

BAB I

DASAR-DASAR JARINGAN KOMPUTER

1.1 Tujuan Praktikum

- Praktikan dapat memahami dasar-dasar jaringan komputer.
- Praktikan dapat mendesain jaringan sederhana.

1.2 Dasar Teori

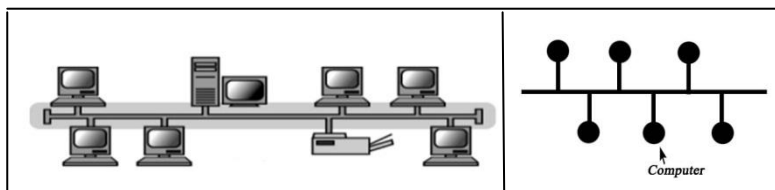
1.2.1 Pengenalan Jaringan Komputer

Computer network atau jaringan komputer ialah dua atau lebih komputer yang saling terhubung sehingga dapat berbagi sumber daya (*resources*) untuk mencapai suatu tujuan tertentu. Dengan begitu diharapkan dapat memunculkan efisiensi, sentralisasi, dan optimasi kerja.

1.2.2 Topologi Fisik Jaringan

Topologi pada sebuah jaringan dibutuhkan karena fungsi dari topologi itu sendiri untuk menggambarkan sebuah jaringan secara fisik. Topologi jaringan dapat berupa topologi bus, topologi ring, topologi star, atau campuran. Pada bagian ini akan dibahas secara ringkas mengenai ketiga topologi jaringan tersebut serta kelebihan dan kekurangannya.

a. Topologi Bus



Gambar 1.1 Topologi Bus

- Pada topologi bus, *node-node* (komputer) dihubungkan secara serial di sepanjang kabel dan pada kedua ujung kabel ditutup dengan **terminator**.
- Sangat sederhana dalam instalasi, lebih ekonomis dalam hal biaya.
- Paket-paket data saling berseliweran pada satu kabel sehingga apabila *node* yang terhubung banyak maka kinerja jaringan akan turun karena *collision* (tabrakan paket data) lebih sering terjadi.
- Tidak memerlukan *hub*, tetapi memerlukan *T-connector* untuk membuat percabangan kabel.
- Masalah yang dapat terjadi pada jaringan bertopologi bus ini adalah seluruh jaringan dapat *down* atau terputus bila salah satu komputer mati atau bermasalah pada *network card*-nya.

Kelebihan :

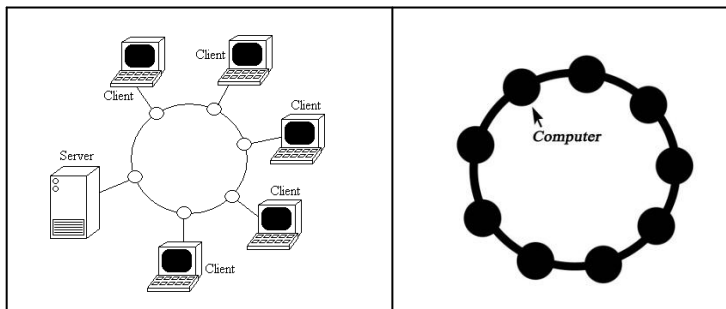
- Jumlah *node* tidak dibatasi, tidak seperti *hub* yang dibatasi oleh jumlah dari *port* (misal : 16 *port* untuk 16 *node*).
- Kecepatan pengiriman data lebih cepat, karena data berjalan searah.

3. Lebih mudah dan murah jika ingin menambah atau mengurangi jumlah *node*, karena yang dibutuhkan hanya kabel dan konektornya saja.

Kelemahan :

1. Jika lalu lintas data yang diolah terlalu besar dapat mengakibatkan kemacetan.
2. Diperlukan *repeater* untuk menguatkan sinyal pada pemasangan jarak jauh.
3. Jika salah satu *node* mengalami kerusakan, maka jaringan tidak dapat beroperasi.

b. Topologi Ring



Gambar 1.2 Topologi Ring

1. *Node-node* dihubungkan secara serial di sepanjang kabel dengan bentuk jaringan seperti lingkaran.
2. Paket-paket data mengalir dalam satu arah sehingga *collision* dapat dihindari.
3. Masalah yang dihadapi sama dengan masalah pada jaringan topologi bus.

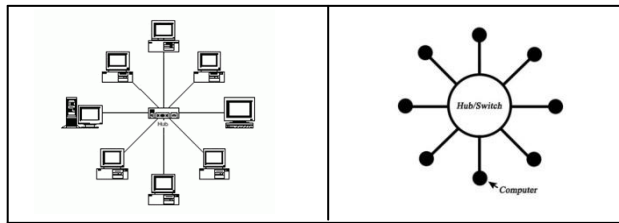
Kelebihan :

1. Aliran data mengalir lebih cepat karena dapat melayani data dari kiri atau kanan dari *server*.
2. Tidak akan terjadi tabrakan pengiriman data (*collision*), karena pada satu waktu hanya satu *node* yang dapat mengirimkan data.
3. Hemat kabel.
4. Waktu untuk mengakses data lebih optimal.

Kelemahan :

1. Penambahan terminal */node* menjadi lebih sulit bila *port* sudah habis.
2. Sulit mendeteksi kerusakan
3. Jika terdapat gangguan di suatu terminal mengakibatkan terganggunya seluruh jaringan.

c. Topologi Star



Gambar 1.3 Topologi Star

1. Komputer saling terhubung menggunakan sebuah *switch* atau *hub*.
2. *Hub* atau *switch* berfungsi sebagai penerima sinyal dari suatu komputer dan kemudian meneruskannya ke semua komputer lain yang terhubung dengan *hub/switch*.
3. Jaringan dengan topologi star membutuhkan biaya yang lebih banyak sebab selain membutuhkan biaya tambahan untuk *hub/switch*, setiap komputer harus ditarik kabel ke *hub/switch*.
4. Pencarian kesalahan pada jaringan lebih mudah sebab masing-masing komputer mempunyai jalur kabel sendiri ke *switch*.
5. Jenis kabel yang sering digunakan untuk jaringan bertopologi star ini adalah kabel UTP *Category-5* untuk kecepatan 100 Mbps dan kabel UTP *Category-6* untuk kecepatan 1 Gbps.

Kelebihan :

1. Jika terjadi penambahan atau pengurangan terminal tidak mengganggu operasi yang sedang berlangsung.
2. Jika salah satu terminal rusak, maka terminal lainnya tidak mengalami gangguan.
3. Arus lalu lintas informasi data lebih optimal.
4. Kecepatan *transfer* data relatif lebih baik.

Kelemahan :

1. Jumlah terminal terbatas, tergantung dari *port* yang ada pada *hub*.
2. Lalu lintas data yang padat dapat menyebabkan jaringan bekerja lebih lambat.
3. Apabila lalu lintas *transfer* data padat, sering terjadi tabrakan *file* (*collision*).

1.2.3 Topologi Logik Jaringan

a. Client Server

Client server adalah suatu jaringan yang terdiri dari beberapa komputer dan dari salah satu komputer bertindak sebagai *Server* yang memiliki tugas untuk melayani komputer lainnya yang disebut *client* (*workstation*), dan komputer *Client* hanya menerima pelayanan dari komputer *server*. Dalam jaringan *client server*, sebuah *server* mengatur akses *resource* (*file* dan *printer*) untuk *client*. *Server* menjalankan *Network Operating System* (*NOS*) untuk menyediakan layanan dan mengautentifikasi *client* dan *client* menjalankan *software NOS-client*. *Server* dapat berupa

dedicated yang berfungsi hanya sebagai *server*, contohnya *server Novell NetWare*, ada pula yang mempunyai dua fungsi sekaligus sehingga bisa dipakai sebagai layaknya sebuah *workstation*.

b. Peer to Peer

Jaringan *peer to peer* (P2P) adalah satu atau lebih komputer yang saling terhubung, baik dengan media kabel maupun nirkabel dan tiap komputer dapat berkomunikasi secara langsung. Pada jaringan P2P, sebuah komputer dapat berfungsi sebagai *server* dan *client* pada saat yang bersamaan dan tidak ada autentifikasi terpusat, autentifikasi diatur tersendiri di setiap *node* yang memberikan layanan.

c. Host Terminal

Satu atau lebih *server* yang dihubungkan dalam suatu *dumb terminal*. Karena *Dumb Terminal* hanyalah sebuah *monitor* yang dihubungkan dengan menggunakan kabel RS-232, maka pemrosesan data dilakukan di dalam *server*, oleh karena itu suatu *server* haruslah sebuah sistem komputer yang memiliki kemampuan pemrosesan data yang tinggi dan penyimpanan data yang besar.

1.2.4 Jenis Jaringan Berdasarkan Jangkauan

a. LAN (Local Area Network)

Jaringan lokal atau *Local Area Network* adalah sekumpulan dua atau lebih komputer yang berada dalam batasan jarak lokasi satu dengan yang lain, yang saling terhubung baik secara langsung maupun tidak langsung.

b. MAN (Metropolitan Area Network)

Pada umumnya MAN mencakup area satu kota yang dapat berupa gabungan dari sejumlah LAN yang terpisah. MAN terhubung dengan jalur transmisi yang dinamakan *backbone* (jaringan utama sistem komunikasi).

c. WAN (Wide Area Network)

Wide Area Network merupakan jaringan komputer yang mencakup area yang besar seperti jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan *router* dan saluran komunikasi publik.

d. Internet

Internet adalah sistem global dari seluruh jaringan [komputer](#) yang saling terhubung menggunakan *standar Internet Protocol Suite* (TCP/IP) untuk melayani miliaran pengguna di seluruh dunia.

e. Intranet

Jaringan lokal yang memberikan layanan pada terminal *client*-nya. Jaringan ini biasanya dipakai pada sebuah perusahaan untuk menghubungkan antara komputer yang satu dengan komputer yang lain. Sebuah *intranet* tidak selalu terhubung pada *internet*.

1.2.5 Pengalamatan Komputer

a. IP Address

IP Address atau alamat IP adalah pengalamatan yang digunakan untuk mengidentifikasi *interface* jaringan pada *host* dari suatu mesin. *IP address* terdiri atas dua versi, yaitu **IPv4** dan **IPv6**.

IP versi 4 berupa sekelompok bilangan biner 32 bit yang dibagi menjadi 4 bagian dan masing-masing bagian terdiri dari 8 bit. Untuk memudahkan kita dalam membaca dan mengingat suatu alamat komputer, maka umumnya penamaan yang digunakan adalah berdasarkan bilangan desimal.

Contoh: 11000000.10101000.00011011.00000010

192. 168. 27. 2

Mengapa bisa seperti itu??

Karena di setiap subnet terdapat 8 bit dan setiap bit bernilai berbeda-beda:

1	1	1	1	1	1	1	1
↓	↓	↓	↓	↓	↓	↓	↓
128	64	32	16	8	4	2	1

Sedangkan IP versi 6 berupa sekelompok bilangan hexadesimal sepanjang 128 bit yang dipisahkan oleh tanda titik dua setiap 8 bit. Pada pembahasan selanjutnya, yang akan digunakan adalah pengalamatan IP versi 4.

b. Pembagian Kelas IP

Agar *IP address* pada komputer tidak simpang siur maka *IP address* dibagi beberapa kelas. Masing-masing kelas mempunyai kapasitas jumlah IP yang berbeda-beda. Berikut ini adalah pembagian kelas IP:

Kelas A

Format : 0xxxxxxx.yyyyyyyy.yyyyyyyy.yyyyyyyy

Subnetmask default : 255.0.0.0

Kisaran : 0.0.0.0 – 127.255.255.255

Jumlah *Host* : 16,777,214

Kelas B

Format : 10xxxxxx.xxxxxxxx.yyyyyyyy.yyyyyyyy

Subnetmask default : 255.255.0.0

Kisaran : 128.0.0.0 – 191.255.255.255

Jumlah *Host* : 65,532

Kelas C

Format : 110xxxxx.xxxxxxxx.xxxxxxxx.yyyyyyyy
Subnetmask default : 255.255.255.0
Kisaran : 192.0.0.0 – 223.255.255.255
Jumlah Host : 254

Keterangan

x menandakan **Network ID**

y menandakan **Host ID**

Tiap-tiap *IP address* hanya bisa berhubungan jika mereka berada di satu jaringan. Contohnya, jika komputer A mempunyai *IP address* 192.168.17.3, komputer B mempunyai *IP address* 192.168.19.3 dan Komputer C mempunyai 192.168.17.20, maka komputer mana yang dapat berhubungan? Ya benar, komputer A dan Komputer C. Kenapa? Karena mereka mempunyai *network ID* yang sama tetapi *Host ID*-nya berbeda. Sedangkan Komputer B mempunyai *Network ID* dan *Host ID* berbeda.

Jumlah *host* yang dimaksud di atas adalah jumlah *IP address* yang dapat digunakan sebagai alamat sebuah *network card*. Kita ambil contoh kelas C. Sebenarnya, jumlah *IP address* yang ada pada jaringan kelas C adalah 256 *IP address*, namun dua buah *IP address* digunakan sebagai alamat pengenalan jaringan (***network address***) dan alamat *broadcast* (***broadcast address***). Jadi jumlah *IP address* yang dapat digunakan untuk pengalamatan komputer adalah 254.

1.2.6 Subnetting

Konsep *subnetting* muncul akibat adanya kekhawatiran menipisnya jumlah IP yang ada di *internet*. *Subnet* adalah segmen fisik di lingkungan TCP/IP yang menggunakan *IP address* yang diturunkan dari *network ID* tunggal. Umumnya, sebuah organisasi memperoleh sebuah *network ID* dari *internic*.

Jika teman-teman pernah menemukan *IP address* 192.168.27.2/26 maksud dari istilah tersebut adalah, komputer dengan *IP address* 192.168.27.2 dan *subnet mask* /26. Angka 26 setelah karakter / menunjukkan bit aktif (angka 1) mulai dari *octet* yang pertama hingga keempat. Jadi jika diterjemahkan,

IP address : 192.168.27.2

subnet mask : 11111111.11111111.11111111.11000000

atau $\underbrace{\hspace{1.5cm}}$ $\underbrace{\hspace{1.5cm}}$ $\underbrace{\hspace{1.5cm}}$ $\underbrace{\hspace{1.5cm}}$
 255. 255. 255. 192

Untuk menghitung jumlah *subnet*, digunakan formula (2^n) , dimana n menunjukkan jumlah *host ID* teratas (jumlah angka 1).

Dengan formula ini dapat dihitung jumlah total *subnet* yang tersedia untuk setiap kelas dan *subnet mask*.

Untuk menghitung jumlah *host* per *subnet*, digunakan formula (2^N-2) , dimana N menunjukkan sisa jumlah bit *host ID* yang masih tersedia (jumlah angka 0).

Contoh :

1. Terdapat sebuah alamat IP pada kelas C 192.168.27.1 dan ingin membaginya menjadi 4 buah *subnet* sehingga kita mempunyai 4 jaringan.

Langkah-langkah mengerjakan :

a. Hitung subnet (bit yang aktif)

$$2^n = 4 \rightarrow n = 2$$

Angka 2 berarti jumlah bit yang aktif (angka 1).

Netmask default kelas C :

11111111.11111111.11111111.00000000=255.255.255.0

jadi *subnetmask* yang kita dapatkan adalah

11111111.11111111.11111111.11000000=255.255.255.192

b. Hitung jumlah host per subnet (bit yang tidak aktif)

$$\begin{aligned} \text{Jumlah } \textit{host} &= 2^N - 2, \\ \text{dimana } N &= 6 \\ \text{Jadi,} &= 2^6 - 2 \\ &= 62 \textit{ host} \end{aligned}$$

c. Range IP address

Ket :	Jaringan1	Jaringan 2	Jaringan 3	Jaringan 4
Net ID	192.168.27. 0	192.168.27. 64	192.168.27. 128	192.168.27. 192
Range IP	192.168.27. 1 - 192.168.27. 62	192.168.27. 65 - 192.168.27. 126	192.168.27. 128 - 192.168.27. 190	192.168.27. 193 - 192.168.27. 254
Broad cast	192.168.27. 63	192.168.27. 127	192.168.64. 191	192.168.64. 255

1.2.7 Tipe – Tipe Koneksi

a. Connection-oriented protocol

Koneksi ini disebut *Connection-oriented* karena membangun hubungan antar titik terlebih dahulu sebelum mengadakan pertukaran data. Informasi tambahan, seperti alamat IP, akan ditambahkan pada *header* paket, untuk mengontrol alur data dan memastikan data sampai ke tempat tujuan dengan urutan yang tepat tanpa ada bagian yang hilang.

TCP (*Transmission Control Protocol*) termasuk *connection-oriented protocol*. Contoh pemakaian TCP adalah *Web Browsers, Email, dan File Transfers*.

b. Connectionless protocol

Komunikasi data menggunakan *connectionless protocol* bekerja dengan mengirimkan paket IP tanpa memberi notifikasi kepada *host* tujuan tentang paket data yang dikirim. Hal ini

menyebabkan paket yang dikirim mungkin saja mengalami perubahan urutan atau terdapat hilangnya paket data.

Contoh dari *connectionless protocol* adalah *UDP (User Datagram Protocol)*. Keuntungan dari menggunakan *connectionless protocol* adalah *low overhead data delivery*. Sebagai perbandingan, tiap segmen TCP mempunyai 20 bytes tambahan pada *header* ketika di-*encapsulasi* pada *application layer*, sedangkan tiap segmen UDP hanya memiliki 8 bytes tambahan pada *header*. Contoh pemakaian UDP adalah *Domain Name System (DNS)*, *Video Streaming*, *Voice over IP (VoIP)*.

1.2.8 Port

Pada jaringan komputer, *port* diasumsikan sebagai pintu *service*. Misalnya di komputer A membuka *port 21*, maka kita tahu bahwa komputer A membuka diri untuk sebuah pelayanan *ftp (file transfer protocol)*. Jadi *port* dapat diartikan sebagai sebuah nilai yang ditetapkan untuk mengidentifikasi sebuah layanan. Berikut beberapa daftar nama *port* yang umum digunakan:

Port	Service	Penjelasan
21	FTP	<i>File Transfer Protocol</i> sering digunakan untuk melakukan <i>download</i> dan atau <i>upload file</i> , program, maupun <i>software</i> dari <i>internet</i> .
23	Telnet	<i>Telnet</i> memungkinkan <i>user</i> dapat bekerja pada sebuah <i>interface command-line</i> pada sebuah sistem <i>remote</i> .
25	SMTP	Digunakan untuk mengirim pesan-pesan <i>e-mail</i> ke sebuah <i>internet mail server</i> .
80	HTTP	Digunakan untuk mengakses halaman <i>web</i>
110	POP3	Digunakan untuk mengirim pesan-pesan <i>e-mail</i> dari sebuah <i>internet mail server</i> .

1.2.9 Media Transmisi

- a. Menggunakan Kabel Jaringan, jenis-jenis kabel jaringan
 1. *Coaxial* : berbentuk seperti kabel TV.
 2. UTP (*unshielded twisted pair*) terdiri dari empat pasang kabel yang tersusun secara terpilin tanpa jaket pelindung tambahan.
 3. STP (*Shielded twisted pair*) jenis kabel telepon yang digunakan dalam beberapa bisnis instalasi dan jaringan data.
 4. *Fiber optic* : salah satu media transmisi yang dapat menyalurkan informasi berkapasitas besar dengan kehandalan yang tinggi. Berbeda dengan media transmisi lainnya yang memakai gelombang elektromagnet atau listrik sebagai media pembawa, pada serat optik, media pembawanya berupa sinar/cahaya laser.
- b. Nirkabel (*wireless*)
 1. Memanfaatkan udara sebagai media transmisi data. Data dikirimkan dalam bentuk gelombang radio dengan frekuensi 2,4 GHz, 5,8 GHz, 3,3 GHz, dan beberapa pita frekuensi lain.

2. Tipe jaringan nirkabel

- a. *AdHoc* : dua buah komputer saling terhubung secara langsung menggunakan *wireless network card* masing-masing. Tidak diperlukan adanya infrastruktur *wireless*.
- b. *Infrastructure* : dibangun sebuah arsitektur *wireless* di sebuah lokasi dengan memasang peralatan tertentu seperti *access point* dan yang lainnya.

3. Pengamanan jaringan nirkabel

- a. Shared Key atau **WEP** (*Wired Equivalent Privacy*) adalah suatu metoda pengamanan jaringan nirkabel, disebut juga dengan Shared Key Authentication. Shared Key Authentication adalah metoda otentikasi yang membutuhkan penggunaan WEP. Enkripsi **WEP** menggunakan kunci yang dimasukkan (oleh administrator) ke client maupun access point. Kunci ini harus cocok dari yang diberikan access point ke client, dengan yang dimasukkan client untuk otentikasi menuju access point.

Shared Key Authentication kelihatannya lebih aman daripada *Open System Authentication*, namun pada kenyataannya tidak. *Shared Key* malah membuka pintu bagi penyusup atau *cracker*. Penting untuk dimengerti dua jalan yang digunakan oleh WEP. WEP bisa digunakan untuk memverifikasi identitas *client* selama proses *shared key* dari autentikasi, tapi juga bisa digunakan untuk mendekripsi data yang dikirimkan oleh *client* melalui *access point*.

4. **WPA** (*Wi-Fi Protected Access*) adalah suatu sistem yang juga dapat diterapkan untuk mengamankan jaringan nirkabel. Metoda pengamanan dengan WPA ini diciptakan untuk melengkapi dari sistem yang sebelumnya, yaitu WEP. Para peneliti menemukan banyak celah dan kelemahan pada infrastruktur nirkabel yang menggunakan metoda pengamanan WEP. Sebagai pengganti dari sistem WEP, WPA mengimplementasikan *layer* dari IEEE, yaitu *layer 802.11i*. Nantinya WPA akan lebih banyak digunakan pada implementasi keamanan jaringan nirkabel. WPA didesain dan digunakan dengan alat tambahan lainnya, yaitu sebuah komputer pribadi (PC).

Fungsi dari komputer pribadi ini kemudian dikenal dengan istilah *authentication server*, yang memberikan *key* yang berbeda kepada masing-masing pengguna/*client* dari suatu jaringan nirkabel yang menggunakan *access point* sebagai media sentral komunikasi. Seperti dengan jaringan WEP, metoda enkripsi dari WPA ini juga menggunakan algoritma RC4.

1.2.10 Perangkat Jaringan

- a. **Network card Adapter**, disebut juga LAN *card*.
- b. **Hub/switch**, sering disebut sebagai konsentrator karena menjadi titik pusat setiap komputer yang terkoneksi ke jaringan.
- c. **Repeater**, berfungsi untuk memulihkan sinyal yang terganggu untuk memperpanjang jangkauan jaringan.

- d. **Bridge**, digunakan untuk mengatur lalu lintas dua buah jaringan bertipe sama ataupun berbeda. Berbeda dengan *repeater*, *bridge* dapat memisahkan lalu lintas antar jaringan.
- e. **Router**, berfungsi untuk menghubungkan dua buah jaringan yang berbeda tipe maupun protokol. *Router* dapat pula digunakan sebagai pelindung jaringan dari pihak luar yang ingin mengakses jaringan.

1.3 Langkah Praktikum

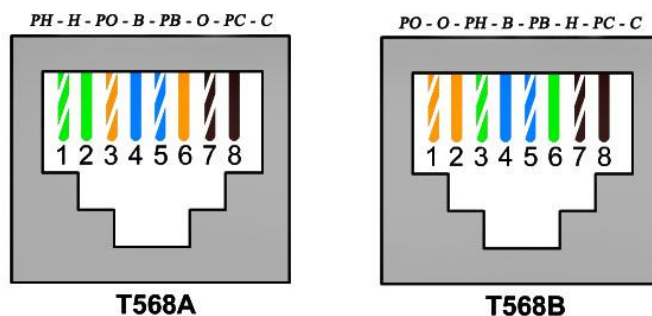
1.3.1 Cabling

a. Alat dan Perlengkapan

1. Kabel UTP *Category-5*
2. *Crimping tool*
3. Konektor RJ-45
4. *Cable Tester*

b. Konfigurasi Urutan Kabel

Terdapat dua tipe urutan kabel berdasarkan kesepakatan konsorsium, **TIA/EIA 568A** dan **TIA/EIA 568B**.



Keterangan

- | | |
|-------------------|------------|
| PH : Putih Hijau | H : Hijau |
| PO : Putih Orange | O : Orange |
| PB : Putih Biru | B : Biru |
| PC : Putih Coklat | C : Coklat |

c. Pemilihan Tipe Konfigurasi

1. Cross-over

Digunakan untuk menyambungkan langsung antar dua PC (komputer - komputer) atau antar hub dengan pemakaian tipe konfigurasi kabel UTP yang salah satu ujungnya menggunakan konfigurasi tipe A dan ujung lainnya memakai konfigurasi tipe B.

c. Straight-through

Digunakan untuk menghubungkan komputer jaringan yang memakai *hub* atau *switch* (komputer - *hub*). Pemakaian *straight - through* dengan menggunakan tipe konfigurasi kabel UTP yang sama pada setiap ujungnya.

d. Langkah Kerja

1. Potong kabel dengan panjang sesuai kebutuhan.
2. Kupas bagian luar kabel (pembungkus kabel-kabel kecil) kira-kira sepanjang 1-2 cm dengan menggunakan pengupas kabel.
3. Atur & urutkan warna kabel sesuai dengan tipe konfigurasi dan urutan diatas.
4. Rapikan susunan kabel dengan cara menekan bagian yang dekat dengan pembungkus kabel supaya susunan kabel terlihat rata.
5. Potong ujung-ujung kabel yang tidak rata dengan pemotong kabel pada *crimping tool*.
6. Masukkan ke dalam konektor, kunci konektor menggunakan *crimping tool*.
7. Lakukan langkah yang sama untuk ujung kabel yang satunya.
8. Uji koneksi kabel menggunakan *cable tester*.