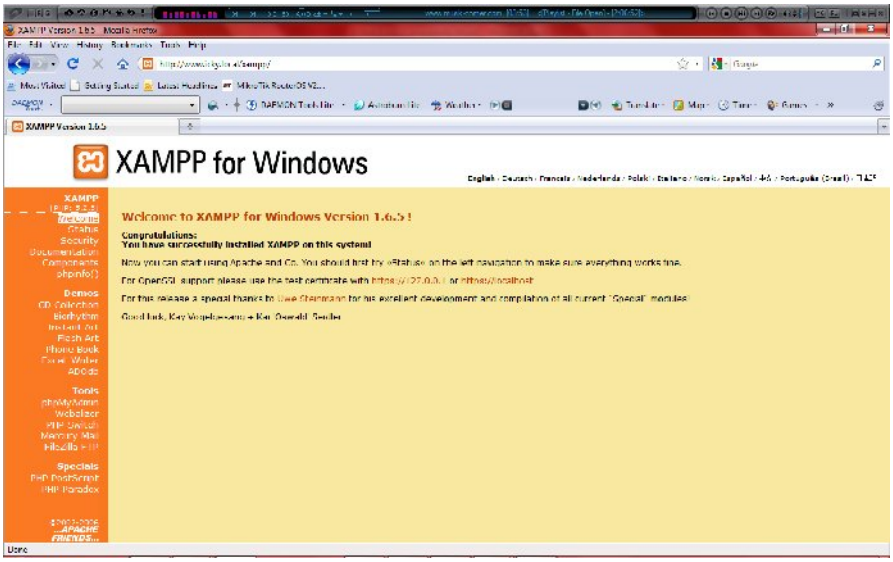
Dibawah ini adalah *screen shoot* dari RaidenDNSD



Gambar 2.29 Tampilan *interface* RaidenDNSD

2.17 Apache, PHP, MySQL dan PhpMyAdmin (XAMPP)

XAMPP merupakan kepanjangan dari Apache, PHP, MySQL dan phpMyAdmin. XAMPP merupakan tool yang menyediakan paket perangkat lunak ke dalam satu buah paket. Dengan menginstall XAMPP maka tidak perlu lagi melakukan instalasi dan konfigurasi web server Apache, PHP dan MySQL secara manual. XAMPP akan menginstalasi dan mengkonfigurasikannya secara otomatis untuk anda atau auto konfigurasi. Kelebihan XAMPP adalah Kelebihan XAMPP adalah multi platform Berjalan di Windows OS, Linux, Mac X OS, dan Solaris.



Gambar 2.30 Tampilan *interface* XAMPP

2.18 Filezilla

FileZilla atau juga dikenal dengan sebutan **FileZilla Client**, adalah salah satu software FTP yang bersifat *free*, *open source* dan *cross-platform.*

Fitur utama dari Filezilla adalah :

a. ***Site manager*** (Manajer fitur).

   Mengizinkan pengguna untuk membuat daftar situs FTP beserta data koneksinya, seperti nomor port yang akan difunakan, protokol yang digunakan, dan apakah akan menggunakan log anonim atau normal. Untuk log normal, nama pengguna dan kata sandinya tersebut akan disimpan. Penimpanan kata sandi adalah opsional.

b. ***Message log*** (Log pesan)

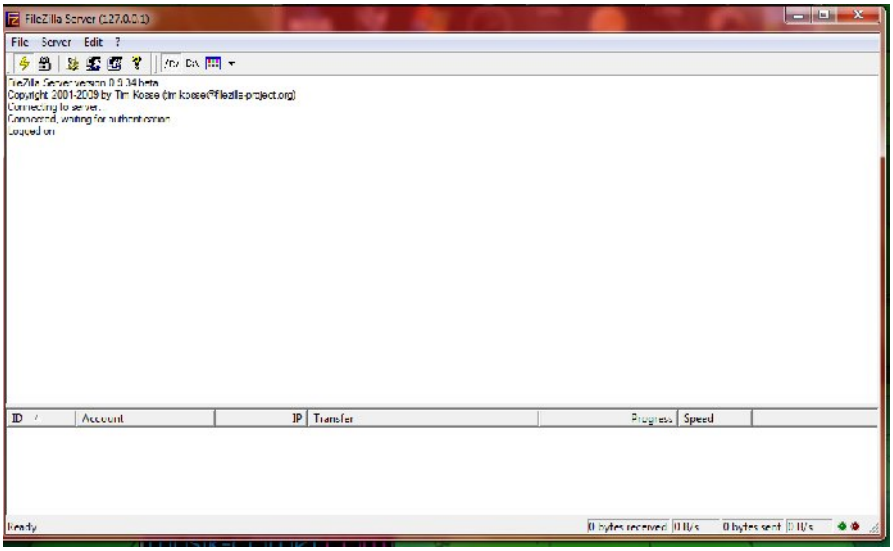
Fitur ini menampilkan output berjenis konsol (*console-type*) yang menunjukkan perintah yang dikirim oleh FileZilla dan respons yang diterima dari server.

c. ***File and folder view***

Ditampilkan di bawah pesan log (Message log), menyediakan sebuah tampilan grafis antarmuka untuk FTP. Pengguna dapat menavigasi folder dan melihat dan mengubah isinya pada komputer lokal dan server dengan menggunakan tampilan antarmuka gaya Explorer. Pengguna dapat men-*drag dan drop* file antara komputer lokal dan server.

d. ***Transfer queue*** (Transfer antrian)

Ditampilkan di sepanjang bagian bawah jendela, menunjukkan status *real-time* setiap antrian atau transfer file yang aktif.



Gambar 2.31 Tampilan *interface* Filezilla