BAB II

LANDASAN TEORI

A. Jaringan Komputer

Jaringan komputer merupakan sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti printer, hardisk, dan sebagainya.

Selain itu jaringan komputer bisa diartikan sebagai kumpulan sejumlah terminal komunikasi yang berada di berbagai lokasi yang terdiri dari lebih satu komputer yang saling berhubungan. Bagian yang menerima disebut client dan bagian yang memberikan layanan disebut *server sistem* ini dikenal juga sebagi sistem *client-server* yang sudah digunakan pada hampir seluruh aplikasi jaringan komputer.

Menurut Forouzan (2007,p7) jaringan adalah seperangkat *devices* (biasanya disebut sebagai *nodes*) yang dihubungkan melalui *communication links*. Pada dasarnya tujuan daripada pembuatan jaringan adalah untuk :

1. Dapat menghemat *hardware* seperti berbagi pemakaian printer dan CPU.
2. Melakukan komunikasi, contohnya surat elektronik, *instant messaging*, *chatting*.

3. Mendapatkan akses informasi dengan *up to date* dan cepat, contohnya: *web browsing*.
4. Melakukan *sharing* data.
5. Membantu berkomunikasi/transaksi.

Berdasarkan luas daerah yang dapat dijangkau, jaringan dibagi menjadi beberapa jenis, yaitu :

1. *Local Area Network* (LAN)

   Menurut *White* (2012:176), LAN merupakan sebuah komunikasi jaringan yang menghubungkan berbagai perangkat komunikasi data dalam sebuah wilayah berskala kecil dan memiliki kecepatan transmisi data yang tinggi.

   Jaringan wilayah lokal (*Local Area Network)* biasa disingkat LAN) adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil, seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah 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 WLAN (*Wireless* LAN). Tempat-tempat yang menyediakan koneksi WLAN dengan teknologi *Wi-fi* biasa disebut *hotspot*.

   Pada sebuah LAN, setiap node atau komputer mempunyai daya komputasi sendiri. 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. Biasanya salah satu komputer di antara jaringan komputer itu akan digunakan menjadi *server* yang mengatur semua sistem di dalam jaringan tersebut.

2. Metropolitan Area Network (MAN)

Sebuah MAN, biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu : jaringan Bank dimana beberapa kantor cabang sebuah Bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya. Misalnya Bank BNI yang ada di seluruh wilayah Pekanbaru atau Medan. (Ardiansyah, 2004).

Jaringan wilayah metropolitan atau *Metropolitan Area Network* atau disingkat dengan MAN adalah suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya. Jaringan MAN adalah gabungan dari beberapa LAN. MAN merupakan jaringan yang tepat untuk membangun jaringan antar

kantor-kantor dalam satu kota antara pabrik/instansi dan kantor pusat yang berada dalam jangkauannya.

Beberapa teknologi yang digunakan untuk tujuan ini adalah *Asynchronous Transfer Mode* (ATM), FDDI, dan SMDS. Teknologi ini sekarang dalam proses digantikan oleh *Ethernet* berbasis koneksi (misalnya, *Metro Ethernet*) di kebanyakan daerah. MAN menghubungkan antara jaringan area lokal yang telah dibangun tanpa kabel baik menggunakan gelombang *microwave*, radio, atau *laser link* infra-merah. Sebagian besar perusahaan menyewa atau meminjam jalur dari operator umum karena peletakan kabel panjang secara membentang berbiaya mahal.

3. *Wide Area Network* (WAN)

(Forouzan, Behrouz A., 2007: 14). *Wide Area Network* (WAN) memungkinkan komunikasi data, gambar, suara bahkan video dengan jarak yang relatif jauh dan dapat pula berjarak antar negara, benua bahkan seluruh dunia sekalipun.

Wide Area Network (WAN) adalah sebuah jaringan yang memiliki jarak yang sangat luas, karena radiusnya mencakup sebuah negara dan benua. WAN menggunakan sarana fasilitas transmisi seperti telepon, kabel bawah laut ataupun satelit. Kecepatan transmisinya beragam dari 2Mbps, 34 Mbps, 45 Mbps, 155 Mbps, sampai 625 Mbps (atau kadang-kadang lebih). Faktor khusus yang

mempengaruhi desain dan *performance*-nya terletak pada siklus komunikasi, seperti jaringan telepon, satelit atau komunikasi pembawa lainnya.

Jika dilihat dari fungsinya, sebenarnya WAN tidak jauh berbeda dengan LAN. WAN pada dasarnya adalah kumpulan LAN yang ada diberbagai lokasi. Dibutuhkan sebuah *device* untuk menghubungkan antara LAN dengan WAN dan *device* tersebut adalah *router*.

B. *VoIP*

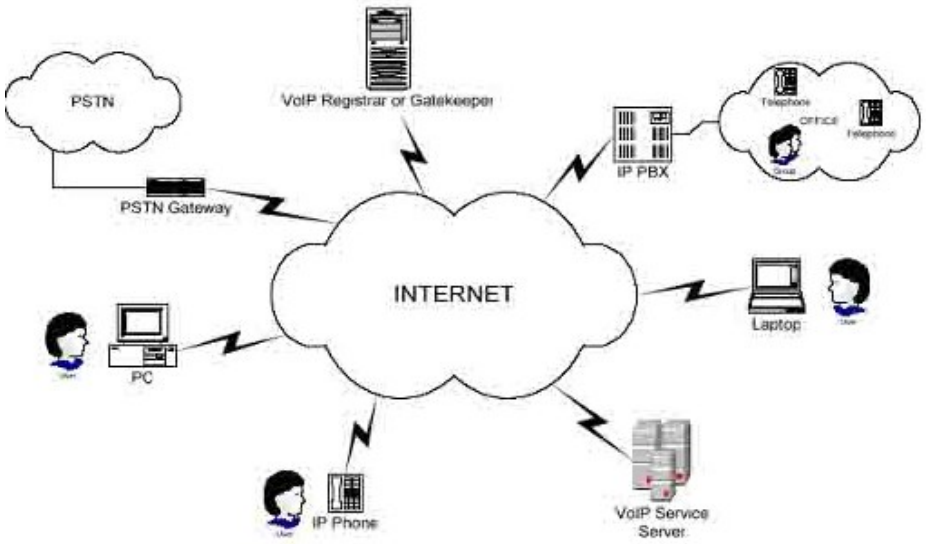
VoIP (*Voice over Internet Protocol*) adalah teknologi yang memanfaatkan *Internet Protocol* untuk menyediakan komunikasi suara secara elektronis dan *real-time* atau teknologi yang menjadikan media internet untuk bisa melakukan komunikasi suara jarak jauh secara langsung.

Trafik *VoIP* dibagi menjadi dua bagian transmisi jaringan yaitu transmisi untuk *signaling* dan untuk RTP *(Realtime Transfer Protocol*). Protokol yang digunakan untuk signaling selalu berbasis TCP *(Transfer Control Protocol*) sedang untuk RTP yang digunakan adalah *protocol* berbasis UDP *(User Datagram Protocol). Signaling* dilakukan diantara *port* TCP yang sudah umum diketahui, misalkan untuk H323 menggunakan *port* 1720, SIP *(session Initiation Protocol)* menggunakan *port* 5060, IAX *(Inter Asterisk Exchange*) menggunakan *port* 4569. Protokol *signaling* dalam *VoIP* diperlukan agar pemakai layanan *VoIP* dapat saling berkomunikasi dengan pesawat telepon. Protokol yang digunakan adalah H.323 dan SIP. H.323 merupakan teknologi

yang dikembangkan oleh *International Telecommunication Union* (ITU-T) sedangkan *Session Initiation Protocol* (SIP) merupakan teknologi yang dikembangkan *Internet Engineering Task Force* (IETF).

Menelepon dengan menggunakan *VoIP* banyak keuntungannya, diantaranya adalah dari segi biaya jelas lebih murah dari tarif telepon tradisional, karena jaringan IP bersifat global. Sehingga untuk hubungan Internasional dapat ditekan hingga 70%. Selain itu, biaya *maintenance* dapat ditekan karena *voice* dan data *network* terpisah.

Sistem *VoIP* terus berkembang dengan berbagai feature, yang juga mempunyai fungsi: *call waiting, call transfer, multiparty conferencing*, dll. Dengan terpisahnya *voice* dan data *network*, *VoIP* termasuk sistem yang dapat menekan biaya *maintenance*. IP *phone* dapat dengan mudah dipindah, ditambah dan diubah. *VoIP* dapat dipasang di sembarang *ethernet* port dan IP *address*, tidak seperti sistem telepon tradisional yang harus mempunyai *port* yang khusus di PBX. Sistem *VoIP* juga *scalable* dalam menangani jumlah panggilan yang banyak (*large call volume*) dan *traffic priorization* yang akan menjamin bahwa *voice packet* dapat dengan cepat diproses di dalam jaringan.



Gambar 2.1 Gambaran cara kerja *VoIP*

Untuk pengiriman sebuah sinyal ke *remote destination* dapat dilakukan secara digital yaitu sebelum dikirim data yang berupa sinyal analog diubah ke bentuk data digital dengan ADC (*Analog to Digital Converter*), kemudian ditransmisikan, dan di penerima dipulihkan kembali menjadi data analog dengan DAC *(Digital to Analog Converter*). Begitu juga dengan *VoIP*, digitalisasi *voice* dalam bentuk *packets* data, dikirimkan dan dipulihkan kembali dalam bentuk *voice* di penerima. Format digital lebih mudah dikendalikan, dalam hal ini dapat dikompresi, dan dapat diubah ke format yang lebih baik dan data digital lebih tahan terhadap *noise* daripada analog.

Bentuk paling sederhana dalam sistem *VoIP* adalah dua buah komputer terhubung dengan internet. Syarat-syarat dasar untuk mengadakan koneksi *VoIP* adalah komputer yang terhubung ke internet, mempunyai *sound card* yang dihubungkan dengan *speaker* dan mikropon. Dengan dukungan *software*

khusus, kedua pemakai bisa saling terhubung dalam koneksi *VoIP* satu sama lain. Bentuk hubungan tersebut bisa dalam bentuk pertukaran file, suara, gambar. Penekanan utama dalam *VoIP* adalah hubungan keduanya dalam bentuk suara.

C. Virtual Private Network (VPN)

VPN adalah singkatan *Virtual Private Network*, yaitu sebuah koneksi *private* melalui jaringan publik atau *internet, virtual network* berarti jaringan yang terjadi hanya bersifat *virtual. Private* yaitu jaringan yang terbentuk *bersifat pribadi* dimana tidak semua orang bisa mengaksesnya. Data yang dikirimkan terenkripsi sehingga tetap rahasia meskipun melalui jaringan publik. Jika menggunakan VPN kita seolah-olah membuat jaringan didalam jaringan atau biasa disebut *tunnel*. VPN menggunakan salah satu dari tiga teknologi *tunneling* yang ada yaitu: PPTP, L2TP dan standar terbaru, *Internet Protocol Security* (biasa disingkat menjadi *IPSec*). VPN merupakan perpaduan antara teknologi *tunneling* dan *enkripsi*.

Ada beberapa keuntungan ketika kita menggunakan VPN, dan pasti sudah agak familiar dengan beberapa manfaat dan fungsi dari VPN itu sendiri, seperti berikut ini keuntungan menggunaan VPN.

4. Dampak Positif / Manfaat VPN
    a. Keamanan, dari segi keamanan tentu pasti, karena ketika kita menggunakan akses *internet* publik (*hotspot, wifi*) dan jika menggunakan VPN tentu akan diubahnya menjadi *internet private*. Maka akan lebih aman dengan mengenkripsi data yang keluar dan masuk supaya keamanan tetap terjaga.
    b. *Remote Acces*, fungsinya kita dapat mengakses jaringan yang terhubung dengan VPN selama terhubung dengan internet.
    c. Hemat, untuk biaya *setup* jaringan cukup murah dimana VPN digunakan sebagai penghubung jaringan lokal yang luas dengan biaya yang lebih kecil. Proses transmisi data menggunakan jaringan publik tanpa membuat jaringan baru yang lebih rumit tentunya.
5. Kegunaan & Fungsi VPN
    a. Kerahasiaan (*Confidentially*)

    VPN menggunakan metode enkripsi untuk mengamankan data yang keluar dan masuk. Dengan metode enkripsi pada VPN, keamanan anda akan lebih aman.

b. Keutuhan Data *(Data Integrity)*

Selain mengamankan, VPN juga mempunya teknologi yang berguna untuk melindungi data yang dikirim dari pengirim hingga sampai tujuan. Sehingga memungkinkan data akan terhindar dari kerusakan, hilang atau dimanipulasi (diubah) oleh pihak yang merugikan.

c. Authentikasi Sumber *(Origin Authentication)*

Mampu untuk mengautentifikasi sumber pengirim data yang akan diterima. VPN juga dapat mengecek atau memeriksa kepada data yang akan masuk dari sumbernya. Setelah proses autentifikasi berhasil, maka informasi dari sumber data akan disetujui.

D. *IPSec*

IPSec atau singkatan dari IP *Security* adalah sebuah protokol jaringan yang dipakai untuk transmisi diagram pada sebuah *Internetwork* dengan basis TCP/IP. *IPSec* sendiri didefinisikan untuk melakukan enrkipsi data dan integritas data di lapisan kedua DARPA *Reference Model* atau *Internetwork Layer*.

E. L2TP

L2TP atau singkatan dari *Layer 2 Tunneling Protocol*. L2TP adalah sebuah standar *IFTF (Internet Engineering Task Force*) yang berguna untuk masalah protokol *tunneling* yang dipakai untuk enkapsulasi terhadap *frame* Protokol PPP (*Point to Point Protocol*). Kemudian ditransmisikan melalui jaringan *TCP/IP X.25, frame* atau jaringan ATM (*Asynchronous Transfer Mode*).

F. *Routing*

Routing adalah proses dimana suatu *item* dapat sampai ke tujuan dari satu lokasi ke lokasi lain. Beberapa contoh *item* yang dapat di-*routing*: *mail*, *telephone call*, dan data. Di dalam jaringan, *Router* adalah perangkat yang digunakan untuk melakukan *routing* trafik.

Konsep dasar *routing* Bahwa dalam jaringan WAN kita sering mengenal yang namanya *TCP/IP (Transmission Control Protocol/ Internet Protocol*) sebagai alamat sehingga pengiriman paket data dapat sampai ke alamat yang dituju (*host* tujuan). TCP/IP membagi tugas masing-masing mulai dari penerimaan paket data sampai pengiriman paket data dalam sistem sehingga jika terjadi permasalahan dalam pengiriman paket data dapat dipecahkan dengan baik. Berdasarkan pengiriman paket data *routing* dibedakan menjadi *routing* lansung dan *routing* tidak langsung.

a. *Routing* langsung merupakan sebuah pengalamatan secara langsung menuju alamat tujuan tanpa melalui *host* lain. Contoh: sebuah

komputer dengan alamat 192.168.1.2 mengirimkan data ke komputer dengan alamat 192.168.1.3

b. *Routing* tidak langsung merupakan sebuah pengalamatan yang harus melalui alamat *host* lain sebelum menuju alamat *host* tujuan. (contoh: komputer dengan alamat 192.168.1.2 mengirim data ke komputer dengan alamat 192.1681.3, akan tetapi sebelum menuju ke komputer dengan alamat 192.168.1.3, data dikirim terlebih dahulu melalui *host* dengan alamat 192.168.1.5 kemudian dilanjutkan ke alamat *host* tujuan.) berikut adalah jenis konfigurasi routing:

    a. Jenis Konfigurasi *Routing*

        1) Minimal *Routing* merupakan proses *routing* sederhana dan biasanya hanya pemakaian lokal saja.
        2) *Static Routing*, dibangun pada jaringan yang memiliki banyak *gateway*. Jenis ini hanya memungkinkan untuk jaringan kecil dan stabil.
        3) *Dynamic Routing*, biasanya digunakan pada jaringan yang memiliki lebih dari satu rute. *Dynamic routing* memerlukan *routing protocol* untuk membuat tabel *routing* yang dapat memakan *resource* komputer.

b. Tabel *Routing*

Router atau perangkat-perangkat lain yang dapat melakukan fungsi *routing*, membutuhkan informasi sebagai berikut :

1) Alamat Tujuan/*Destination Address* – Tujuan atau alamat item yang akan *dirouting.*
2) Mengenal sumber informasi – Dari mana sumber (*router* lain) yang dapat dipelajari oleh *router* dan memberikan jalur sampai ke tujuan.
3) Menemukan rute – Rute atau jalur mana yang mungkin diambil sampai ke tujuan.
4) Pemilihan rute – Rute yang terbaik yang diambil untuk sampai ke tujuan.
5) Menjaga informasi *routing* – Suatu cara untuk menjaga jalur sampai ke tujuan yang sudah diketahui dan paling sering dilalui.

Sebuah *router* mempelajari informasi *routing* dari mana sumber dan tujuannya yang kemudian ditempatkan pada tabel *routing*. *Router* akan berpatokan pada tabel ini, untuk memberitahu *port interface* yang akan digunakan untuk meneruskan paket ke alamat tujuan. Jika jaringan tujuan, terhubung langsung (*directly connected*) di *router*, *Router* sudah langsung mengetahui *port interface* yang harus digunakan untuk meneruskan paket. Jika jaringan tujuan tidak terhubung

langsung di badan *router, Router* harus mempelajari rute terbaik yang akan digunakan untuk meneruskan paket. Informasinya dapat dipelajari dengan cara :

1) Manual oleh "*Network Administrator*"
2) Pengumpulan informasi melalui proses dinamik dalam jaringan.

c. *Router Static* dan *Dinamic*

Ada dua cara untuk memberitahu *router* bagaimana cara meneruskan paket ke jaringan yang tidak terhubung langsung (*not directly connected*) di badan *router*.

Dua metode untuk mempelajari rute melalui jaringan adalah :

1) Rute Statik

   Rute yang dipelajari oleh *router* ketika seorang *Administrator* membentuk rute secara manual. *Administrator* harus memperbarui atau mengupdate rute statik ini secara manual ketika terjadi perubahan topologi antar jaringan.

2) Rute Dinamik

   Rute secara Dinamik dipelajari oleh *router* setelah seorang *administrator* mengkonfigurasi sebuah protokol *routing* yang membantu menentukan rute. Tidak seperti rute Statik, pada rute Dinamik, sekali seorang *administrator*

jaringan mengaktifkan rute Dinamik, maka rute akan diketahui dan *diupdate* secara otomatis oleh sebuah proses *routing* ketika terjadi perubahan di topologi jaringan. Berikut adalah macam-macam protocol routing dinamik :

a) RIP (*Routing Information Protocol*)

RIP merupakan *routing information protokol* yang memberikan routing tabel berdasarkan *router* yang terhubung langsung, Kemudian *router* selanjutnya akan memberikan informasi *router* selanjutnya yang terhubung langsung dengan itu. Adapun informasi yang dipertukarkan oleh RIP yaitu : *Host, network, subnet, rute default*. RIP dibagi menjadi RIPv1 dan RIPv2.

b) IGRP (*Interior Gateway Routing Protocol*)

Interior Gateway Routing Protocol (IGRP) adalah sebuah routing *protocol* berpemilik yang dikembangkan pada pertengahan tahun 1980-an oleh *Cisco Systems, Inc Cisco* tujuan utama dalam menciptakan IGRP adalah untuk menyediakan protokol yang kuat untuk *routing* dalam sistem otonomi (*AS). IGRP* memiliki *hop* maksimum 255, tetapi *defaultnya* adalah 100. IGRP menggunakan *bandwidth* dan garis menunda secara *default* untuk menentukan rute terbaik dalam sebuah *internetwork (Composite Metrik*). Pada

IGRP ini *routing* dilakukan secara matematik berdasarkan jarak. Untuk itu pada IGRP ini sudah mempertimbangkan hal berikut sebelum mengambil keputusan jalur mana yang akan ditempuh. Adapun hal yang harus diperhatikan: *load, delay, bandwitdh, realibility*.

c) OSPF (*Open Short Path First*)

OSPF adalah sebuah *protocol* standar terbuka yang telah dimplementasikan oleh sejumlah *vendor* jaringan. OSPF bekerja dengan sebuah algoritma yang disebut algoritma *Djikstra*. Pertama sebuah pohon jalur terpendek *(shortest path tree*) akan dibangun, dan kemudian *routing table* akan diisi dengan jalur-jalur terbaik yang dihasilkan dari pohon tersebut. OSPF hanya mendukung *routing* IP saja.

d) EIGRP *(Enhanced Interior Gateway Routing Protocol*)

EIGRP menggabungkan konsep *link state protocol. Broadcast-broadcast di-update* setiap 90 detik ke semua EIGRP *router* berdekatan. Setiap *update* hanya memasukkan perubahan jaringan. EIGRP sangat cocok untuk jaringan besar. Tapi EIGRP hanya tersedia di *Router* dengan merk *Cisco*

Pada EIGRP ini terdapat dua tipe *routing* protokol yaitu dengan *distance* vektor dan dengan *Link state*. IGRP dan EIGRP sama-sama sudah mempertimbangkan masalah *bandwitdh* yang ada dan *delay* yang terjadi.

e) BGP (*Border Gateway Protocol*)

BGP merupakan salah satu jenis *routing protocol* yang ada di dunia komunikasi data. Sebagai sebuah *routing protocol*, BGP memiliki kemampuan melakukan pengumpulan rute, pertukaran rute dan menentukan rute terbaik menuju ke sebuah lokasi dalam jaringan. *Routing protocol* juga pasti dilengkapi dengan algoritma yang pintar dalam mencari jalan terbaik. Namun yang membedakan BGP dengan *routing protocol* lain seperti misalnya OSPF dan IS-IS ialah, BGP termasuk dalam kategori *routing protocol* jenis *Exterior Gateway Protocol* (EGP). BGP merupakan *distance vector exterior gateway protocol* yang bekerja secara cerdas untuk merawat *path-path* ke jaringan lainnya, dan *update*-nya dikirim melalui koneksi TCP.

d. Kabel

Kabel jaringan merupakan salah satu media transmisi yang digunakan pada jaringan komputer agar setiap komputer/perangkat yang tergabung di dalamnya bisa saling

berkomunikasi. Selain menggunakan kabel, terdapat juga media transmisi yang tidak menggunakan kabel yang lebih sering kita sebut *wireless*. Dibandingkan media tanpa kabel, media kabel lebih memiliki kecepatan dan stabilitas yang tinggi serta jangkauan yang lebih jauh. Ada tiga jenis kabel yang digunakan dalam media komunikasi via Kabel, yaitu *Coaxial*, *Twisted Pair*, dan Fiber Optik.

Perancangan jaringan kali ini lebih banyak menggunakan kabel *Twisted Pair.* Kabel tersebut dibagi menjadi dua, yaitu kabel STP dan kabel UTP.

1) Kabel STP

Kabel STP (*Shielded Twisted Pair*) merupakan salah satu media transmisi yang digunakan untuk membuat sebuah jaringan yang berbasis lokal atau biasa disebut LAN (*Local Area Network*). Sesuai namanya *Shielded Twisted Pair* berarti kabel pasangan berpilin atau terbelit dengan pelindung. Hampir sama dengan kabel UTP tapi kabel STP mempunyai selubung lagi yang menyelubungi ke 4 lilitan kabel di dalamnya. Fungsi lilitan dan kulit penyelubung ini adalah sebagai eleminasi terhadap induksi dan kebocoran.

2) Kabel UTP

Kabel UTP (*Unshielded Twisted Pair*) merupakan salah satu media transmisi yang paling banyak digunakan untuk

membuat sebuah jaringan yang berbasis lokal atau biasa disebut LAN (*Local Area Network*). Sesuai namanya yaitu *Unshielded Twisted Pair* berarti kabel pasangan yang berpilin atau terbelit tanpa pelindung. Fungsi dari lilitan ini adalah sebagai eleminasi terhadap induksi dan kebocoran. Kabel jenis banyak digunakan untuk membuat sebuah jaringan selain harganya yang tidah terlalu mahal, kabel ini juga mudah untuk memotongnya karena hanya mempunyai satu kulit penyelubung. Oleh karena itu banyak orang yang menggunakan kabel jenis ini untuk membuat sebuah jaringan.

Penggunaan kabel UTP dalam jaringan dibagi menjadi dua, yaitu kabel *straight* dan kabel *cross over*.

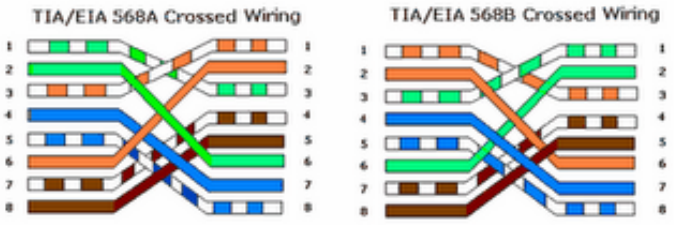
a) Kabel *Straight*

Kabel *straight* merupakan kabel yang memiliki cara pemasangan yang sama antara ujung satu dengan ujung yang lainnya. Kabel *straight* digunakan untuk menghubungkan 2 *device* yang berbeda. Urutan standar kabel *straight* adalah seperti dibawah ini yaitu sesuai dengan standar TIA/EIA 368B (yang paling banyak dipakai) atau kadang-kadang juga dipakai sesuai standar TIA/EIA 368A sebagai berikut:

Gambar 2.2 Urutan susunan kabel *straight*

b) Kabel *Cross Over*

Kabel *cross over* merupakan kabel yang memiliki susunan berbeda antara ujung satu dengan ujung dua. Kabel *cross over* digunakan untuk menghubungkan 2 *device* yang sama. Gambar dibawah adalah susunan standar kabel *cross over*.



Gambar 2.3 Urutan susunan kabel cross over

G. Cisco Packet Tracer

Packet Tracer adalah *simulator* alat-alat jaringan *Cisco* yang sering digunakan sebagai media pembelajaran dan pelatihan, dan juga dalam bidang penelitian simulasi jaringan komputer. Program ini dibuat oleh *Cisco Systems* dan disediakan gratis untuk fakultas, siswa dan alumni yang telah berpartisipasi di *Cisco Networking Academy*. Tujuan utama *Packet Tracer* adalah untuk menyediakan alat bagi siswa dan pengajar agar dapat memahami prinsip jaringan komputer dan juga membangun *skill* di bidang alat-alat jaringan *Cisco*.

Packet Tracer dapat mensimulasikan *Application Layer protocols*, *Routing* dasar RIP, OSPF, dan EIGRP, sampai tingkat yang dibutuhkan pada kurikulum CCNA yang berlaku, sehingga bila dilihat sekilas *software* ini bertujuan untuk kelas CCNA.

Target *Packet Tracer* yaitu menyediakan simulasi jaringan yang *real*, namun terdapat beberapa batasan berupa penghilangan beberapa perintah yang digunakan pada alat aslinya yaitu pengurangan *command* pada *Cisco IOS*. Dan juga *Packet Tracer* tidak bisa digunakan untuk memodelkan jaringan produktif/aktif.

Packet Tracer biasanya digunakan siswa *Cisco Networking Academy* melalui sertifikasi *Cisco Certified Network Associate* (CCNA). Dikarenakan batasan pada beberapa fiturnya, *software* ini digunakan hanya sebagai alat bantu belajar, bukan seabagai pengganti *router* dan *switch Cisco*.