BAB III

LANDASAN TEORI

3.1 Konsep Dasar Jaringan Komputer

Menurut Iwan Sofana (2008:12) definisi jaringan komputer adalah sekelompok komputer yang saling dihubungkan dengan menggunakan suatu protokol komunikasi sehingga antara satu komputer dengan komputer yang lainnya dapat berbagi data atau berbagi sumber daya (*sharing resource)*, saling bertukar informasi, program-program dan berkomunikasi melalui media jaringan tersebut.

Sistem pemasangan jaringan dapat dibedakan menjadi dua macam, yaitu:

1. Jaringan Terpusat

   Adalah jaringan yang terdiri dari beberapa *node* (*workstation*) yang terhubung dengan sebuah komputer pusat atau disebut *server*. Pada jaringan ini sistem kerja *workstation* tergantung dari komputer pusat. Dan komputer pusat tugasnya melayani permintaan akses dari *workstation*.

2. Jaringan Peer-to-Peer

   Adalah jaringan yang terdiri dari beberapa komputer yang saling berhubungan antara satu dengan lainnya tanpa komputer pusat (*server base*). Pada masing-masing komputer *workstation* terdapat media penyimpanan (*harddisk*) yang berfugsi sebagai *server* individu.

Secara umum jaringan komputer terdiri atas lima jenis yaitu:

a. Local Area Network (LAN)

Merupakan jaringan komputer yang jaringannya hanya mencakup wilayah kecil, seperti jaringan komputer kampus, kantor, gedung, sekolah, dalam rumah, atau yang lebih kecil. Saat ini kebanyakan LAN berbasis pada teknologi IEEE 802.3 *ethernet* menggunakan perangkat *switch*, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s. Selain teknologi *ethernet*, saat ini teknologi 802.11b (atau biasa disebut *Wi-fi*) juga sering digunakan untuk membentuk LAN. Tempat-tempat yang menyediakan koneksi LAN dengan teknologi *Wi-fi* biasa disebut *hotspot.* Pada sebuah LAN, setiap node atau komputer mempunyai daya komputasi sendiri, berbeda dengan konsep *dump terminal*. Setiap komputer juga dapat mengakses sumber daya yang ada di LAN sesuai dengan hak akses yang telah diatur. Sumber daya tersebut dapat berupa data atau perangkat seperti printer. Pada LAN, seorang pengguna juga dapat berkomunikasi dengan pengguna yang lain dengan menggunakan aplikasi yang sesuai.

b. Metropolitan Area Network (MAN)

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.

c. Wide Area Network (WAN)

Merupakan jaringan (network) komputer yang luas secara geografik. WAN adalah kumpulan dari LAN atau *workgroup* yang dihubungkan dengan menggunakan alat komunikasi modem dan jaringan internet, dari atau ke kantor pusat dan kantor cabang, maupun antar kantor cabang. Dengan sistem jaringan ini, pertukaran data antar kantor dapat dilakukan dengan cepat serta dengan biaya yang relatif murah. Sistem jaringan ini dapat menggunakan jaringan Internet yang sudah ada, untuk menghubungkan antara kantor pusat dan kantor cabang atau dengan PC *stand alone* atau *notebook* yang berada di lain kota ataupun Negara.

d. Internet

Internet berasal dari kata *interconnected-networking*. Internet merupakan jaringan global yang menghubungkan suatu jaringan (*network*) dengan jaringan lainnya di seluruh dunia. Media yang menghubungkan bisa berupa kabel, kanal satelit maupun frekuensi radio. Jaringan internet bekerja bekerja berdasarkan suatu protokol (aturan). TCP/IP yaitu Transmission Control Protocol Internet Protocol adalah protokol standar yang digunakan untuk menghubungkan jaringan-jaringan di dalam internet sehingga data dapat dikirim dari satu komputer ke komputer lainnya. Setiap komputer diberikan suatu nomor unik yang disebut dengan alamat IP.

e. Wireless (Jaringan Tanpa Kabel)

Definisi jaringan nirkabel atau jaringan *wireless* pada prinsipnya sama dengan jaringan komputer biasa menggunakan kabel. Yang membedakan antara keduanya hanyalah media yang digunakan. Jaringan *nirkabel* atau *wireless* menggunakan media udara (gelombang radio) sebagai jalur lintas data. Ada beberapa hal yang mendorong terjadinya pengembangan teknologi *wireless* untuk komputer, antara lain :

a) Munculnya perangkat-perangkat berbasis gelombang radio, seperti *walki talkie, remote control, handpone, gadget,* dan peralatan radio lainnya yang menandai dimulainya proses komunikasi tanpa kabel ini.
b) Adanya kebutuhan untuk menjadikan komputer sebagai barang yang mudah dibawa (mobile) dan mudah dihubungkan dengan jaringan yang sudah ada.

3.2 Firewall

Firewall merupakan suatu cara atau sistem yang diterapkan baik terhadap *hardware, software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan atau kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation, server, router,* atau *local area network* (LAN).

Firewall secara umum di peruntukkan untuk melayani :

1. Mesin / komputer

Setiap individu yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.

2. Jaringan

Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang dimiliki oleh perusahaan, organisasi dsb. (Irzam, 2004).

3.2.1 Karakteristik Firewall

Karakteristik *firewall* dibagi menjadi 3, yaitu:

1. Seluruh hubungan atau kegiatan dari dalam ke luar , harus melewati *firewall*. Hal ini dapat dilakukan dengan cara memblok atau membatasi baik secara fisik semua akses terhadap jaringan lokal, kecuali melewati *firewall*. Banyak sekali bentuk jaringan yang memungkinkan.
2. Hanya kegiatan yang terdaftar atau dikenal yang dapat melewati atau melakukan hubungan, hal ini dapat dilakukan dengan mengatur *policy* pada konfigurasi keamanan lokal. Banyak sekali jenis *firewall* yang dapat dipilih sekaligus berbagai jenis *policy* yang ditawarkan.
3. Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan atau kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan *operating system* yang relatif aman. (Irzam, 2004).

3.2.2 Teknik Yang Digunakan Firewall

Teknik-teknik yang digunakan *firewall* ada 4, yaitu:

1. Service control (kendali terhadap layanan)

   Berdasarkan jenis-jenis layanan yang digunakan di internet dan boleh diakses baik untuk kedalam ataupun keluar *firewall*. Biasanya *firewall* akan memeriksa nomor *IP Address* dan juga nomor *port* yang digunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi *software* untuk *proxy* yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya. Bahkan bisa jadi *software* pada *server* itu sendiri, seperti layanan untuk *web* ataupun untuk *mail*.

2. Direction Conrol (kendali terhadap arah)

   Berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati *firewall.*

3. User control (kendali terhadap pengguna)

   Berdasarkan pengguna atau *user* untuk dapat menjalankan suatu layanan, artinya ada *user* yang dapat dan ada yang tidak dapat menjalankan suatu servis, hal ini di karenakan *user* tersebut tidak diijinkan untuk melewati *firewall*. Biasanya digunakan untuk membatasi *user* dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

4. Behavior Control (kendali terhadap perlakuan)

   Berdasarkan seberapa banyak layanan itu telah digunakan. Misal, *firewall* dapat memfilter email untuk menanggulangi atau mencegah *spam*. (Irzam, 2004).

3.2.3 Jenis-Jenis Firewall

Jenis-jenis *firewall* ada 3, yaitu:

1. Packet Filtering Router

   Packet Filtering diaplikasikan dengan cara mengatur semua *packet* IP baik yang menuju, melewati atau akan dituju oleh packet tersebut. Pada jenis ini packet tersebut akan diatur apakah akan diterima dan diteruskan, atau di tolak. Penyaringan *packet* ini di konfigurasikan untuk menyaring *packet* yang akan di transfer secara dua arah (baik dari atau ke jaringan lokal). Aturan penyaringan didasarkan pada *header* IP dan *transport header*, termasuk juga alamat awal (IP) dan alamat tujuan (IP), protokol transport yang digunakan (UDP,TCP), serta nomor *port* yang digunakan.

   Kelebihan dari jenis ini adalah mudah untuk diimplementasikan, transparan untuk pemakai, lebih cepat. Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi.

   Adapun serangan yang dapat terjadi pada firewall dengan jenis ini adalah:

   a. IP *address spoofing* : intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan atau menggunakan *ip address* jaringan lokal yang telah diijinkan untuk melalui *firewall*.
   b. *Source routing attacks* : jenis ini tidak menganalisa informasi *routing* sumber IP, sehingga memungkinkan untuk mem-*bypass firewall.*
   c. *Tiny Fragment attacks* : intruder (penyusup) membagi IP kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP *header*. Serangan jenis ini di *design* untuk menipu aturan

penyaringan yang bergantung kepada informasi dari TCP *header*. Penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protokol TCP dan memiliki *offset* sama dengan 1 pada IP *fragment* (bagian IP).

2. Application-Level Gateway

Application-level Gateway yang biasa juga di kenal sebagai *proxy server* yang berfungsi untuk memperkuat atau menyalurkan arus aplikasi. Jenis ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu ftp, http, gopher dll. Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal ftp untuk mengakses secara *remote*, maka *gateway* akan meminta user memasukkan alamat *remote host* yang akan di akses. Saat pengguna mengirimkan *user ID* serta informasi lainnya yang sesuai maka *gateway* akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada *remote host*, dan menyalurkan data diantara kedua titik. Apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada jenis ini *firewall* dapat di konfigurasikan untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati *firewall.*

Kelebihannya adalah relatif lebih aman daripada jenis *packet filtering router* lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi. Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. Yang akan mengakibatkan

terdapat dua buah sambungan koneksi antara pemakai dan *gateway*, dimana *gateway* akan memeriksa dan meneruskan semua arus dari dua arah.

3. Circuit-level Gateway

Jenis ketiga ini dapat merupakan sistem yang berdiri sendiri , atau juga dapat merupakan fungsi khusus yang terbentuk dari jenis *application-level gateway*. Jenis ini tidak mengijinkan koneksi TCP *end to end* (langsung). Cara kerjanya yaitu: gateway akan mengatur kedua hubungan TCP tersebut, 1 antara dirinya dengan TCP pada pengguna lokal (inner host), serta 1 lagi antara dirinya dengan TCP pengguna luar (outside host). Saat dua buah hubungan terlaksana, *gateway* akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang diijinkan. Penggunaan jenis ini biasanya dikarenakan administrator percaya dengan pengguna internal (internal users). (Irzam, 2004).

3.3 Linux

Linux adalah sistem operasi yang menyerupai sistem operasi Unix. Unix pada waktu itu adalah sistem operasi yang tangguh dan biasa digunakan oleh komputer *mainframe* sebagai *server*.

Pada sekitar pertengahan 1991, seorang mahasiswa universitas Finlandia bernama Linus Bennedict Torvalds mengerjakan proyek hobi yakni mengotak-atik Minix, sebuah sistem operasi kecil turunan dari Unix yang kemudian diberi nama Linux. Linus kemudian menjadikan Linux sebagai piranti lunak yang bersifat Open Source. *Open Source* berarti setiap orang bisa melihat

kode suatu program, bebas mendistribusikan, serta bebas merubah atau menambah fitur dari program tersebut.

Pada awalnya, Linux banyak digunakan pada mode teks. Dalam artian setiap perintah harus kita ketikkan melalui terminal konsol. Kemudian para *developer* Linux ingin agar tampilan Linux lebih "manusiawi" dengan membuat antarmuka berbasiskan grafis (GUI). Maka muncullah banyak *window manager* seperti KDE, *Gnome, Xfce, Enlightenment,* dll yang kemudian memunculkan distribusi linux cantik seperti *Mandriva, Redhat, Suse,* dan *Knoppix.*

Pada Linux kita mengenal istilah Distro. Distro adalah istilah untuk menyebut distribusi Linux. Karena sifatnya yang bebas dan kodenya yang terbuka, hal itu memungkinkan seseorang, komunitas pengembang, atau perusahaan membuat Linux versi mereka sendiri.

Sekalipun Linux juga suatu sistem operasi, tetapi Linux disertai dengan banyak program didalamnya. Setelah diinstal, anda akan menemui banyak program dari hampir semua kategori program. Sebut saja kategori *Office, Multimedia (Sound, Video, Graphics), Internet (Browser, Email, Chat, Message), Games, Utility (Burning Tools),* dll. Dengan waktu instalasi yang hampir sama, anda bukan hanya mendapatkan suatu sistem operasi tetapi juga semua program yang diperlukan untuk kegiatan sehari-hari di Linux. (Iwan, 2006).

3.3.1. IPCop Linux

IPCop Linux adalah distribusi Linux yang lengkap dengan fungsi khusus untuk pengamanan jaringan, IPCop sendiri adalah sebuah *stateful firewall* dibangun diatas *framework Linux netfilter*. Mulanya merupakan *fork* dari *SmoothWall Linux firewall* yang dikembangkan sebagai proyek terbuka secara

terpisah dibawah lisensi bebas GPL, didukung banyak pengembang diseluruh dunia dan menyediakan edisi untuk lebih dari 17 bahasa. IPCop menyertakan mekanisme yang simpel untuk mengelola dan menginstalasi *security updates* kapan saja bila dibutuhkan pengguna.

Tersedia banyak komponen tambahan (addons), walaupun ia tidak terkait secara resmi dengan proyek *IPcop*, yang dapat menambahkan fungsionalitas dan kemampuan *IPCop* seperti: advanced *QoS*, *email virus checking*, *traffic summary*, *extended interfaces for controlling the proxy*, dan lainnya.

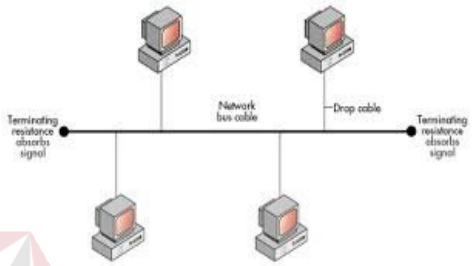
IPCop dapat digunakan seperti distribusi Linux lainnya bagi mereka yang serius ingin menjaga keamanan komputer dan jaringannya dengan penerapan teknologi yang ada bersama teknologi baru yang beorientasi pada 'secure programming', Tim *IPCop* Linux senantiasa siaga dan fokus mengembangkan software untuk meningkatkan sekuriti agar: "The Bad Packets Stop Here!". (Ali, 2010).

3.4 Topologi

Topologi menggambarkan struktur dari suatu jaringan atau bagaimana sebuah jaringan didesain. Dalam definisi topologi terbagi menjadi dua, yaitu topologi fisik (*physical topology*) yang menunjukan posisi pemasangan kabel secara fisik dan topologi logik (*logical topology*) yang menunjukan bagaimana suatu media diakses oleh *host*.

3.4.1. Topologi Bus

Topologi ini menggunakan satu *segment* (panjang kabel) *backbone*, yaitu yang menyambungkan semua host secara langsung. Apabila komunikasinya dua arah di sepanjang ring, maka jarak maksimum antara dua simpul pada ring dengan n simpul adalah n/2. Topologi ini cocok untuk jumlah prosesor yang relatif sedikit dengan komunikasi data minimal.



Gambar 3.1. Topologi Bus

Keuntungan Topologi Bus :

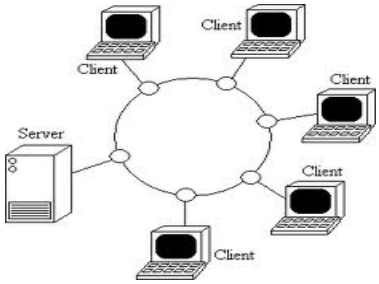
1. Hemat kabel.
2. Layout kabel sederhana.
3. Mudah dikembangkan.

Kerugian Topologi Bus :

1. Deteksi dan isolasi kesalahan sangat kecil.
2. Kepadatan lalu lintas.
3. Bila salah satu client rusak, maka jaringan tidak bisa berfungsi.
4. Diperlukan repeater untuk jarak jauh. (Rahmat, 2003).

3.4.2. Topologi Ring

Topologi ini menghubungkan satu *host* ke *host* setelah dan sebelumnya. Secara fisik jaringan ini berbentuk *ring* (lingkaran).



Gambar 3.2. Topologi Ring

Topologi ini juga merupakan topologi jaringan dimana setiap titik terkoneksi ke dua titik lainnya, membentuk jalur melingkar membentuk cincin. Pada topologi cincin, komunikasi data dapat terganggu jika satu titik mengalami gangguan. Jaringan FDDI mengantisipasi kelemahan ini dengan mengirim data searah jarum jam dan berlawanan dengan arah jarum jam secara bersamaan.

Keuntungan Topologi Ring :

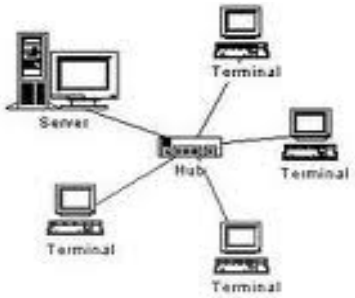
1. Hemat Kabel.
2. Tidak terjadi tabrakan saat pengiriman data.

Kerugian Topologi Ring :

1. Peka kesalahan.
2. Pengembangan jaringan lebih kaku. (Rahmat, 2003).

3.4.3. Topologi Star

Menghubungkan semua kabel pada *host* ke satu titik utama. Titik ini biasanya menggunakan *hub* atau s*witch*. Topologi bintang merupakan bentuk topologi jaringan yang berupa konvergensi dari *node* tengah ke setiap *node* atau pengguna. Topologi jaringan bintang termasuk topologi jaringan dengan biaya menengah.



Gambar 3.3. Topologi Star

Keuntungan Topologi Star :

1. Kerusakan pada satu saluran hanya akan mempengaruhi jaringan pada saluran tersebut dan *station* yang terpaut.
2. Tingkat keamanan termasuk tinggi.
3. Tahan terhadap lalu lintas jaringan yang sibuk.
4. Penambahan dan pengurangan *station* dapat dilakukan dengan mudah.

Kerugian Topologi Star :

1. Jika *node* tengah mengalami kerusakan, maka seluruh jaringan akan terhenti.
2. Penggunaan kabel terlalu boros. (Rahmat, 2003).

3.4.4. Faktor Pertimbangan Dalam Pemilihan Topologi

1. Biaya : Sistem apa yang paling efisien yang dibutuhkan dalam organisasi.
2. Kecepatan : Sampai sejauh mana kecepatan yang dibutuhkan dalam sistem.

3. Lingkungan : Misalnya listrik atau faktor–faktor lingkungan yang lain, yang berpengaruh pada jenis perangkat keras yang digunakan.
4. Ukuran : Sampai seberapa besar ukuran jaringan. Apakah jaringan memerlukan *file server* atau sejumlah *server* khusus.
5. Konektivitas ***:*** Apakah pemakai yang lain yang menggunakan komputer laptop perlu mengakses jaringan dari berbagai lokasi. (Rahmat, 2003).

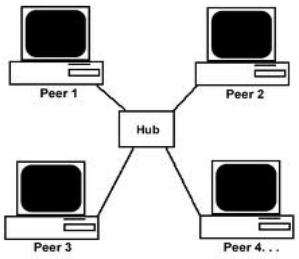
3.5 Jenis Jaringan

Secara garis besar jenis jaringan dibagi menjadi dua macam, yaitu jenis jaringan *Peer to peer* dan *Client-Server.*

3.5.1. Jaringan Peer To Peer

Pada jaringan jenis ini, setiap komputer yang terhubung dalam jaringan dapat saling berkomunikasi dengan komputer lainnya secara langsung tanpa perantara. Bukan hanya komunikasi langsung tetapi juga sumber daya komputer dapat digunakan oleh komputer lainnya tanpa ada pengendali dan pembagian hak akses.

Setiap komputer dalam jaringan *Peer to Peer* mampu berdiri sendiri sekalipun komputer yang tidak bekerja atau beroperasi. Masing-masing komputer tidak terikat dan tidak tergantung pada komputer yang lainnya. Komputer yang digunakanpun bias beragam dan tidak harus setara, karena fungsi komputer dan keamanannya diatur dan dikelola sendiri oleh masing-masing komputer.



Gambar 3.4. *Jaringan Peer to Peer*

Keunggulan Jaringan Peer to peer :

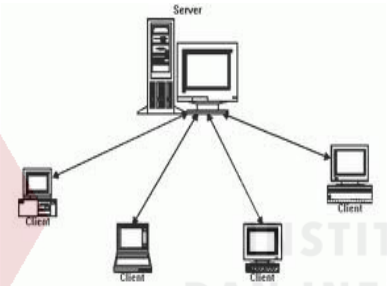
1. Antar komputer dalam jaringan dapat saling berbagi-pakai fasilitas yang dimilikinya seperti: *harddisk, drive, fax/modem, printer.*
2. Biaya operasional relatif lebih murah dibandingkan dengan jenis jaringan client-server, salah satunya karena tidak memerlukan adanya server yang memiliki kemampuan khusus untuk mengorganisasikan dan menyediakan fasilitas jaringan.
3. Kelangsungan kerja jaringan tidak tergantung pada satu server. Sehingga bila salah satu komputer/peer mati atau rusak, jaringan secara keseluruhan tidak akan mengalami gangguan.

Kelemahan Jaringan Peer to peer :

1. Troubleshooting jaringan relatif lebih sulit, karena pada jaringan jenis peer to peer setiap komputer dimungkinkan untuk terlibat dalam komunikasi yang ada. Di jaringan *client-server*, komunikasi adalah antara *server* dengan *workstation.*
2. Unjuk kerja lebih rendah dibandingkan dengan jaringan client- server, karena setiap komputer/peer disamping harus mengelola pemakaian fasilitas jaringan juga harus mengelola pekerjaan atau aplikasi sendiri.
3. Sistem keamanan jaringan ditentukan oleh masing-masing *user* dengan mengatur masing-masing fasilitas yang dimiliki. (Melwin, 2005).

3.5.2. Jaringan Client-Server

Sesuai dengan namanya, jaringan komputer jenis ini memerlikan sebuah (atau lebih) komputer yang difungsikan sebagai pusat pelayanan dala jaringan yang disebut *server.* Komputer-komputer lain disebut sebagai *Client* atau *Workstation.* Sesuai sebutannya , komputer *server* bertugas melayani semua kebutuhan komputer lain yang berada dalam jaringan. Semua fungsi jaringan dikendalikan dan diatur oleh komputer *server*, termasuk masalah keamanan jaringan seperti hak akses data, waktu akses, sumber daya dan sebagainya.



Gambar 3.5. *Jaringan Client-Server*

Keunggulan Jaringan *Client-Server* :

1. Memberikan keamanan yang lebih baik.
2. Lebih mudah pengaturannya bila networknya besar karena administrasinya disentralkan.
3. Semua data dapat di backup pada satu lokasi sentral.

Kelemahan Jaringan *Client-Server* :

1. Membutuhkan hardware yang lebih tinggi dan mahal untuk mesin server.
2. Mempunyai satu titik lemah jika menggunakan satu *server*, data *user* menjadi tak ada jika *server* mati. (Melwin, 2005).

3.6 Protokol Jaringan

Protokol adalah serangkaian aturan yang mengatur unit fungsional agar komunikasi bisa terlaksana. Misalnya mengirim pesan, data, dan informasi. Protokol juga berfungsi untuk memungkinkan dua atau lebih komputer dapat berkomunikasi dengan bahasa yang sama.

Secara umum fungsi dari protocol adalah untuk menghubungkan sisi pengirim dan penerima dalam berkomunikasi serta dalam bertukar informasi agar dapat berjalan dengan baik dan benar dengan kehandalan yang tinggi.
(Melwin, 2005).

3.7 IP Address

Alamat IP (Internet Protocol Address atau sering disingkat IP) adalah deretan angka biner antara 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host yang berada dalam jaringan internet. Panjang dari angka ini adalah 32-bit (untuk IP versi 4) dan 128-bit (untuk IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan internet berbasis TCP/IP. IP address yang terdiri dari bilangan biner 32-bit tersebut dipisahkan oleh tanda titik pada setiap 8 bitnya. Tiap 8 bit ini disebut sebagai oktet, bentuk IP address dapat dituliskan sebagai berikut: xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx jadi IP address ini mempunyai range dari 00000000.00000000.00000000.00000000. Sampai 11111111.11111111.11111111.11111111. Notasi IP address dengan bilangan seperti ini susah untuk digunakan, sehingga sering ditulis dalam 4 bilangan decimal yang masing-masing dipisahkan 4 buah titik yang lebih dikenal dengan

"notasi desimal bertitik". Setiap bilangan desimal merupakan nilai dari satu oktet IP address. Contoh hubungan suatu IP address dalam format biner dan desimal :

Tabel 3.1. Tabel Kelas IP address.

Desimal	167	205	206	100
Biner	10100111	11001101	11001110	01100100

3.7.1. Kelas-kelas IP address

IP address dapat dipisahkan menjadi 2 bagian , yakni bagian *network (net ID)* dan bagian *host (host ID). Net ID* berperan dalam identifikasi suatu *network* dari *network* yang lain, sedangkan *host ID* berperan untuk identifikasi *host* dalam suatu *network*.

1. Bit pertama IP address kelas A adalah 0, dengan panjang net ID 8 bit dan panjang host ID 24 bit. Jadi byte pertama IP address kelas A mempunyai range dari 0-127. Jadi pada kelas A terdapat 127 network dengan tiap network dapat menampung sekitar 16 juta host (255x255x255x255).
2. Dua bit IP address kelas B selalu diset 10 sehingga byte pertamanya selalu bernilai antara 128-191. Network ID adalah 16 bit pertama dan 16 bit sisanya adalah host ID sehingga kalau ada komputer mempunyai IP address 192.168.26.161, net ID = 192.168 dan host ID = 26.161. Pada IP address kelas B ini mempunyai range IP dari 128.0.xxx.xxx sampai 191.155.xxx.xxx yakni berjumlah 65.255 network dengan jumlah host tiap network 255x255 host atau sekitar 65 ribu host.
3. IP address kelas C mulanya digunakan untuk jaringan berukuran kecil seperti LAN. Tiga bit pertama IP address kelas C selalu diset 111. Network ID terdiri dari 24 bit dan host ID 8 bit sisanya sehingga dapat terbentuk sekitar 2 juta

network dengan masing-masing network memiliki 256 host. (www.gap.web.id, 2011).

3.8 Protokol TCP/IP

TCP/IP (Transmission Control Protokol/Internet Protocol) merupakan standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan internet. Protokol ini tidaklah dapat berdiri sendiri , karena memang protokol ini berupa kumpulan protokol **(**protocol suite**).** Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (s*oftware*) di sistem operasi. Istilah yang diberikan kepada peragkat lunak ini adalah TCP/IP *stack.*

Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). 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. Protokol ini juga bersifat *routable* yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga UNIX) untuk membentuk jaringan yang *heterogen*. (Melwin, 2005).

3.8.1 DNS (*Domain Name System*)

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:

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. Simple, *user* hanya menggunakan satu nama *domain* untuk mencari baik di *internet* maupun di *intranet*.

DNS dapat disamakan fungsinya dengan buku telepon. Dimana setiap komputer di jaringan internet memiliki *host name* (nama komputer) dan *internet Protocol* (IP) address. Secara umum, setiap client yang akan mengkoneksikan komputer yang satu ke komputer yang lain, akan menggunakan host name. Lalu komputer anda akan menghubungi DNS *server* untuk mencek *host name* yang anda minta tersebut berapa IP address-nya. IP address ini yang digunakan untuk mengkoneksikan komputer anda dengan komputer lainnya. (Melwin, 2005).

3.8.2. DHCP (*Dynamic Host Configuration Protocol*)

Dynamic Host Configuration Protocol (DCHP) adalah protokol yang berbasis arsitektur *client/server* yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara manual. Jika DHCP dipasang di jaringan lokal, maka semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari server DHCP. Selain alamat IP, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti *default gateway* dan *DNS server*. (Melwin, 2005).

3.8.3. Proxy Server

Proxy server adalah sebuah komputer *server* atau program komputer yang dapat bertindak sebagai komputer lainnya untuk melakukan *request* terhadap content dari internet maupun intranet. Proxy Server bertindak sebagai *gateway* terhadap dunia *internet* untuk setiap komputer klien. *Proxy server* tidak terlihat oleh komputer klien: seorang pengguna yang berinteraksi dengan internet melalui sebuah *proxy server* tidak akan mengetahui bahwa sebuah *proxy server* sedang menangani *request* yang dilakukannya. *Web server* yang menerima request dari proxy server akan menginterpretasikan request-request tersebut seolah-olah request itu datang secara langsung dari komputer klien, bukan dari proxy server.

Proxy server juga dapat digunakan untuk mengamankan jaringan pribadi yang dihubungkan ke sebuah jaringan publik (seperti halnya Internet). *Proxy server* memiliki lebih banyak fungsi daripada router yang memiliki fitur packet filtering karena memang proxy server beroperasi pada level yang lebih tinggi dan memiliki kontrol yang lebih menyeluruh terhadap akses jaringan. *Proxy*

server yang berfungsi sebagai sebuah “agen keamanan” untuk sebuah jaringan pribadi, umumnya dikenal sebagai firewall. (Melwin, 2005).

3.9 Protokol-Protokol Aplikasi

Protokol-protokol aplikasi tersebut merupakan suatu aplikasi yang berhubungan dan digunakan dalam protokol seperti halnya:

3.9.1. FTP (*File Transfer Protocol*)

Protokol transfer berkas (*File transfer Protocol*) adalah sebuah protokol internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas (*file*) komputer antar mesin-mesin dalam sebuah antar jaringan.

FTP merupakan salah satu protokol internet yang paling awal dikembangkan, dan masih digunakan hingga saat ini untuk melakukan pengunduhan (*download*) dan penggugahan (upload) berkas-berkas komputer antara klien FTP dan server FTP. Sebuah Klien FTP merupakan aplikasi yang dapat mengeluarkan perintah-perintah FTP ke sebuah server FTP, sementara server FTP adalah sebuah Windows Service atau daemon yang berjalan di atas sebuah komputer yang merespons perintah-perintah dari sebuah klien FTP. Perintah-perintah FTP dapat digunakan untuk mengubah direktori, mengubah modus transfer antara biner dan ASCII, menggugah berkas komputer ke server FTP, serta mengunduh berkas dari server FTP. (Irzam, 2004).

3.9.2. TELNET (*Terminal Network*)

Telnet (*Terminal network*) adalah sebuah protokol jaringan yang digunakan pada Internet atau Local Area Network untuk menyediakan fasilitas

komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal. TELNET dikembangkan pada 1969 dan distandarisasi sebagai IETF STD 8, salah satu standar Internet pertama. TELNET memiliki beberapa keterbatasan yang dianggap sebagai risiko keamanan. Telnet ini juga disebut sebagai general-purpose client atau server application program. (Irzam, 2004).

3.9.3. SMTP

SMTP (*Simple Mail Transfer Protocol*) merupakan salah satu protokol yang umum digunakan untuk pengiriman surat elektronik di Internet. Protokol ini dipergunakan untuk mengirimkan data dari komputer pengirim surat elektronik ke server surat elektronik penerima.

Protokol ini timbul karena desain sistem surat elektronik yang mengharuskan adanya server surat elektronik yang menampung sementara sampai surat elektronik diambil oleh penerima yang berhak. (Irzam, 2004).