

ADMINISTRASI DAN PENGELOLAAN JARINGAN KOMPUTER



وَمَا رَمَيْتَ إِذْ رَمَيْتَ وَلَكِنَّ اللَّهَ رَمَىٰ . . .

when you threw, but it was Allah who threw
(QS:Al-Anfal :17)

FASILITATOR

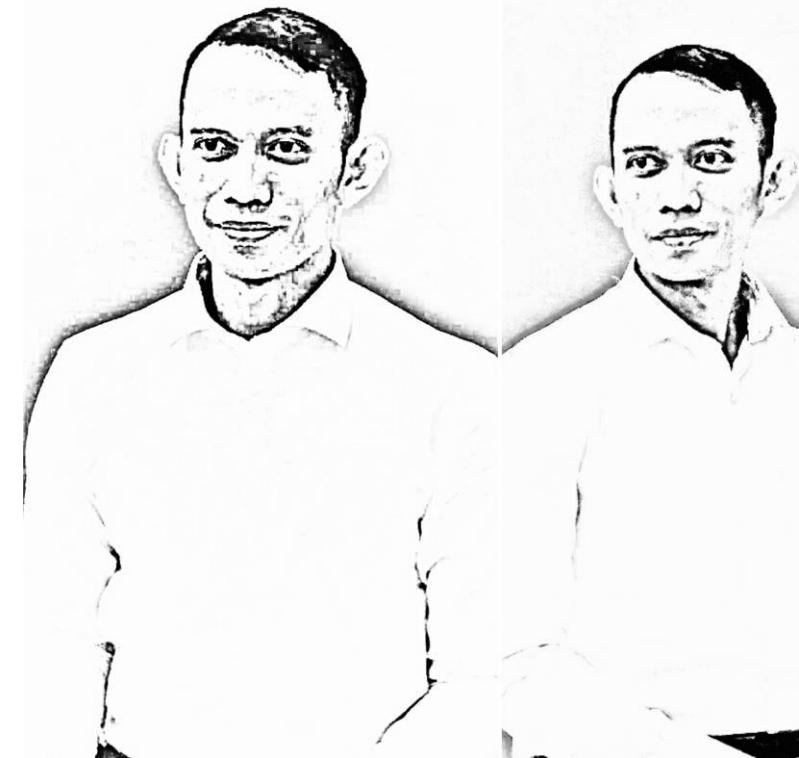
Nama *Budi Subandriyo*

NIP 19780720 200212 1 007

Jabatan Widyaiswara Ahli Madya

Pangkat Pembina (IV/a)

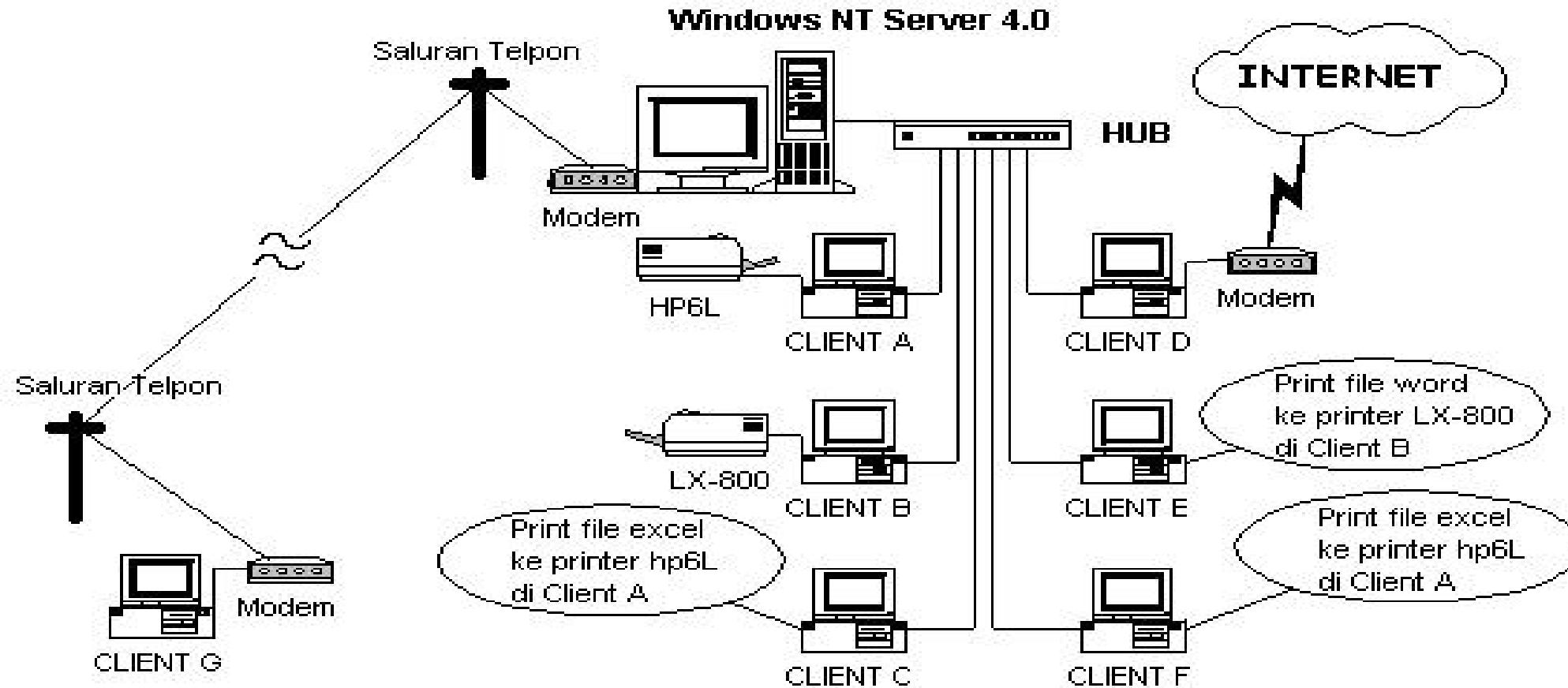
Unit Kerja Pusdiklat BPS

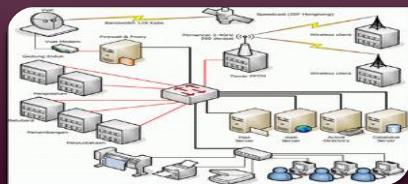


SEBELUM MENGGUNAKAN SISTEM JARINGAN KOMPUTER



SETELAH MENGGUNAKAN SISTEM JARINGAN KOMPUTER





INDIKATOR HASIL BELAJAR

Memahami tentang konsep komunikasi data, model-model jaringan, komponen jaringan, dan sistem operasi serta perangkat lunak jaringan komputer.

Memahami mengenai konsep LAN dan logika *switching* untuk mengelola jaringan lokal di tempatnya bekerja, mengetahui bagaimana mekanisme komunikasi diantara perangkat dalam suatu jaringan komputer.

Memahami mengenai IP Addressing dan konsep routing untuk mengelola jaringan.

Memahami dan melaksanakan sistem keamanan jaringan komputer.

ADMINISTRASI DAN PENGELOLAAN JARINGAN KOMPUTER

TEORI DASAR



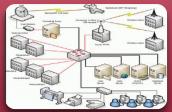
JARINGAN KOMPUTER



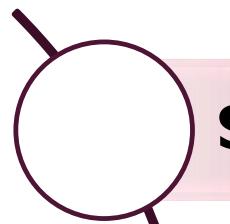
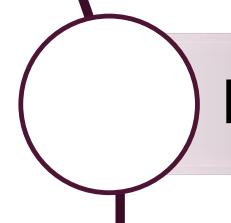
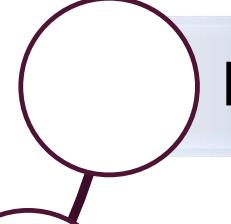
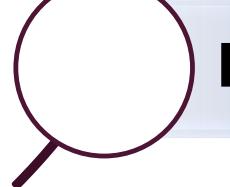


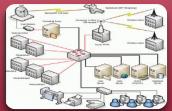
PENGERTIAN

Jaringan komputer adalah sekumpulan perangkat-perangkat yang dapat menyimpan dan mengolah data-data elektronis, dimana satu perangkat dihubungkan dengan perangkat-perangkat lain sedemikian rupa sehingga para pemakai jaringan dapat menyimpan, mengambil serta berbagi informasi dengan pemakai-pemakai lain



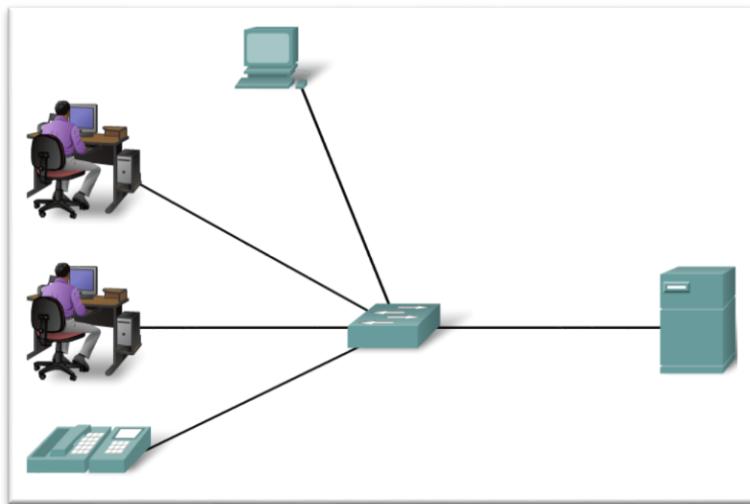
KEGUNAAN JARINGAN

-  **Sharing resource (data, printer, dll)**
-  **Efisiensi waktu**
-  **Efisiensi tempat**
-  **Effisiensi dana**

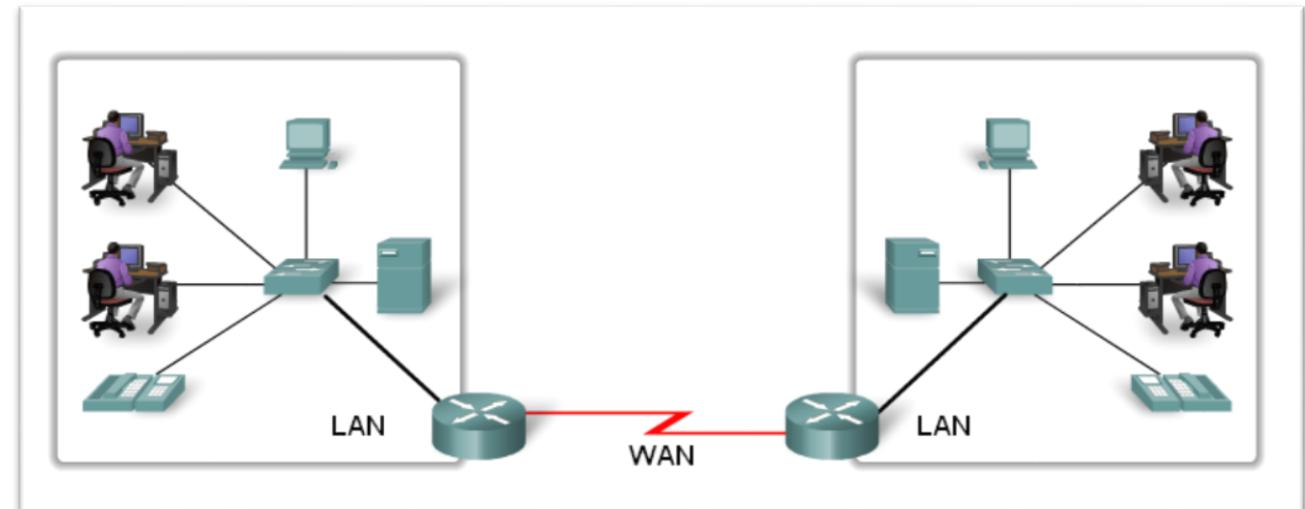


TIPE JARINGAN

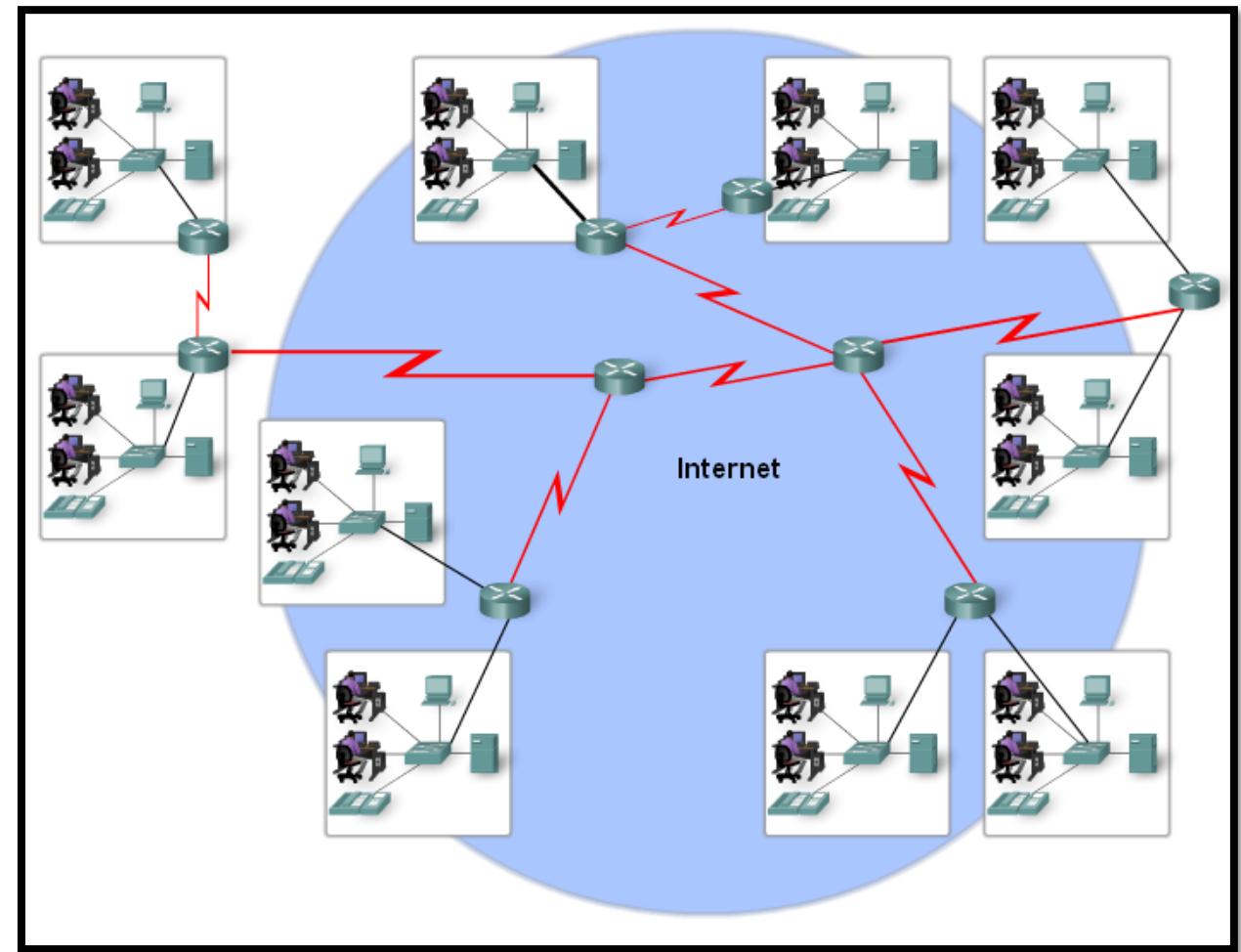
I. LAN (Local Area Network)



2. WAN (Wide Area Network)



3. MAN (Metropolitan Area Network) / Internetwork



Guided Media

- sinyal yang melalui media tersebut dapat terkontrol serta terjamin keutuhannya
- Cth: kabel twisted-pair, seperti yang sering dipakai untuk menghubungkan pesawat telepon; kabel koaksial, seperti yang dipergunakan untuk kabel antena TV; serta kabel optik

Unguided media

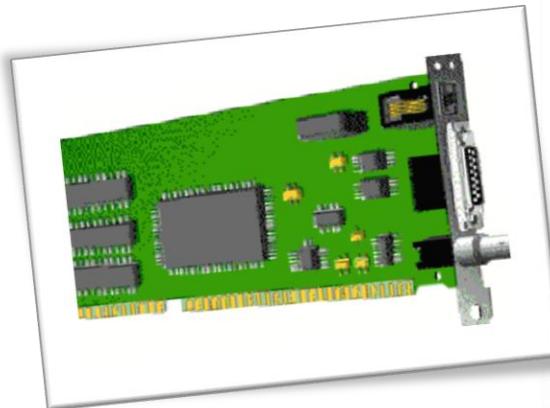
- adalah media transmisi yang merupakan bagian dari alam dan dapat dipergunakan untuk melewatkkan sinyal-sinyal elektronik
- Cth : Atmosfir bumi serta ruang angkasa

Apapun jenis media yang dipergunakan, sinyal-sinyal elektronik akan dipancarkan dalam suatu bentuk gelombang

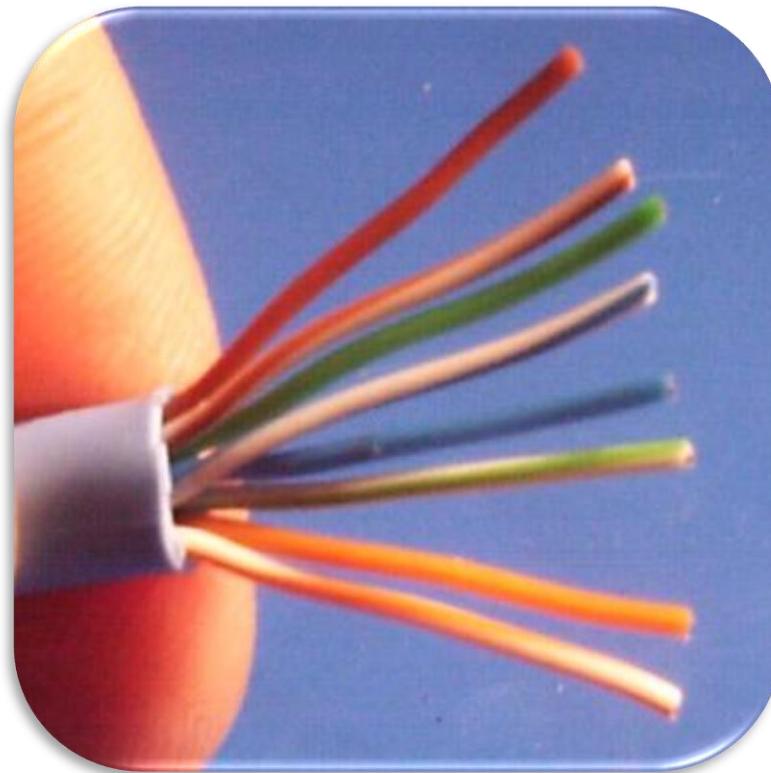
- ✓ Apabila media yang dilalui berupa kawat atau kabel-kabel tembaga -> gelombang elektronik.
- ✓ Apabila kabel optik dipergunakan sebagai media -> gelombang cahaya.
- ✓ Apabila salah satu dari unguided media digunakan -> gelombang radio.

Perangkat Media Transmisi

Network adapter (NIC) Network Interface Card



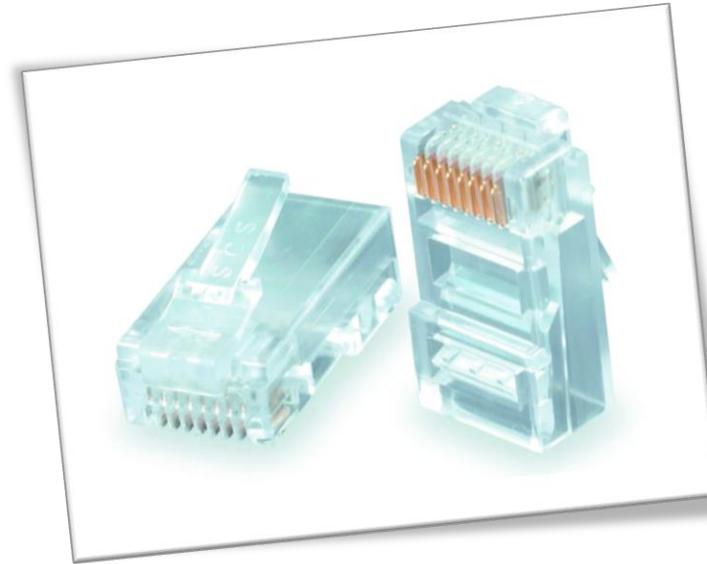
Kabel UTP (*Unshielded twisted-pair*)



Kabel Koaksial



RJ45 - (Registered Jack)45



CABLING

Aturan Pengkabelan UTP

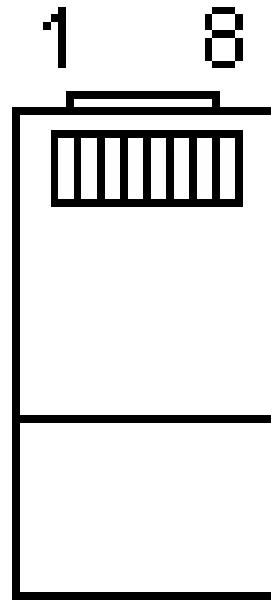


Pin number	Wire Color
Pin 1	==> Orange/White
Pin 2	==> Orange
Pin 3	==> Green/White
Pin 4	==> Blue
Pin 5	==> Blue/White
Pin 6	==> Green
Pin 7	==> Brown/White
Pin 8	==> Brown

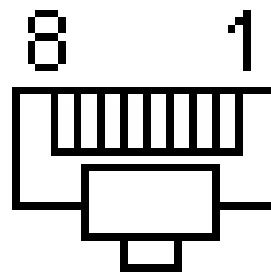
Straight-Through

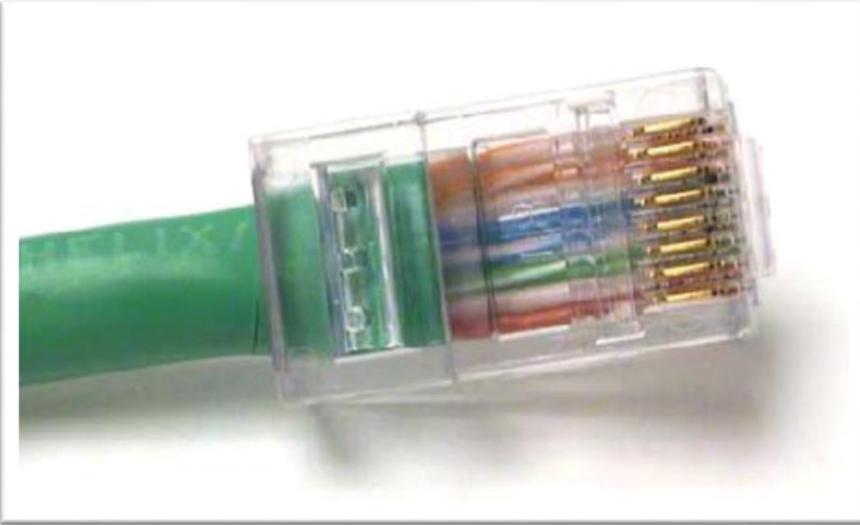
Wire	Becomes
1	→ 1
2	→ 2
3	→ 3
6	→ 6

Top
View

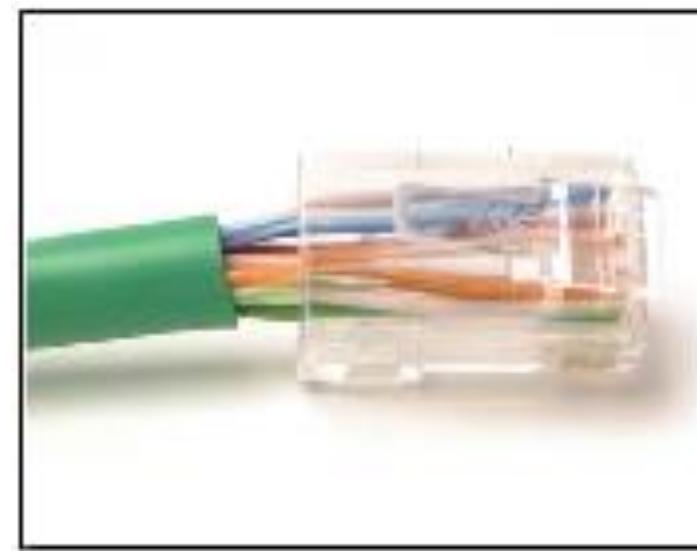


Front
View



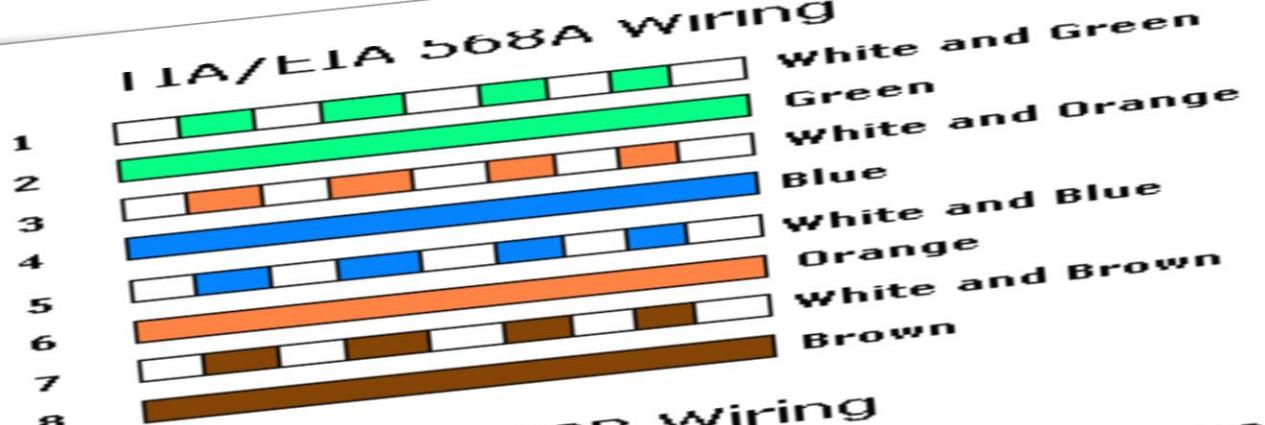


Pemasangan Kabel UTP yang Baik

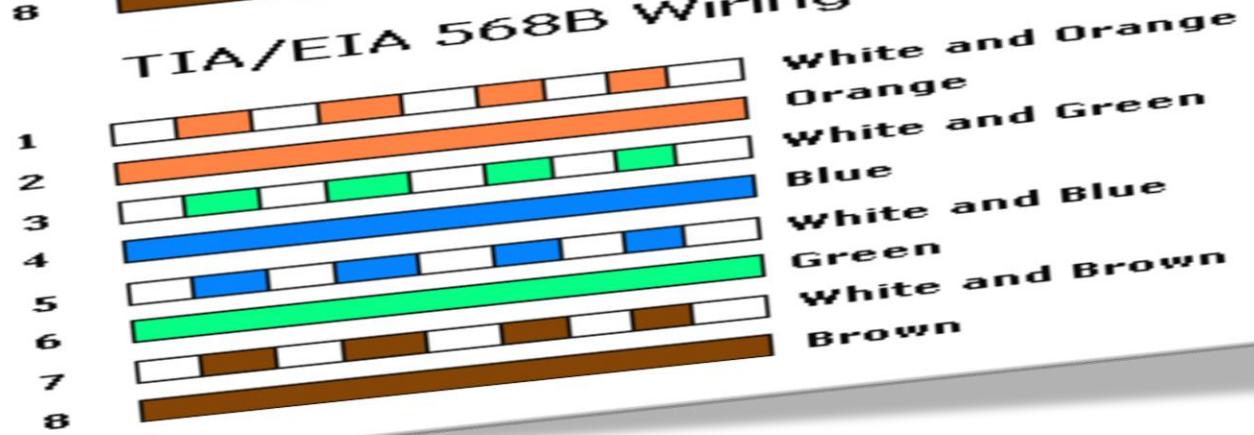


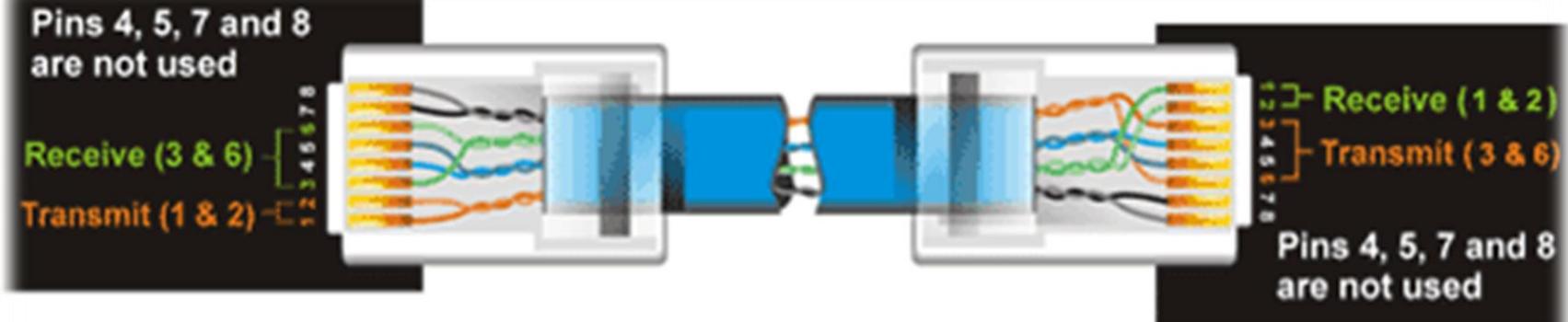
Pemasangan Kabel UTP yang buruk

TIA/EIA 568A Wiring



TIA/EIA 568B Wiring



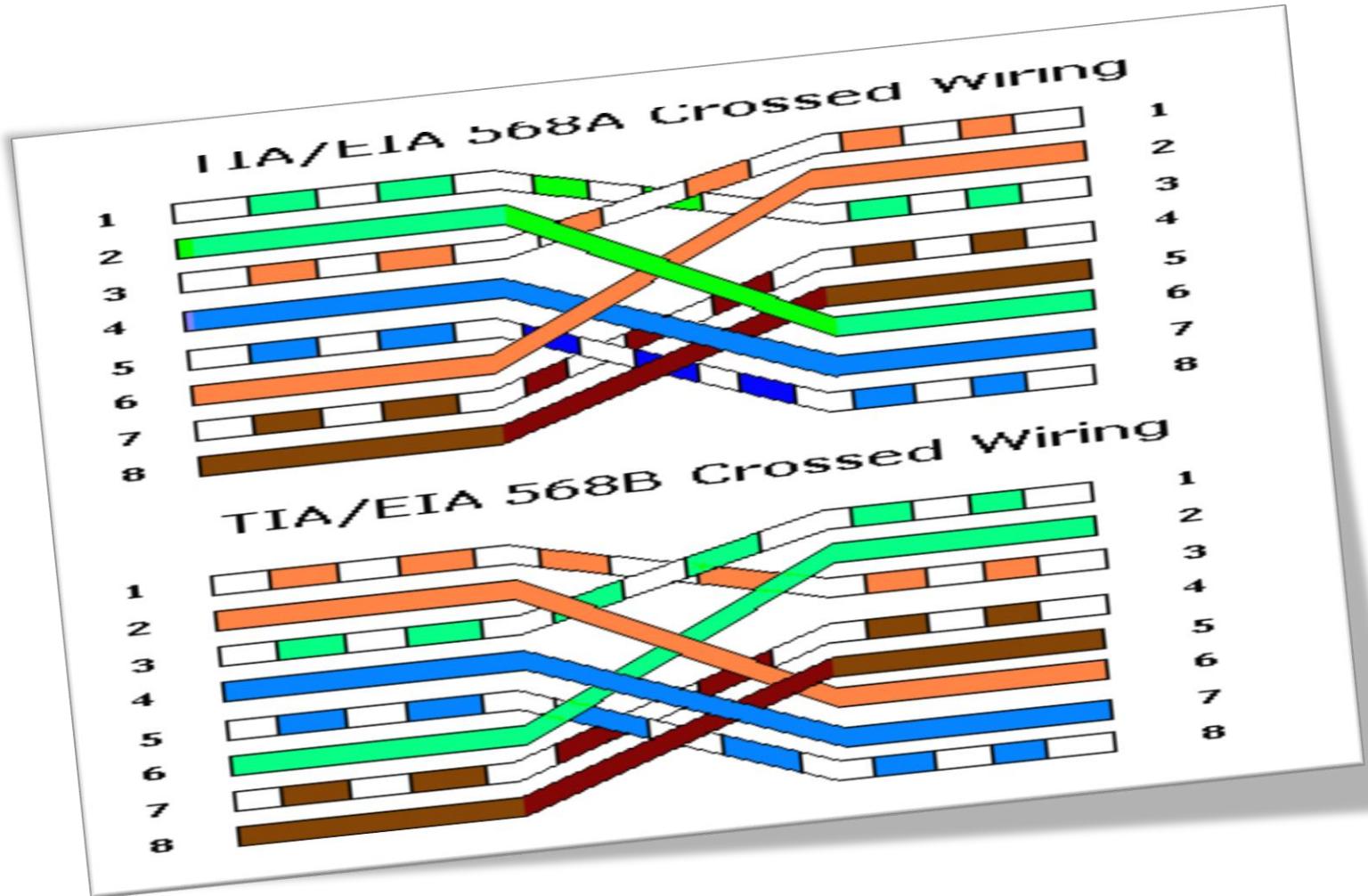


Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Crossed-Over

Wire	Becomes
1	3
2	6
3	1
6	2

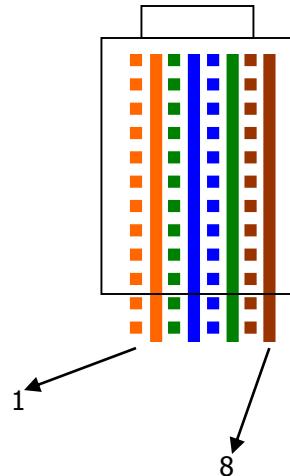
Pin number	Wire Color
Pin 1 ==>	Green/White
Pin 2 ==>	Green
Pin 3 ==>	Orange/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Orange
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown



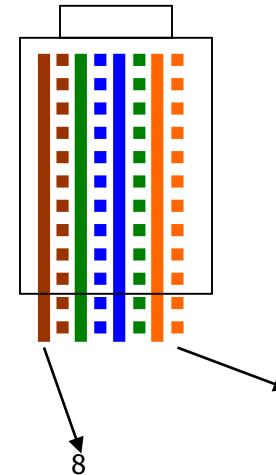
Aturan Pengkabelan UTP

Roll Over

- Digunakan untuk menghubungkan sebuah terminal dan modem ke Cisco Router seri 2500 Access Server



1. Putih Orange
2. Orange
3. Putih Hijau
4. Biru
5. Putih Biru
6. Hijau
7. Putih Coklat
8. Coklat

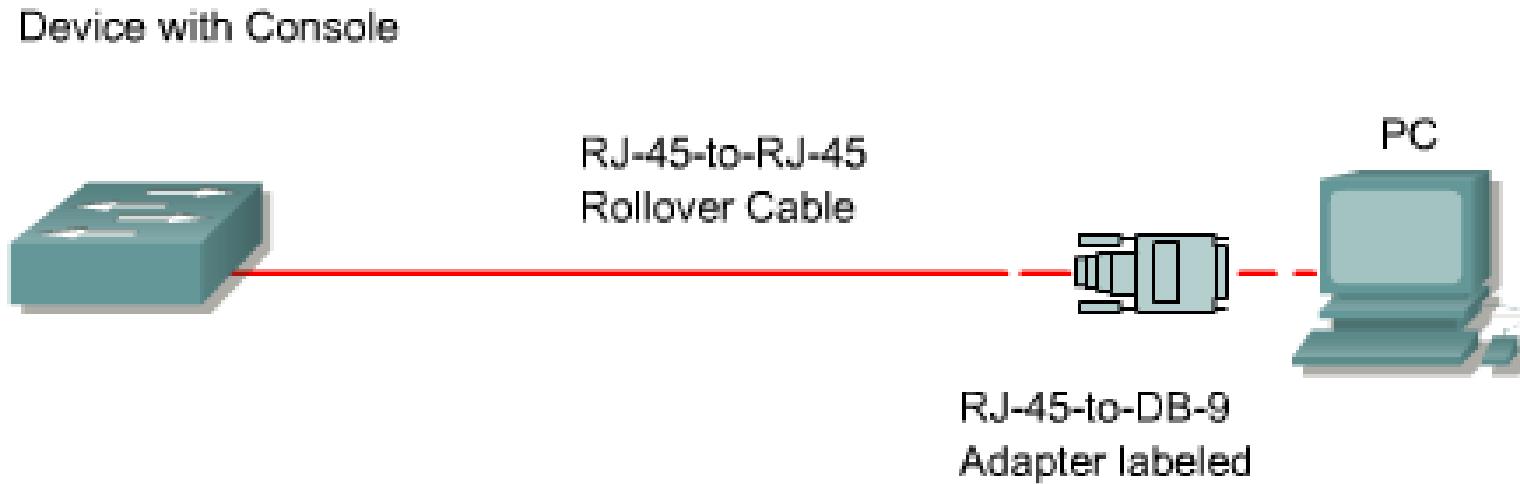


1. Coklat
2. Putih Coklat
3. Hijau
4. Putih Biru
5. Biru
6. Putih Hijau
7. Orange
8. Putih Orange

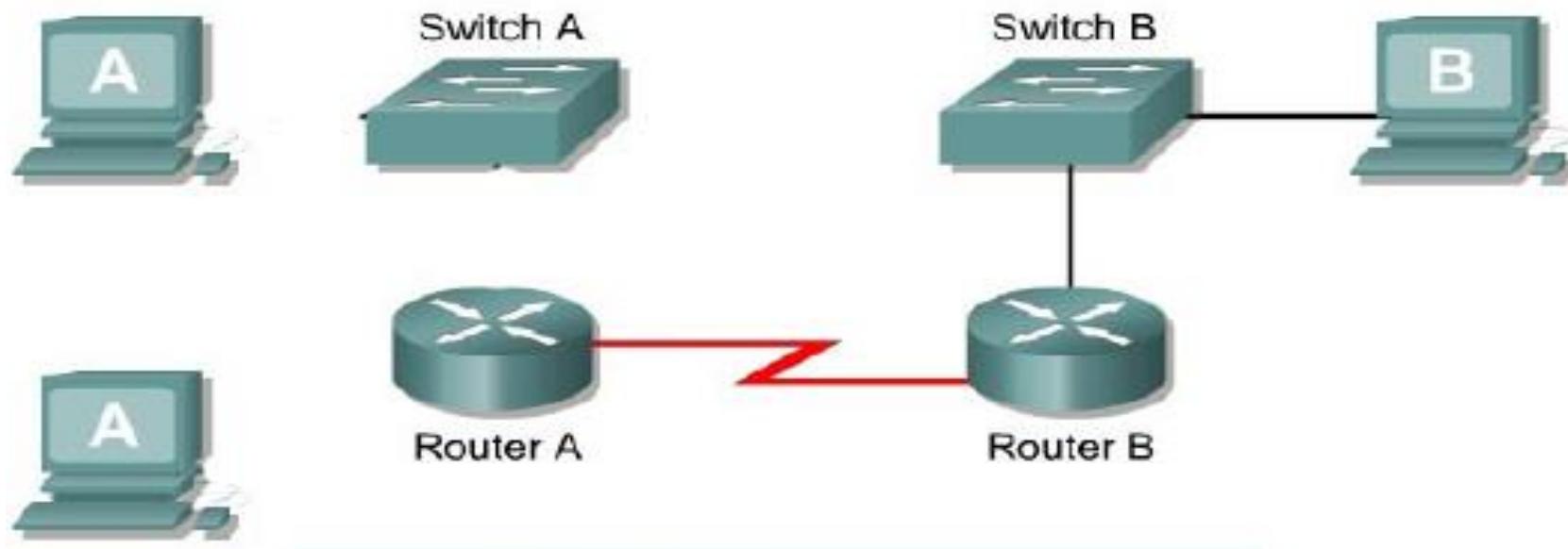
Roll Over

Router Pin name	Router Pin	Direction	Workstation Pin	Workstation Pin name
White-Orange	1		8	Brown
Orange	2		7	White-Brown
White-Green	3		6	Green
Blue	4		5	White-Blue
White-Blue	5		4	Blue
Green	6		3	White-Green
White-Brown	7		2	Orange
Brown	8		1	White- Orange

Roll Over

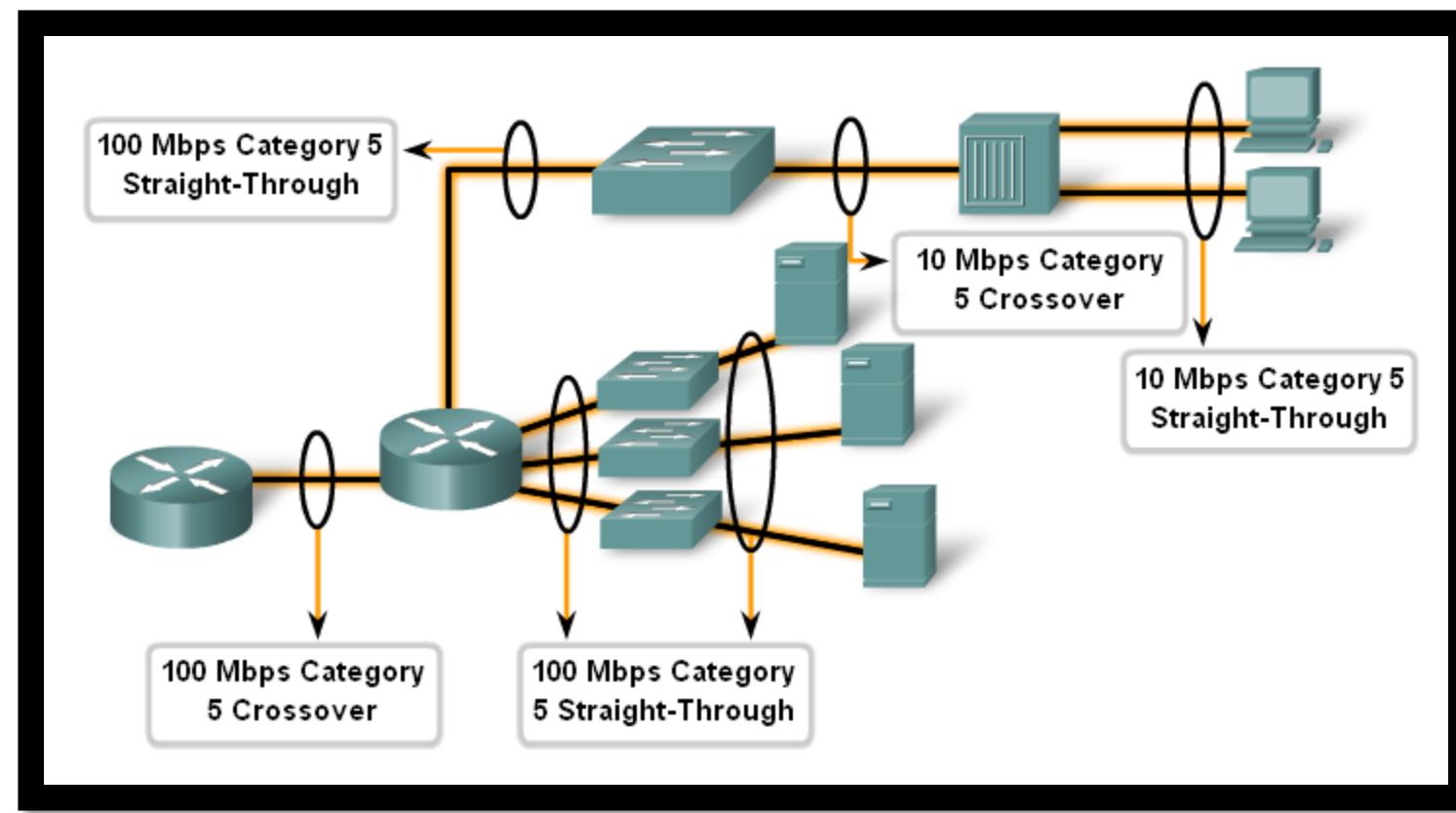


Penggunaan Kabel



Straight-through cable	—
Serial cable	—
Rollover (console)
Crossover cable	- - - - -

Penggunaan Kabel



Types of Ethernet

Ethernet Type	Bandwidth	Cable Type	Duplex	Maximum Distance
10Base-5	10 Mbps	Thicknet Coaxial	Half	500 m
10Base-2	10 Mbps	Thinnet Coaxial	Half	185 m
10Base-T	10 Mbps	Cat3/Cat5 UTP	Half	100 m
100Base-TX	100 Mbps	Cat5 UTP	Half	100 m
100Base-TX	200 Mbps	Cat5 UTP	Full	100 m
100Base-FX	100 Mbps	Multimode Fiber	Half	400 m
100Base-FX	200 Mbps	Multimode Fiber	Full	2 km
1000Base-T	1 Gbps	Cat5e UTP	Full	100 m
1000Base-TX	1 Gbps	Cat6 UTP	Full	100 m
1000Base-SX	1 Gbps	Multimode Fiber	Full	550 m
1000Base-LX	1 Gbps	Single-Mode Fiber	Full	2 km
10GBase-CX4	10 Gbps	Twin-axial	Full	100 m
10GBase-T	10 Gbps	Cat6a/Cat7 UTP	Full	100 m
10GBase-LX4	10 Gbps	Multimode Fiber	Full	300 m
10GBase-LX4	10 Gbps	Single-Mode Fiber	Full	10 km



TOPOLOGI JARINGAN

TOPOLOGI JARINGAN

Topologi adalah bentuk koneksi fisik untuk menghubungkan setiap node pada sebuah jaringan.

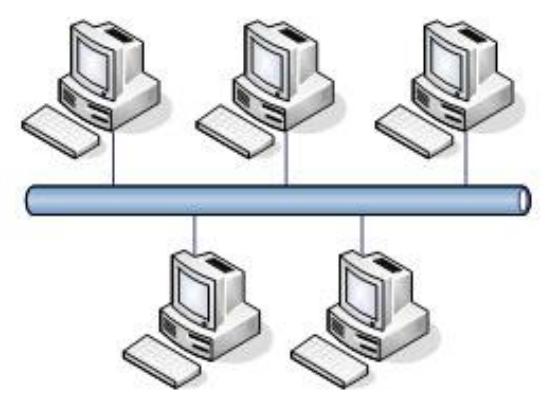
Pada sistem LAN terdapat tiga topologi utama yang paling sering digunakan, yaitu **topologi bus, ring, dan star**.

Topologi jaringan ini kemudian berkembang menjadi topologi **tree, mesh, dan topologi wireless**

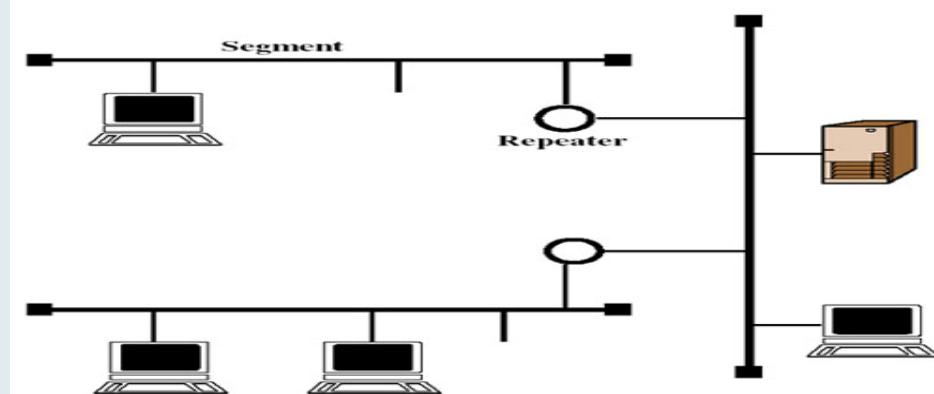
TOPOLOGI BUS

Topologi bus sering disebut juga topologi backbone, dimana ada sebuah kabel coaxial yang dibentang kemudian beberapa computer dihubungkan pada kabel tersebut.

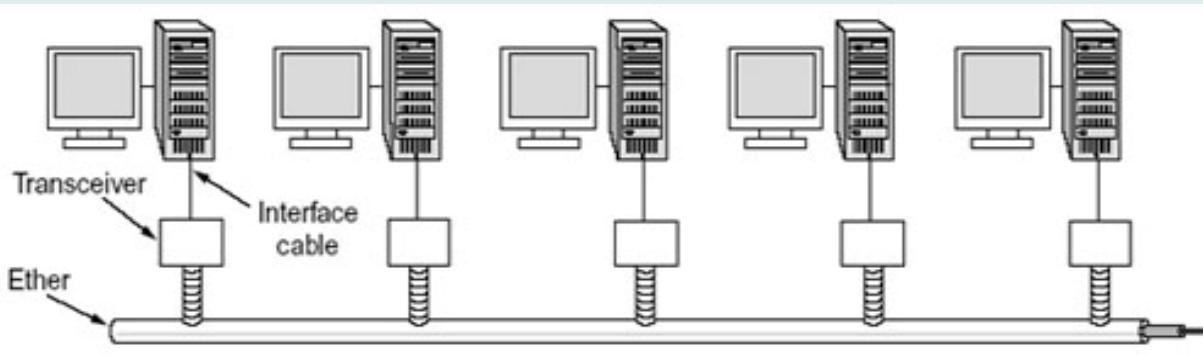
Secara sederhana pada topologi bus, satu kabel media transmisi dibentang dari ujung ke ujung, kemudian kedua ujung di tutup dengan terminator/terminating-resistance yang berupa tahanan listrik lebih kurang 60 ohm.



Gambar Topologi Bus



Gambar Perluasan Topologi Bus Menggunakan Repeater



Gambar Koneksi Kabel-Transceiver Pada Topologi Bus

KELEBIHAN

- Instalasi relative lebih murah.
- Kerusakan satu komputer client tidak akan mempengaruhi komunikasi antar client lainnya .
- Biaya relative lebih murah

KELEMAHAN

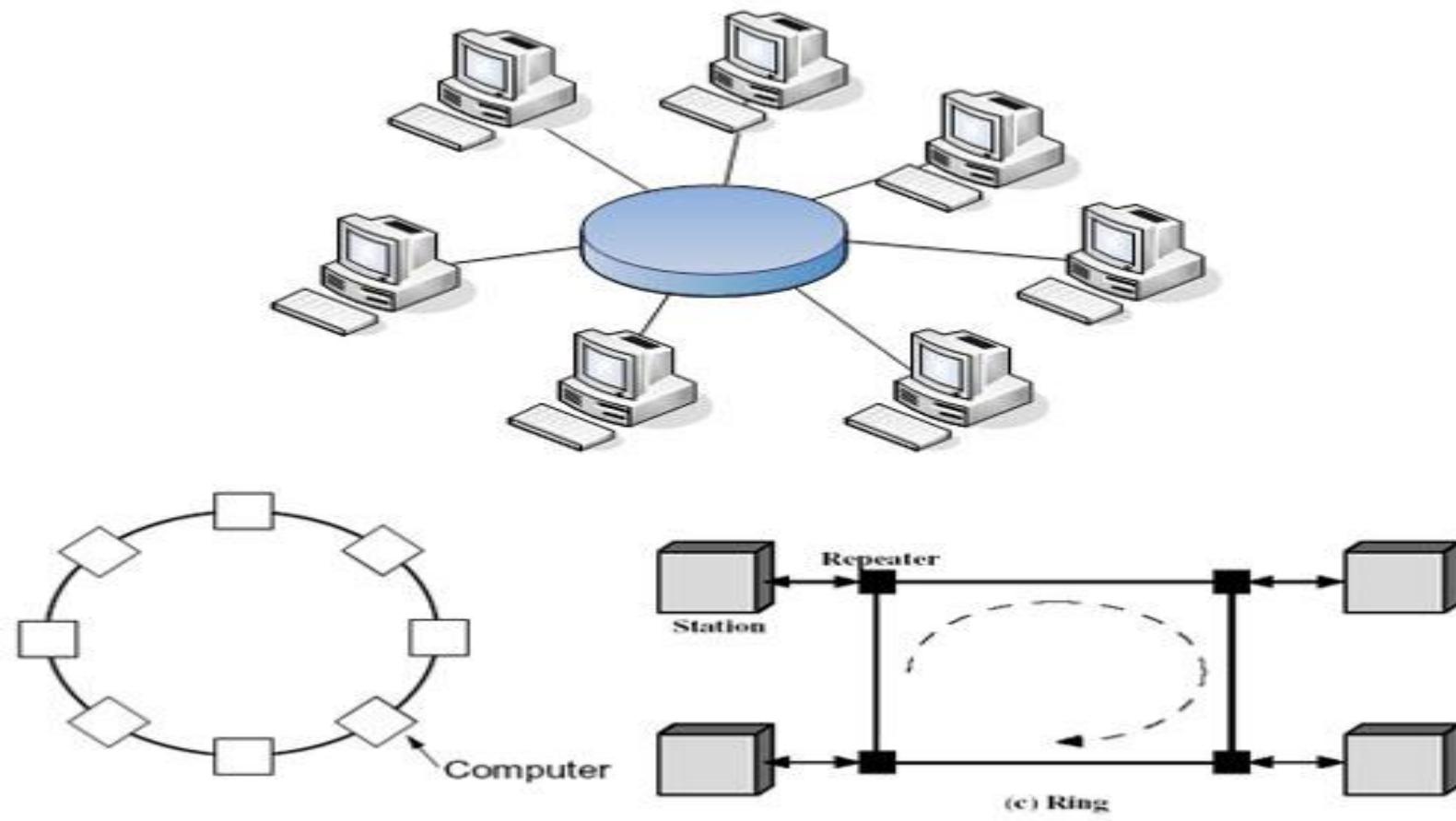
- Jika kabel utama atau backbone putus, maka komunikasi gagal
- Bila kabel utama sangat panjang, maka pencarian gangguan menjadi sulit.
- Kemungkinan akan terjadi tabrakan data/data collision apabila banyak client yang mengirim pesan dan ini akan menurunkan kecepatan komunikasi

TOPOLOGI RING (CINCIN)

Topologi ring biasa disebut juga sebagai topologi cincin karena bentuknya seperti cincin yang melingkar.

Semua komputer dalam jaringan akan dihubungkan pada sebuah cincin.

Cincin ini hampir sama fungsinya dengan konsentrator pada topologi star yang menjadi pusat berkumpulnya ujung kabel dari setiap computer yang terhubung



Gambar Topologi Ring

Secara lebih sedehana topologi cincin merupakan untaian media transmisi dari satu terminal ke terminal lainnya hingga membentuk suatu lingkaran, di mana jalur transmisi hanya satu arah.

Tiga fungsi yang diperlukan dalam topologi cincin : penyelipan data, penerimaan data, dan pemindahan data.

- ▶ Penyelipan data adalah proses dimana data dimasukkan ke dalam saluran transmisi oleh terminal pengirim setelah diberi alamat dan bit-bit tambahan lainnya .
- ▶ Penerimaan data adalah proses ketika terminal yang dituju telah mengambil data dari satu saluran, yaitu dengan cara membandingkan alamat yang ada pada paket data dengan alamat terminal itu sendiri. Apabila alamat tersebut sama, maka data kiriman di salin.
- ▶ Pemindahan data adalah proses dimana kiriman data diambil kembali oleh terminal pengirim karena tidak ada terminal yang menerimanya (mungkin akibat salah alamat).

Pada dasarnya setiap terminal dalam jaringan cincin adalah repeater, dan mampu melakukan ketiga fungsi dari topologi cincin.

Sistem yang mengatur bagaimana komunikasi data berlangsung pada jaringan cincin sering disebut token-ring.

Kemungkinan permasalahan yang bisa timbul dalam jaringan cincin adalah:

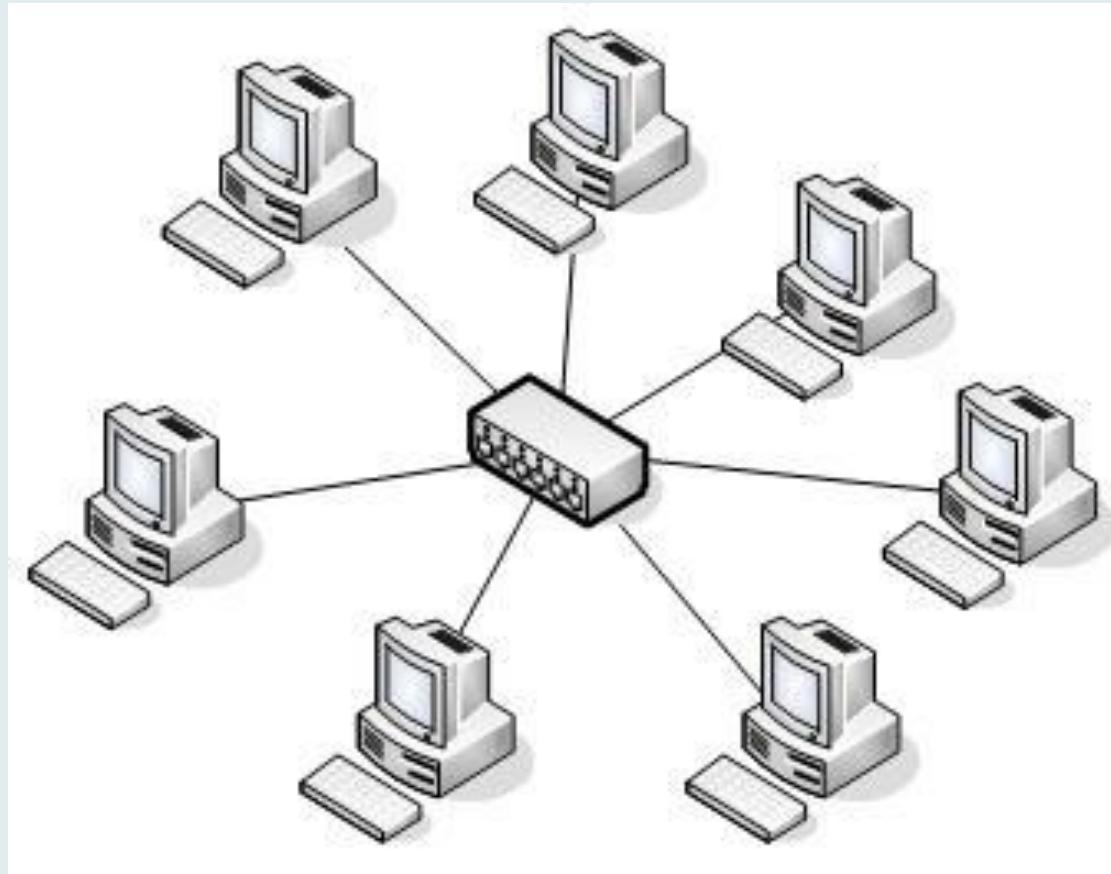
- ▶ Kegagalan satu terminal/repeater akan memutuskan komunikasi ke semua terminal.
- ▶ Pemasangan terminal baru menyebabkan gangguan terhadap jaringan, terminal baru harus mengenal dan dihubungkan dengan kedua terminal tetangganya

TOPOLOGI STAR (BINTANG)

Topologi star bentuknya seperti bintang, sebuah alat yang disebut concentrator bisa berupa hub atau switch menjadi pusat, di mana semua komputer dalam jaringan di hubungkan ke concentrator ini.

Pada toplogi star sebuah terminal pusat bertindak sebagai pengatur dan pengendali semua komunikasi yang terjadi. Terminal-terminal lainnya melakukan komunikasi melalui terminal pusat ini.

Terminal kontrol pusat bisa berupa sebuah komputer yang difungsikan sebagai pengendali tetapi bisa juga berupa HUB atau MAU (Multi Access Unit).



Gambar Topologi Star

Terdapat dua alternatif untuk operasi simpul pusat :

Simpul pusat beroperasi secara broadcast yang menyalurkan data keseluruhan arah. Pada operasi ini walaupun secara fisik kelihatan sebagai bintang, secara logik sebenarnya beroperasi seperti bus, alternatif ini menggunakan HUB.

Simpul pusat beroperasi sebagai switch, data kiriman diterima oleh simpul kemudian dikirim hanya ke terminal tujuan (bersifat point-to-point), alternatif ini menggunakan MAU sebagai pengendali

Bila menggunakan HUB maka secara fisik sebenarnya jaringan berbentuk topologi star namun secara logis bertopologi Bus. Bila menggunakan Mau, maka baik fisik maupun logis bertopologi star.

KELEBIHAN

- Karena setiap komponen dihubungkan langsung ke simpul pusat maka pengelolaan menjadi mudah, kegagalan komunikasi mudah di telusuri.
- Kegagalan pada satu komponen/terminal tidak memengaruhi komunikasi terminal lain.

KELEMAHAN

- Kegagalan pusat kontrol (simpul pusat) memutuskan semua komunikasi.
- Bila yang digunakan sebagai pusat kontrol adalah HUB maka kecepatan akan berkurang sesuai dengan penambahan komputer, semakin banyak semakin lambat

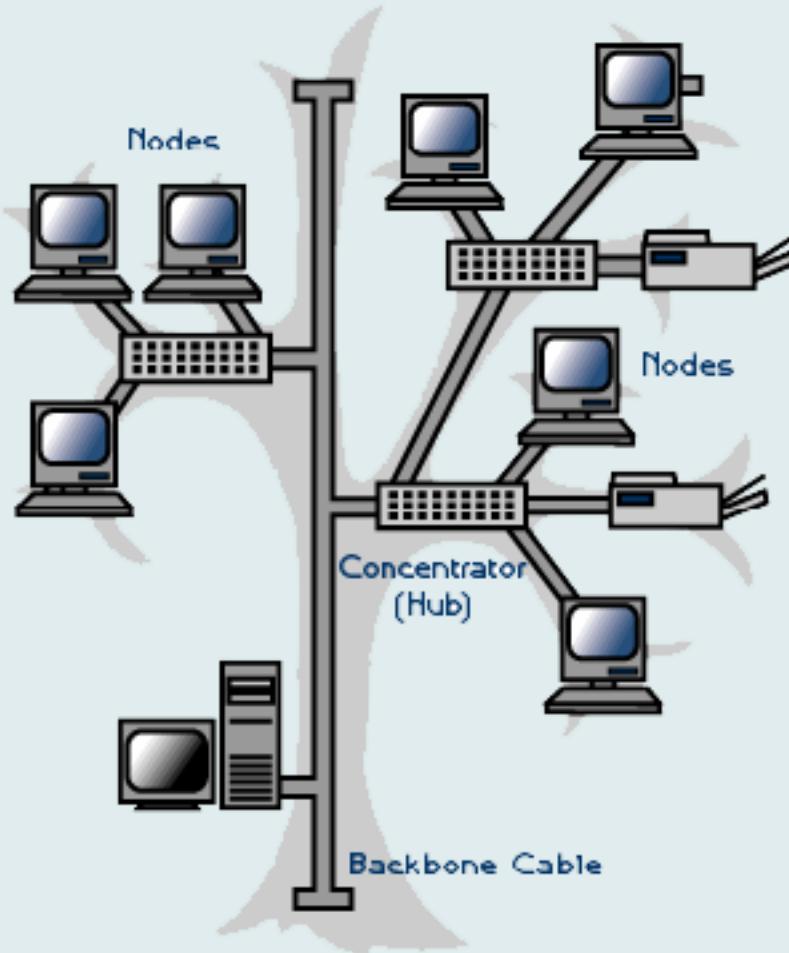
TOPOLOGI TREE (POHON)

Topologi tree adalah pengembangan atau generalisasi topologi bus. Media transmisi merupakan satu kabel yang bercabang namun loop tidak tertutup.

Topologi tree dimulai dari suatu titik yang disebut headend. Dari headend beberapa kabel ditarik menjadi cabang, dan pada setiap cabang terhubung beberapa terminal dalam bentuk bus, atau dicabang lagi hingga menjadi rumit.

Ada dua kesulitan pada topologi ini:

- Karena bercabang maka diperlukan cara untuk menunjukkan kemana data dikirim, atau kepada siapa transmisi data ditujukan.
- Perlu suatu mekanisme untuk mengatur transmisi dari terminal terminal dalam jaringan

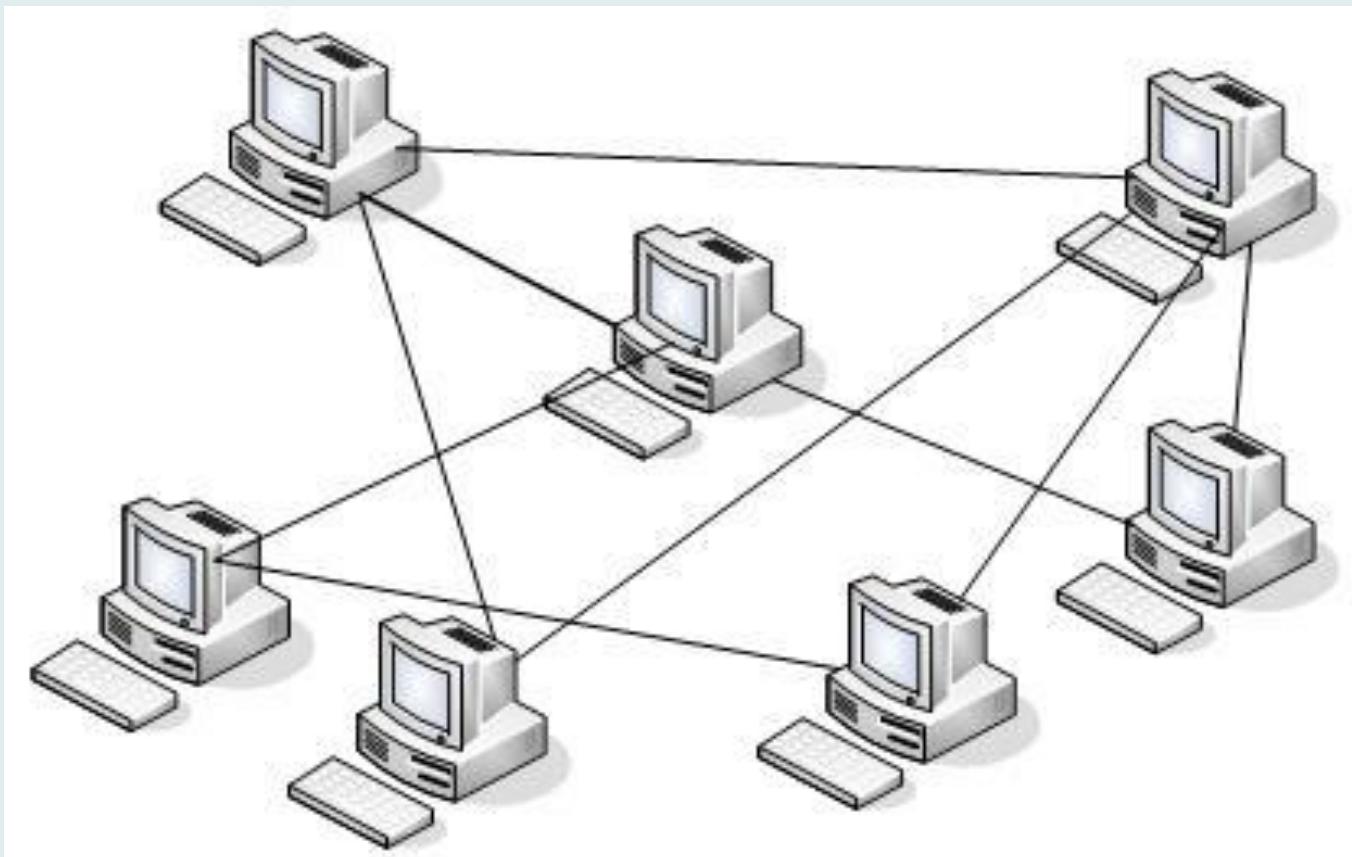


Gambar Topologi Tree

TOPOLOGI MESH (TAK BERATURAN)

Topologi mesh adalah topologi yang tidak memiliki aturan dalam koneksi. Topologi ini biasanya timbul akibat tidak adanya perencanaan awal ketika membangun suatu jaringan.

Karena tidak teratur maka kegagalan komunikasi menjadi sulit dideteksi, dan ada kemungkinan boros dalam pemakaian media transmisi.



Gambar Topologi Mesh

TOPOLOGI WIRELESS (NIRKABEL)

Jaringan nirkabel menjadi trend sebagai alternatif dari jaringan kabel, terutama untuk pengembangan LAN tradisional karena bias mengurangi biaya pemasangan kabel dan mengurangi tugas-tugas relokasi kabel apabila terjadi perubahan dalam arsitektur bangunan dan seterusnya.

Topologi ini dikenal dengan berbagai nama, misalnya WLAN, WaveLAN, HotSpot dan sebagainya.

Penjelasan:

Penggunaan teknologi LAN nirkabel lainnya adalah untuk menghubungkan LAN pada bangunan yang berdekatan.

- a) Syarat-syarat LAN nirkabel :
- b) Laju penyelesaian: Protokol medium acces control harus bisa digunakan se-efesien mungkin oleh media nirkabel untuk memaksimalkan kapasitas.
- c) Jumlah simpul: LAN nirkabel perlu mendukung ratusan simpul pada sel-sel multiple
- d) koneksi ke LAN backbone: modul control (CM) harus mampu menghubungkan suatu jaringan LAN ke jaringan LAN lainnya atau suatu jaringan ad-goc nirkabel
- e) Daerah layanan: daerah jangkauan untuk LAN nirkabel biasanya memiliki diameter 100 hingga 300 meter
- f) Kekokohan dan keamanan transmisi: system LAN nirkabel harus andal dan mampu menyediakan system pengamanan terutama penyadapan.

- i. Teknologi LAN nirkabel:
- ii. LAN infrared (IR) : terbatas dalam sebuah ruangan karena IR tidak mampu menembus dinding yang tidak tembus cahaya.
- iii. LAN gelombang audio: terbatas dalam sebuah kompleks gedung, seperti Bluetooth, Wi-Fi, dan Home RF.
- iv. LAN spectrum penyebaran: beroperasi pada band-band ISM (industrial, scientific, medical) yang tidak memerlukan lisensi.
- v. Gelombang mikro narrowband: beroperasi pada frekuensi gelombang mikro yang tidak termasuk dalam spectrum penyebaran.



Gambar Wi-Fi Internet Connection

TEKNOLOGI WI-FI (NIRKABEL)

Wi-Fi atau wireless fidelity adalah satu standar Wireless Networking, dengan menggunakan komponen yang sesuai, dapat terkoneksi ke jaringan tanpa menggunakan kabel.

Teknologi Wi-Fi memiliki standar yang ditetapkan oleh sebuah institusi internasional yang bernama Institute of Electrical and Electronic Engineers (IEEE), yang secara umum sebagai berikut:

- ▶ Standar IEEE 802.11a yaitu Wi-Fi dengan frekuensi 5 GHz mempunyai kecepatan 54 Mbps, jangkauan jaringan 300 m.
- ▶ Standar IEEE 802.11b yaitu Wi-Fi dengan frekuensi 2,4 GHz mempunyai kecepatan 11 Mbps, jangkauan jaringan 100 m.
- ▶ Standar IEEE 802.11g yaitu Wi-Fi dengan frekuensi 2,4 GHz mempunyai kecepatan 54 Mbps, jangkauan jaringan 300 m
- ▶ Standar IEEE 802.11n yaitu Wi-Fi dengan frekuensi 2,4 GHz atau 5 GHz mempunyai kecepatan 100Mbps s.d 210 Mbps, jangkauan 70 m.

Teknologi Wi-Fi yang akan diimplementasikan adalah standar IEEE 802.11g, karena lebih cepat dalam proses transfer data dengan jangkauan jaringan yang lebih jauh serta dukungan vendor (perusahaan pembuat hardware).

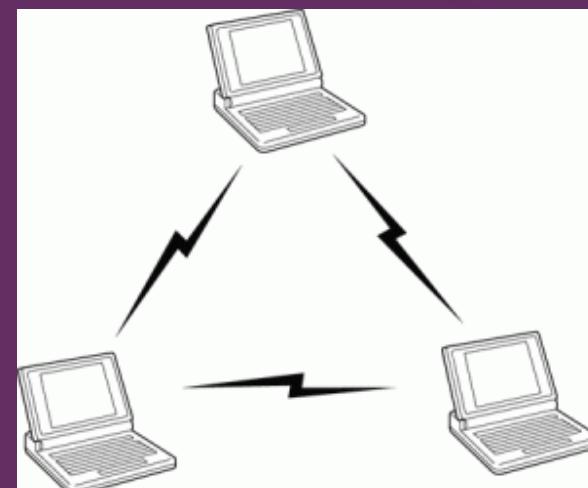
Perangkat ini bekerja di frekuensi 2,4 GHz atau disebut sebagai pita frekuensi ISM (Industrial, Scientific and medical), frekuensi ini juga digunakan oleh peralatan lain, seperti microwave oven, cordless phone, dan Bluetooth.

Tipe Jaringan Wi-Fi

Seperti halnya Ethernet-LAN (Jaringan dengan kabel), Jaringan Wi-Fi juga di konfigurasikan dalam dua jenis jaringan:

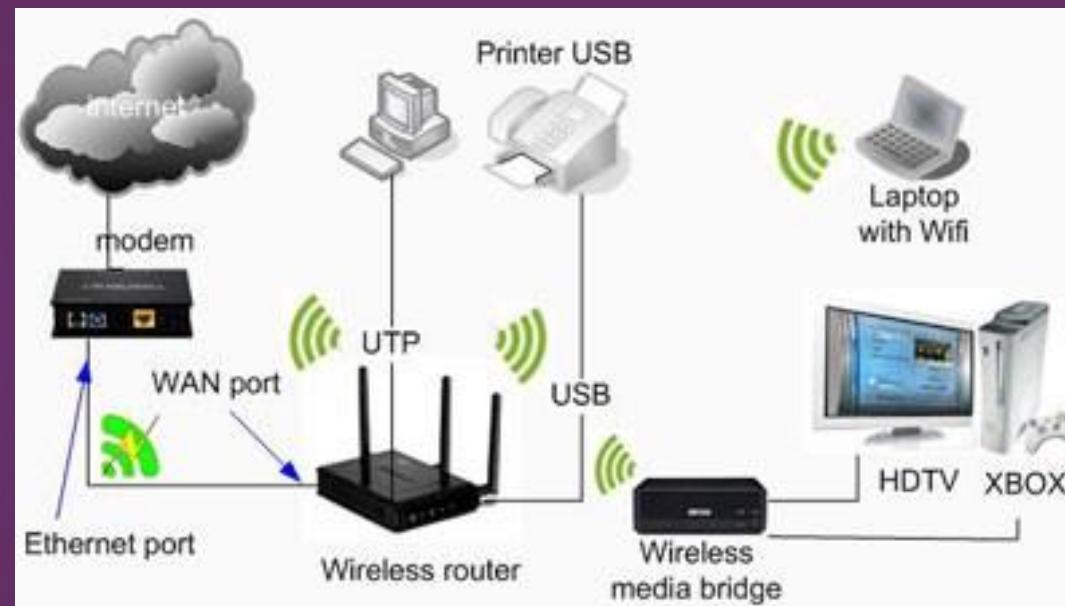
a) **Jaringan peer to peer/Ad hoc Wireless LAN**

Komputer ini juga dapat saling berhubungan berdasarkan nama SSID (Service St Identifier). SSID adalah nama identitas computer yang memiliki komponen wireless.



b) Jaringan Server Based/Wireless Infrastructure

Sistem Infrastructure membutuhkan sebuah komponen khusus yang berfungsi sebagai access point.



► Keamanan Jaringan Wi-Fi

Pancaran sinyal yang ditransmisikan pada Jaringan Wi-Fi menggunakan frekuensi secara bebas, sehingga dapat ditangkap oleh computer lain sesama user Wi-Fi.

Untuk mencegah user yang tidak berhak masuk ke dalam jaringan, maka ditambahkan system pengamanan misalnya WEP (Wired Equivalen Privacy). Jadi user tertentu yang telah mempunyai otoritas saja yang dapat menggunakan sumber daya jaringan Wi-Fi.



Keamanan jaringan W-Fi secara umum terdiri dari :

- Non secure/Open : Komputer yang memiliki Wi-fi dapat menangkap transmisi pancaran dari sebuah Wi-Fi dan langsung dapat masuk ke dalam jaringan tersebut.
- Share Key : untuk dapat masuk ke jaringan Wi-Fi di perlukan kunci atau password, contohnya sebuah network yang menggunakan WEP.

Cara lain agar jaringan Wi-Fi dapat berjalan dengan baik dan aman, antara lain:

- ▶ Membeli access point dengan fasilitas password bagi administratornya sehingga user tidak dapat dengan mudah mengacak-acak jaringan.
- ▶ Selain menggunakan WEP, dapat ditambahkan WPA (Wi-Fi Protected Access)
- ▶ Membatasi akses dengan mendaftarkan MAC address dari computer klien yang berhak mengakses jaringan.

KEUNGGULAN WI-FI

- Biaya pemeliharaan murah
- Infrastruktur berdimensi kecil
- Pembangunannya cepat
- Mudah dan murah untuk di relokasi
- Mendukung portabilitas

KELEMAHAN

- Biaya peralatan mahal
- Delay yang sangat besar
- Kesulitan karena masalah propagasi radio
- Mudah untuk terinterferensi
- Kapasitas jaringan karena keterbatasan spectrum(pita frekuensi yang tidak dapat diperlebar)
- Keamanan/kerahasiaan data kurang terjamin

PROTOKOL JARINGAN



Protokol adalah aturan yang ditetapkan dalam melakukan komunikasi data.

Protokol mendefinisikan :

1. Apa yang dikomunikasikan ?
2. Bagaimana cara berkomunikasinya ?
3. Kapan dilakukan komunikasi ?

I. TCP/IP (Transmission Control Protocol/Internet Protocol)

Protokol yang digunakan secara luas pada jaringan karena merupakan protokol transportasi yang paling fleksibel dan dapat digunakan pada area yang luas.

2. IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange)

Jenis protocol yang digunakan terutama oleh sistem dari Novell Netware yang disusun kembali oleh Microsoft dan diimplementasikan di Window NT dengan nama NWLink.

3. UDP (User Diagram Protocol)

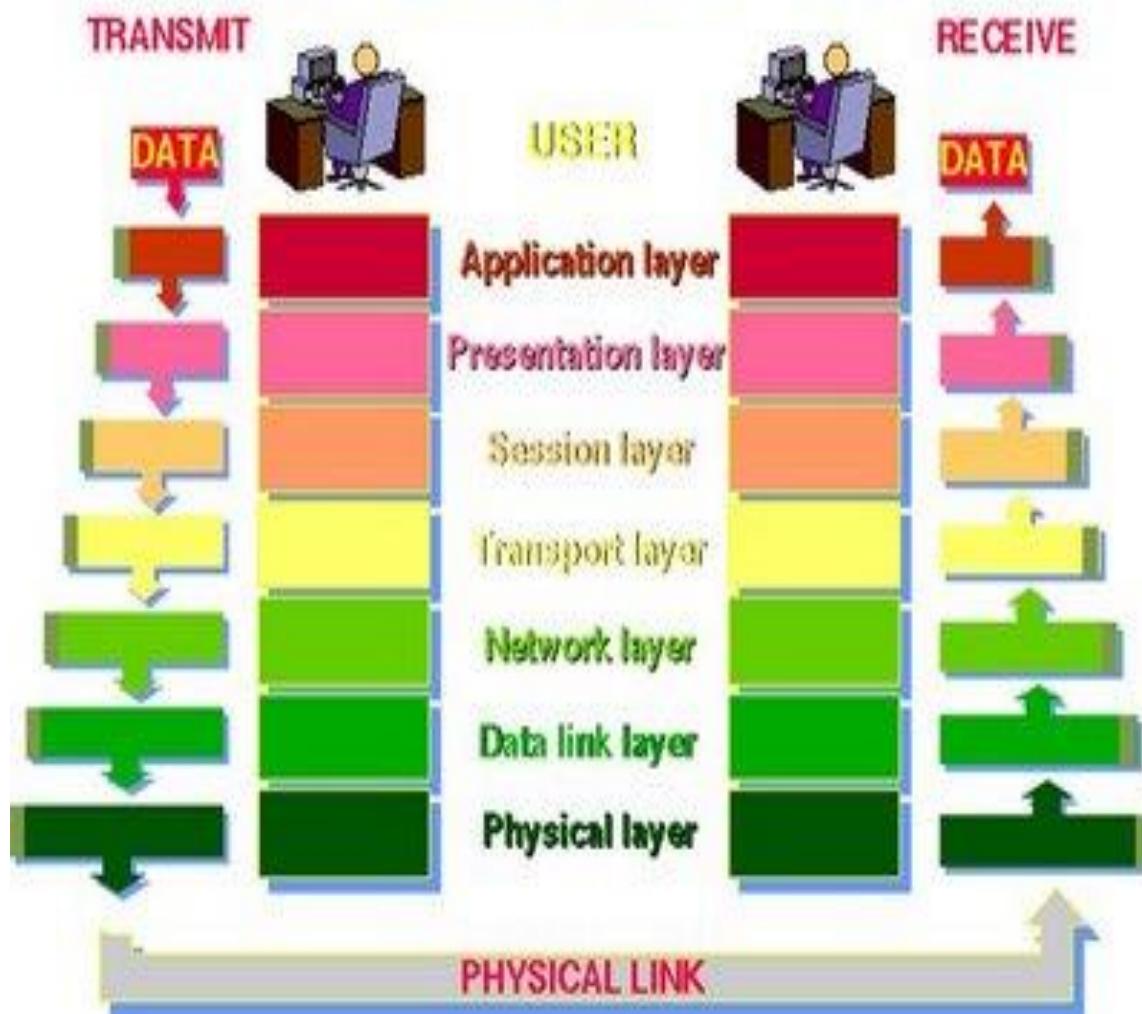
Dalam layanan protokolnya menggunakan service tranmisi data yang sedikit sekali. Sering kali UDP tidak melakukan pengecekan pada paket-paket data. UDP tidak menjamin paket-paket data akan sampai pada tujuannya atau tidak.

4. Apple Talk

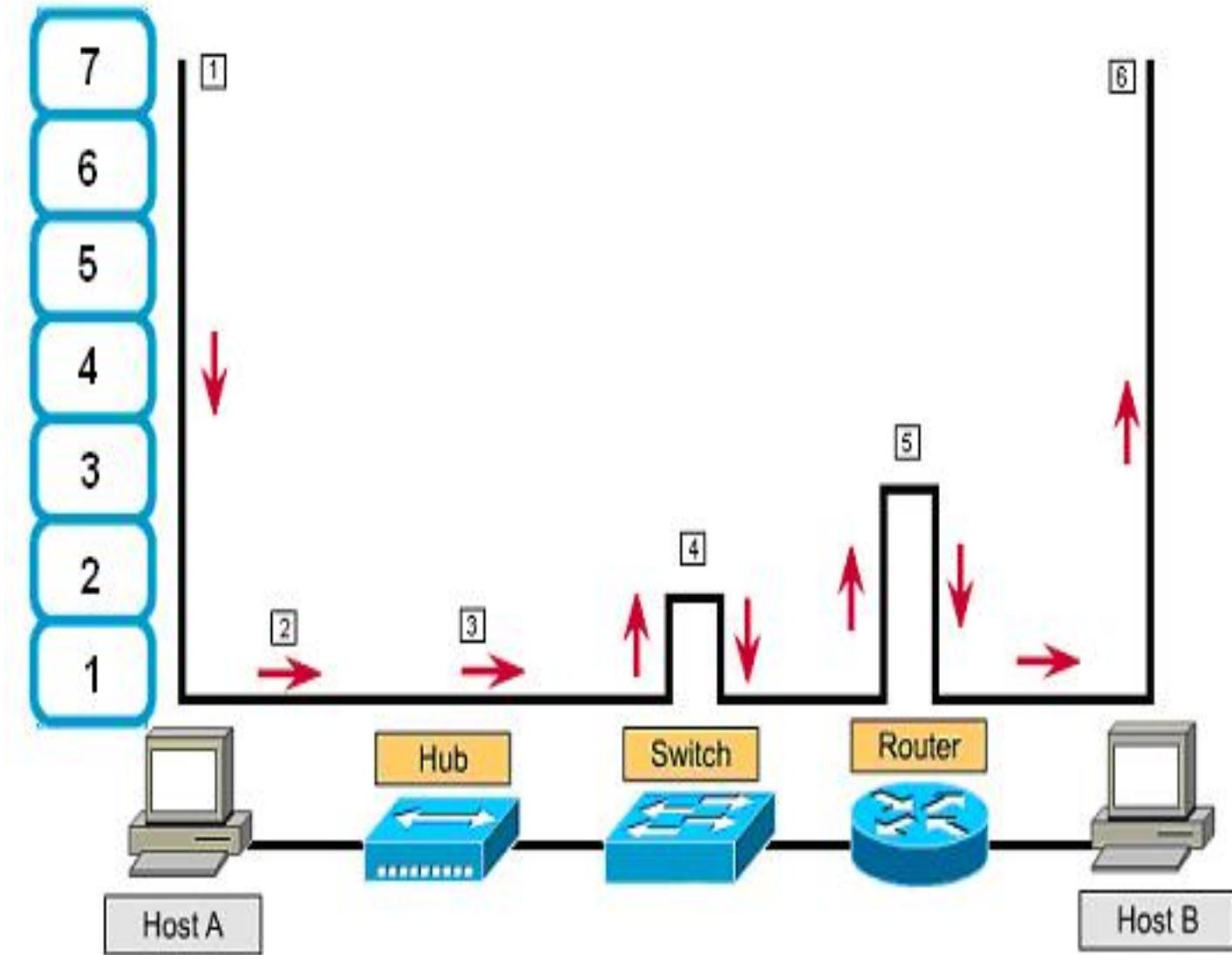
Protokol yang digunakan pada komputer Apple Mac OS

Model OSI

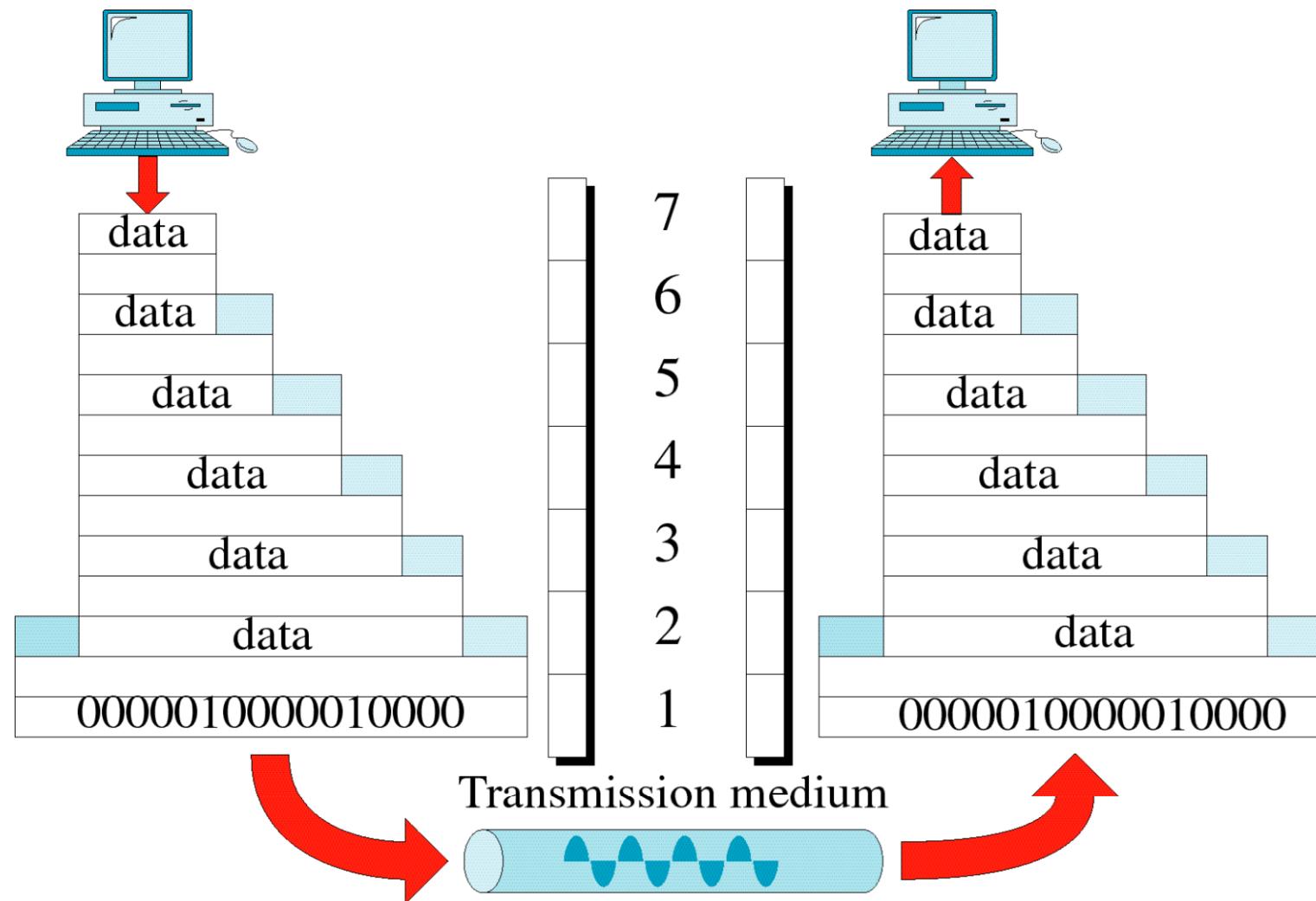
Open System Interconnection



OSI Layer



OSI



Enkapsulasi

Enkapsulasi adalah suatu proses untuk menyembunyikan atau memproteksi suatu proses dari kemungkinan interferensi atau penyalahgunaan dari luar sistem sekaligus menyederhanakan penggunaan sistem itu sendiri, juga membuat satu jenis paket data jaringan menjadi jenis data lainnya. Enkapsulasi terjadi ketika sebuah protokol yang berada pada lapisan yang lebih rendah menerima data dari protokol yang berada pada layer yang lebih tinggi dan meletakkan data ke format data yang dipahami oleh protokol tersebut. Akses ke internal sistem diatur sedemikian rupa melalui seperangkat interface.

Dengan enkapsulasi data menjadi memiliki identitas.

Contoh sederhana proses enkapsulasi dalam proses pengiriman surat, jika sebuah surat akan dikirim namun tanpa adanya amplop, alamat dan perangko. Surat tersebut hendaknya memiliki identitas agar dapat sampai ke tujuan, jika tidak memiliki identitas maka surat tersebut tidak akan dapat sampai ke tujuan. Amplop dengan alamat dan perangko sama dengan enkapsulasi pada data.

Proses enkapsulasi berbeda-beda dalam tiap layernya, berikut prosesnya :

Awalnya data dibuat, ketika memulai proses pengiriman, data turun melalui **Application layer (layer 7)** yang bertanggung jawab dalam pertukaran informasi dari komputer ke jaringan, pada dasarnya layer ini merupakan interface antara jaringan dengan aplikasi yang digunakan user.

Dapat juga disebut bahwa layer ini berfungsi untuk mendefinisikan request dari user.

Kemudian data diteruskan ke **layer Presentation (layer 6)**, yang mana layer ini bertanggung jawab dalam menentukan apakah ia perlu untuk melakukan enkripsi terhadap request ini ataupun ke bentuk lain dari translasi data. Jika proses sudah lengkap, selanjutnya ditambahakan informasi yang diperlukan

Kemudian di forward ke **Session layer (layer 5)** yang mana layer ini akan memeriksa apakah aplikasi merequest suatu informasi dan memverifikasi layanan yang direquest itu pada server.

Setiap informasi yang akan dilewatkan ditambahkan header setiap turun 1 layer . Namun, pada pemrosesan layer 5, 6 dan 7 terkadang tidak diperlukan adanya header. Ini dikarenakan tidak ada informasi baru yang perlu diproses.

Sampailah data di **Transport layer (layer 4)**, memastikan bahwa ia mempunya suatu koneksi yang sudah tepat dengan server dan memulai proses dengan mengubah informasi itu ke bentuk segment. Pengecekan error dan penggabungan data yang berasal dari aplikasi yang sama dilakukan di layer transport ini serta keutuhan data di jamin pula di sini.

Terbentuk L4PDU dari proses ini.

Selanjutnya segment tersebut diteruskan ke **Network layer (layer 3)**, disini diterima segment-segment tadi dan ditambahkan alamat network untuk station yang merequest dan alamat network untuk server yang direquest.

Segment-segment tersebut akan diubah menjadi packet-packet, Kemudian layer Network membuat header Network, dimana didalamnya terdapat juga alamat layer Network, dan ditempatkan L4PDU dibaliknya, dan terbentuklah **L3PDU**.

Kemudian packet-packet tadi dilewatkan ke **layer Data Link (layer 2)** dan paket-paket tadi diatur dan kemudian akan dibungkus lagi ke dalam individual frame, salah satu contoh dalam proses ini adalah memberikan alamat MAC tujuan dan MAC address sumber yang kemudian informasi tersebut digunakan untuk membuat trailer.

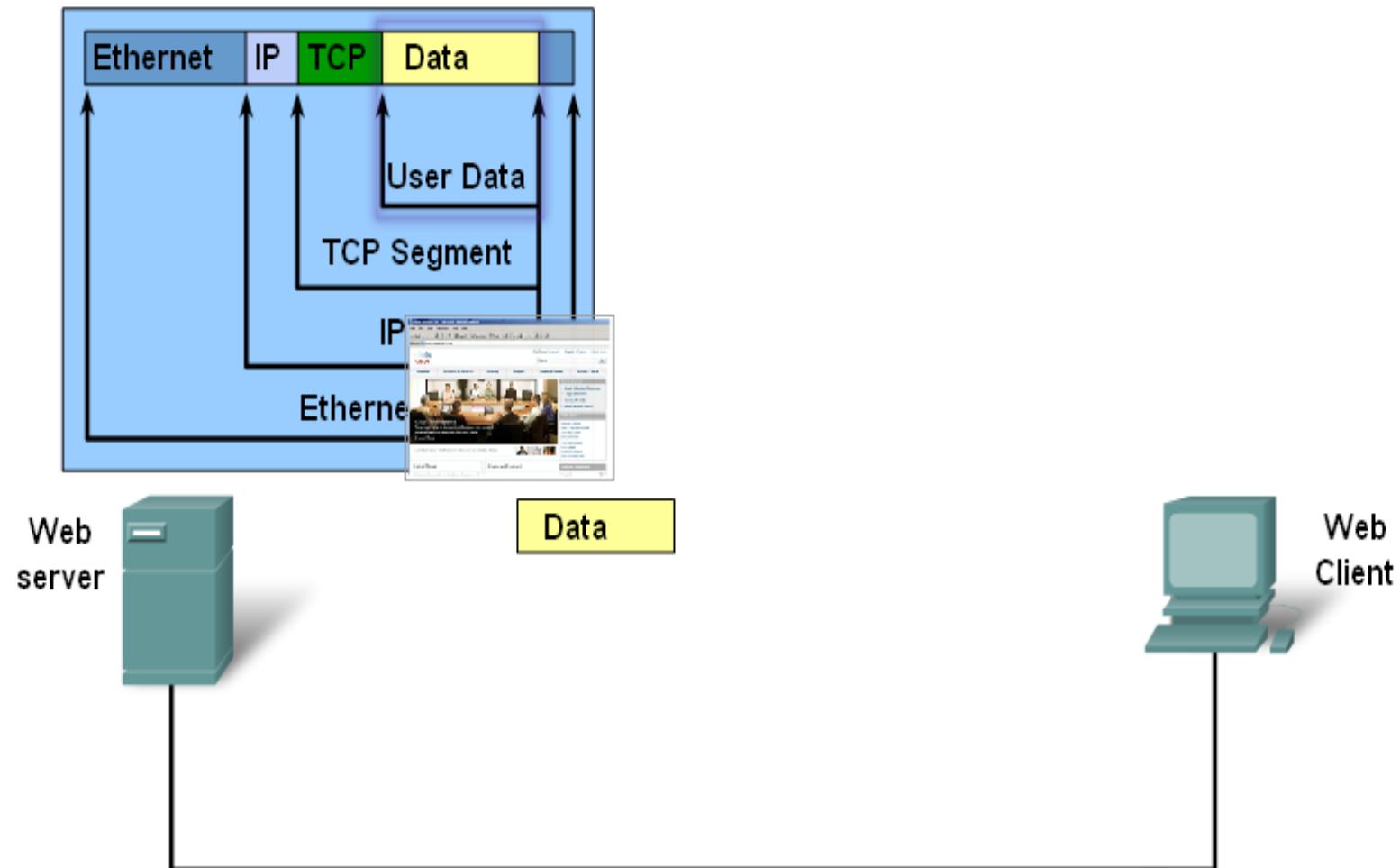
Dikarenakan suatu paket dapat dikirimkan melalui banyak sekali perangkat dan router, disinilah peran MAC Address dalam mengirimkan paket antara satu router dan router lainnya. Kemudian akan ditransmisikan ke media.

Seluruh informasi yang ditambahkan oleh tiap layer sebelumnya (sebagai suatu actual file request) harus cocok ke dalam ukuran 46-1500 byte data field pada frame ethernet . Data link layer bertanggung jawab untuk mengirimkan frame menurut topologi yang digunakan. Terbentuklah **L2PDU** pada proses ini.

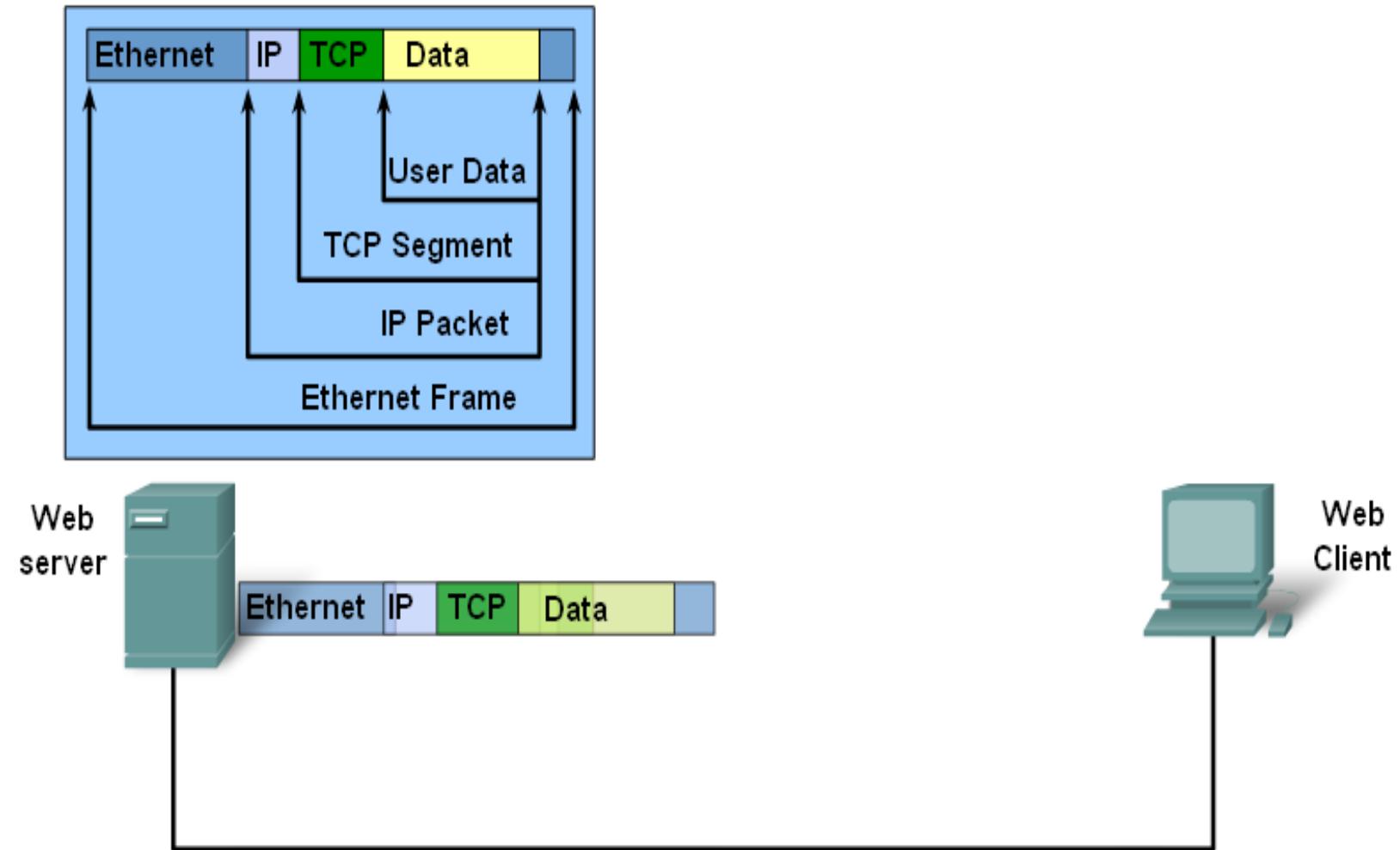
Terakhir, sampailah data di **layer Physical (layer I)**, informasi akan dibawa dari source menuju destination. Karena Physical layer tidak mengenal frame, ia akan melewatkannya informasi itu ke bentuk bits. Tidak terjadi penambahan header pada layer ini. Layer Physical ini berhubungan dengan perangkat keras. Akhirnya bit-bit tersebut nantinya akan disinkronisasi dan kemudian diubah menjadi sinyal listrik yang berupa tinggi rendahnya tegangan dan selanjutnya ditransmisikan melalui media. Misalnya dari kabel ke tujuan, hal ini sesuai dengan karakteristik lapisan Physical layer yang menentukan rangkaian kejadian dimana arus bit berpindah melalui medium fisik.

Pada tiap layer terdapat LxPDU (Layer N Protocol Data Unit), dimana merupakan bentuk dari byte pada header-trailer pada data. PDU merupakan proses-proses pada setiap layer dari model OSI. Pada tiap-tiap layer juga terbentuk bentukan baru, pada layer 2 PDU termasuk header dan trailer disebut bentukan frame. Pada layer 3 disebut paket (packet). Sedangkan pada layer 4 disebut segmen (segment).

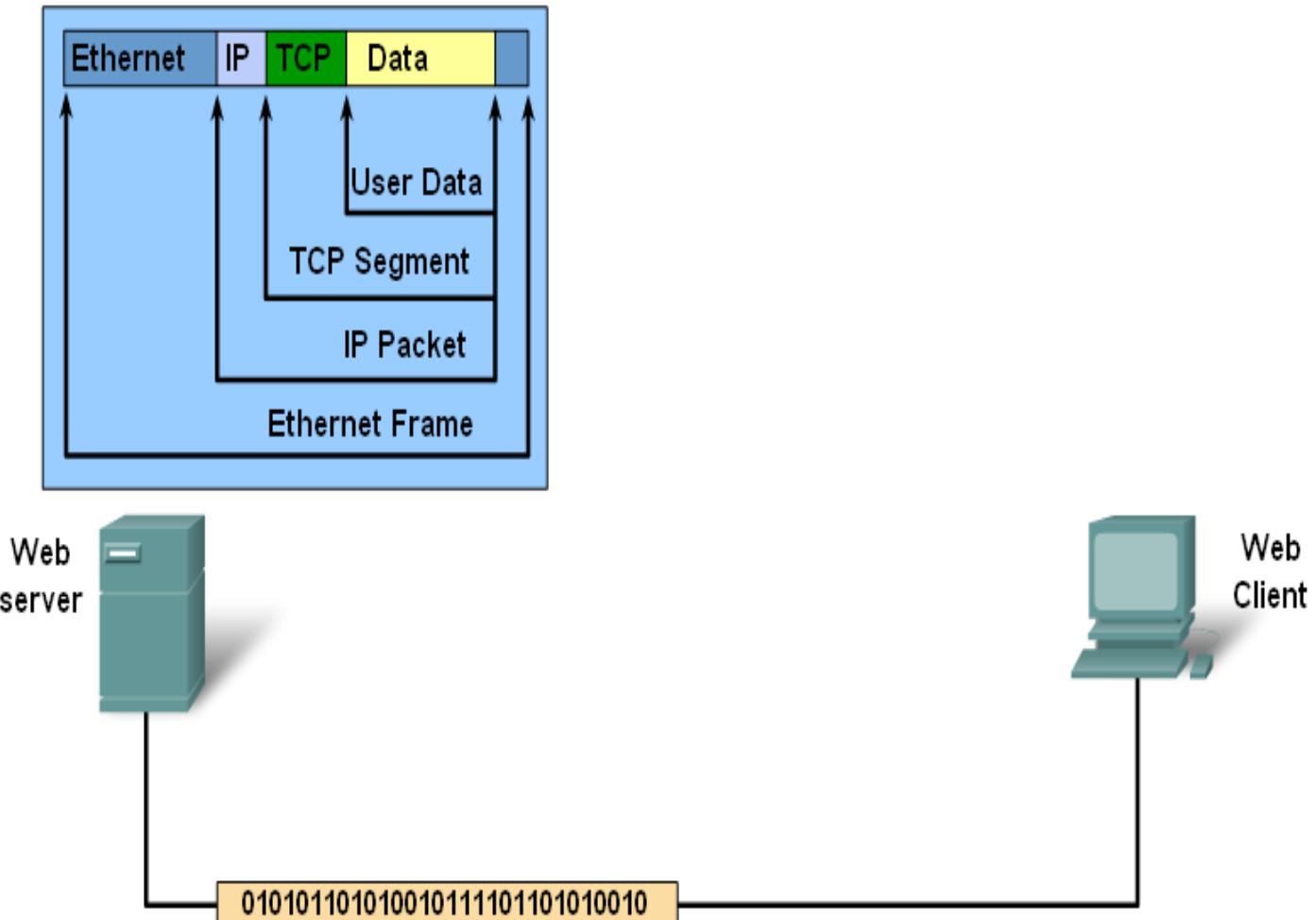
Encapsulasi



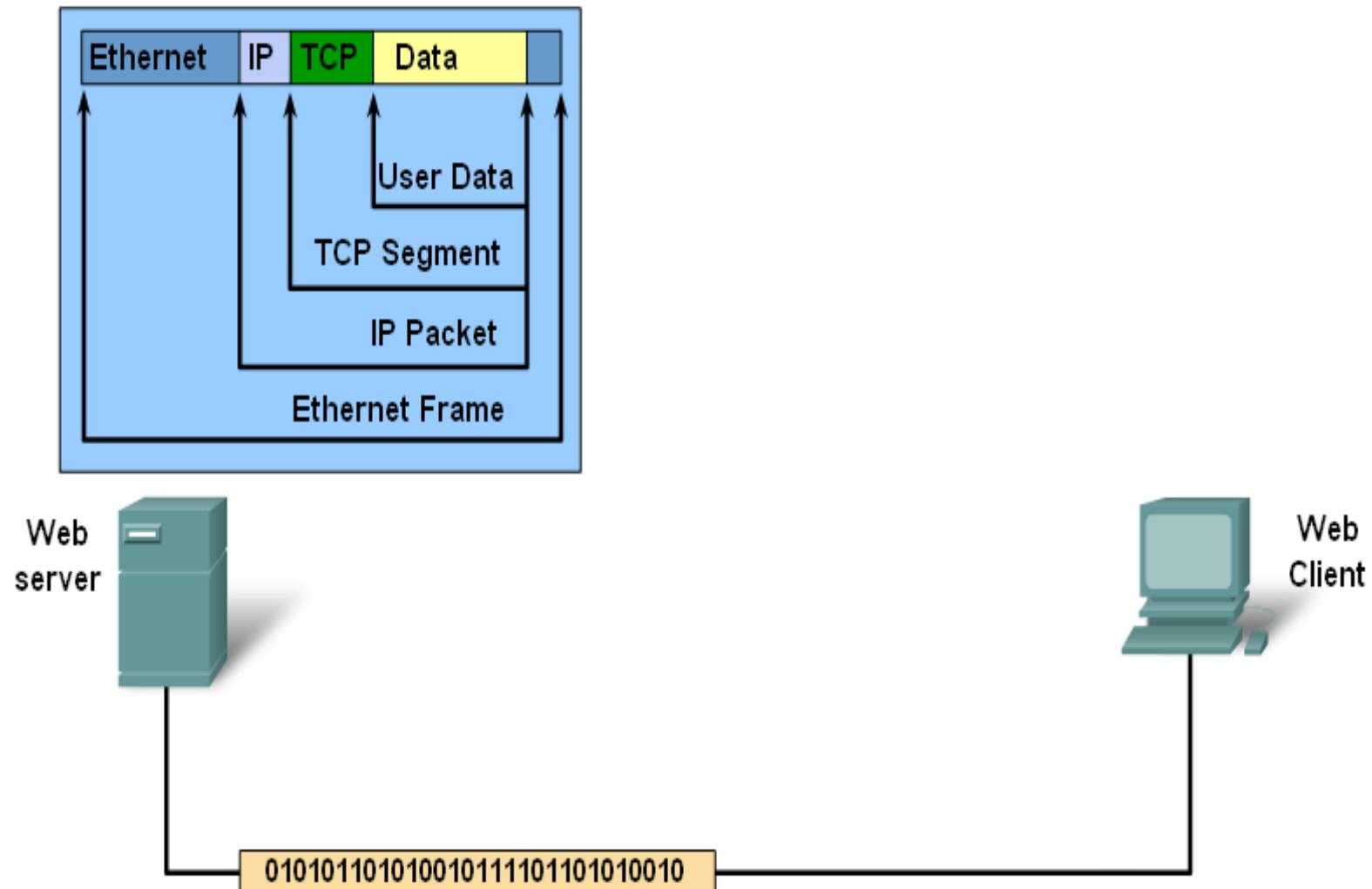
Encapsulasi

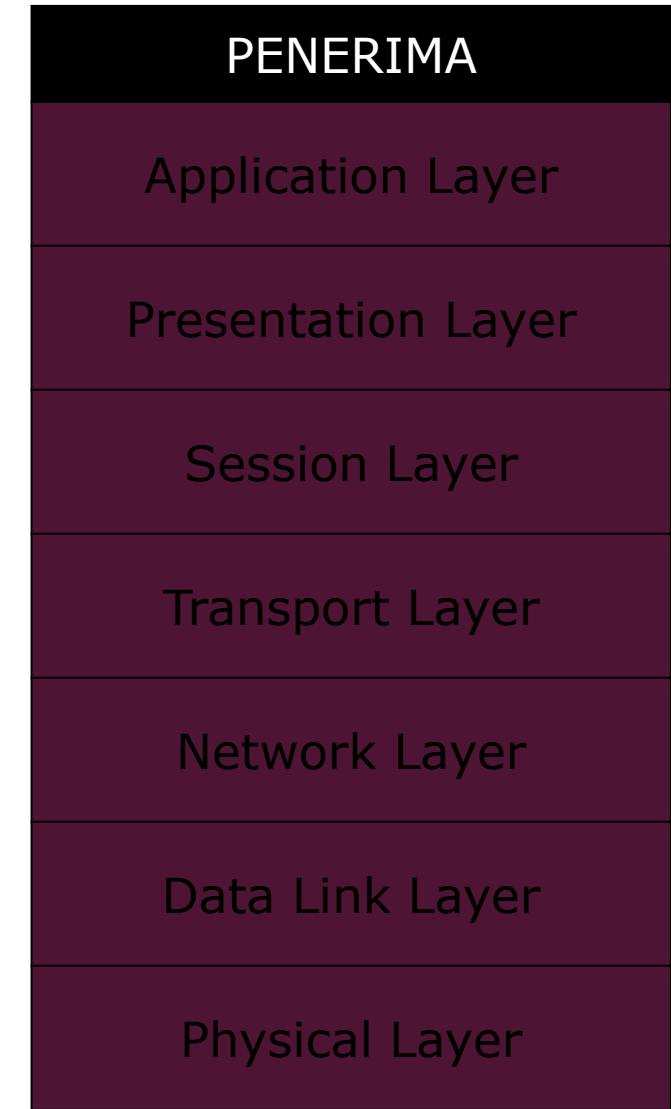
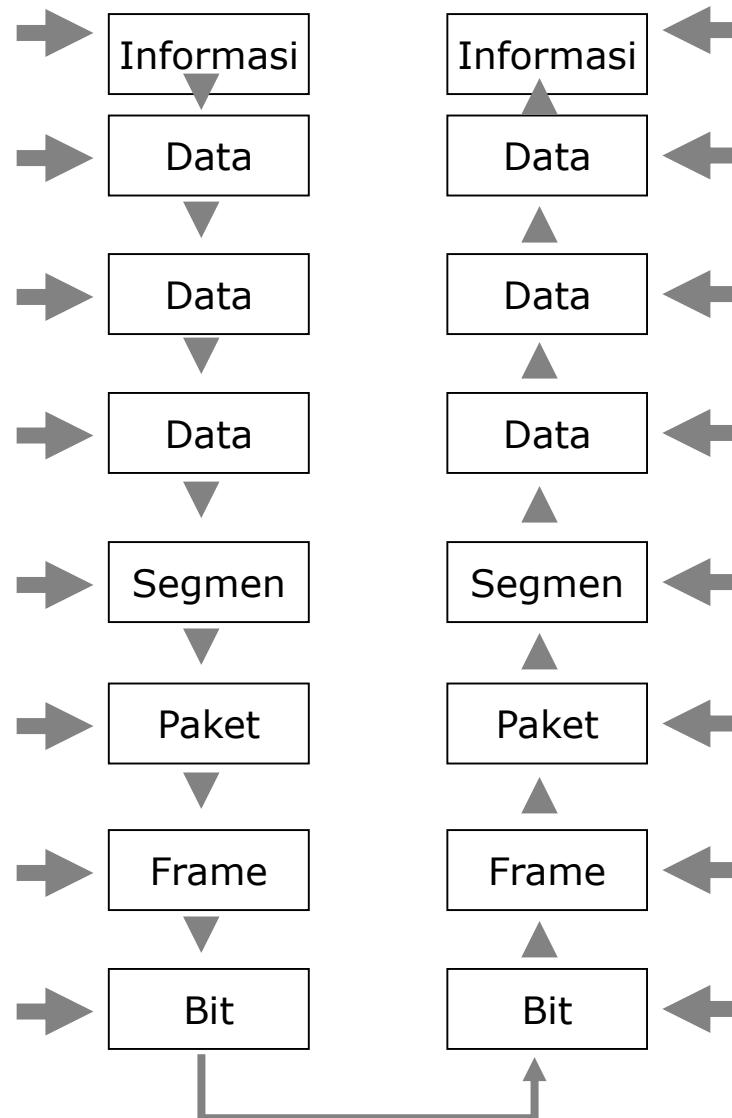
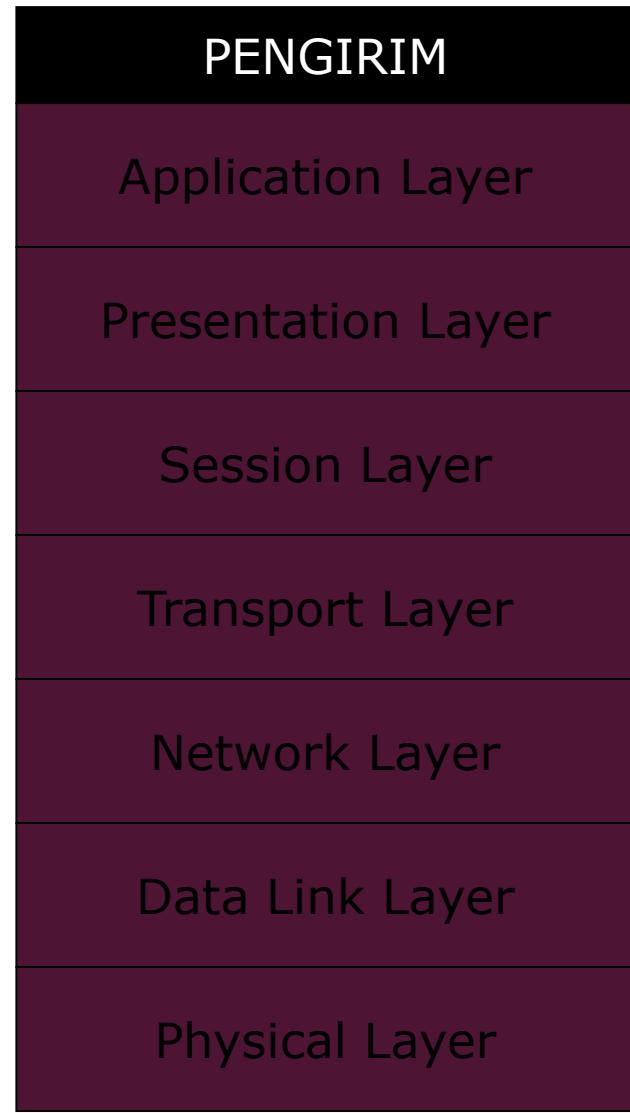


Encapsulasi



Encapsulasi





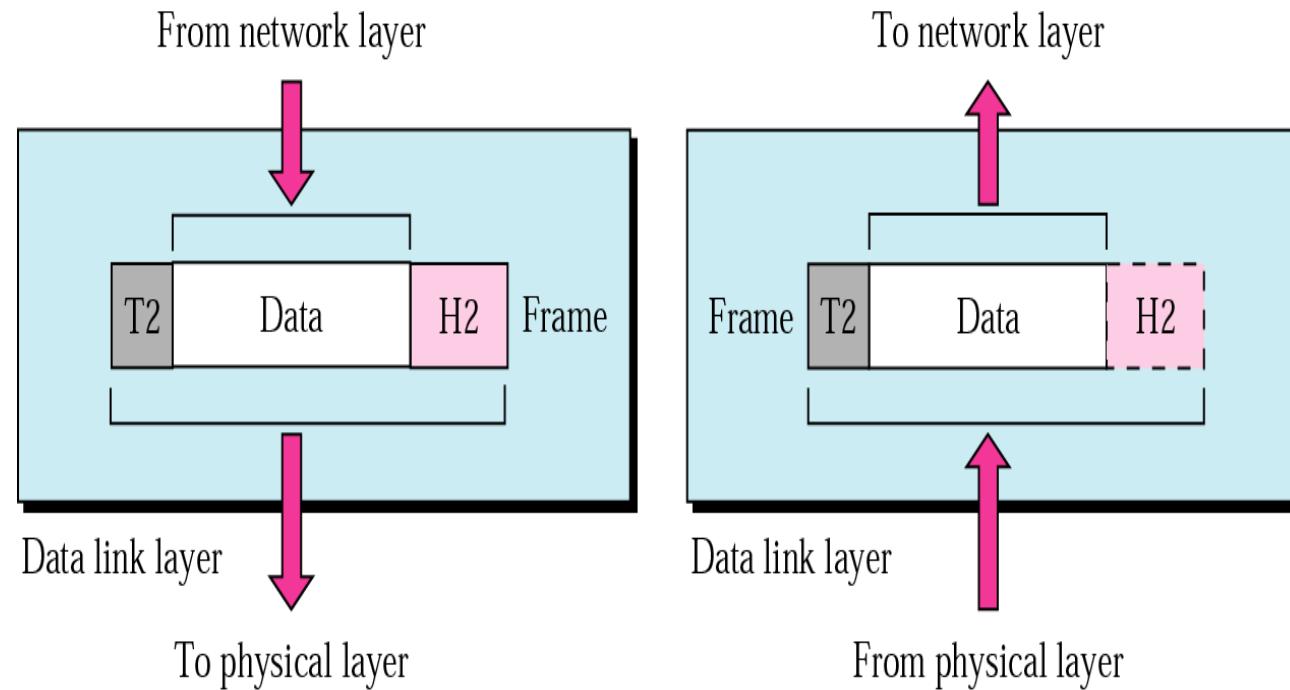
Lapisan Fisik

- Bertanggung jawab: mengkoordinasi fungsi yang dibutuhkan untuk mengirimkan serangkaian bit melewati media fisik.
- Tugasnya adalah menentukan :
 - Karakteristik fisik antarmuka dan media
 - Representasi bit
 - Data rate
 - Sinkronisasi bit

Lapisan Data Link

- Bertanggung jawab pada pengantaran (delivery) dari satu titik ketitik yang lain dan memastikan data bebas dari error.
- Tugasnya adalah menentukan :
 - Framing
 - Pengalaman Fisik
 - Kendali aliran
 - Kendali kesalahan
 - Kendali akses

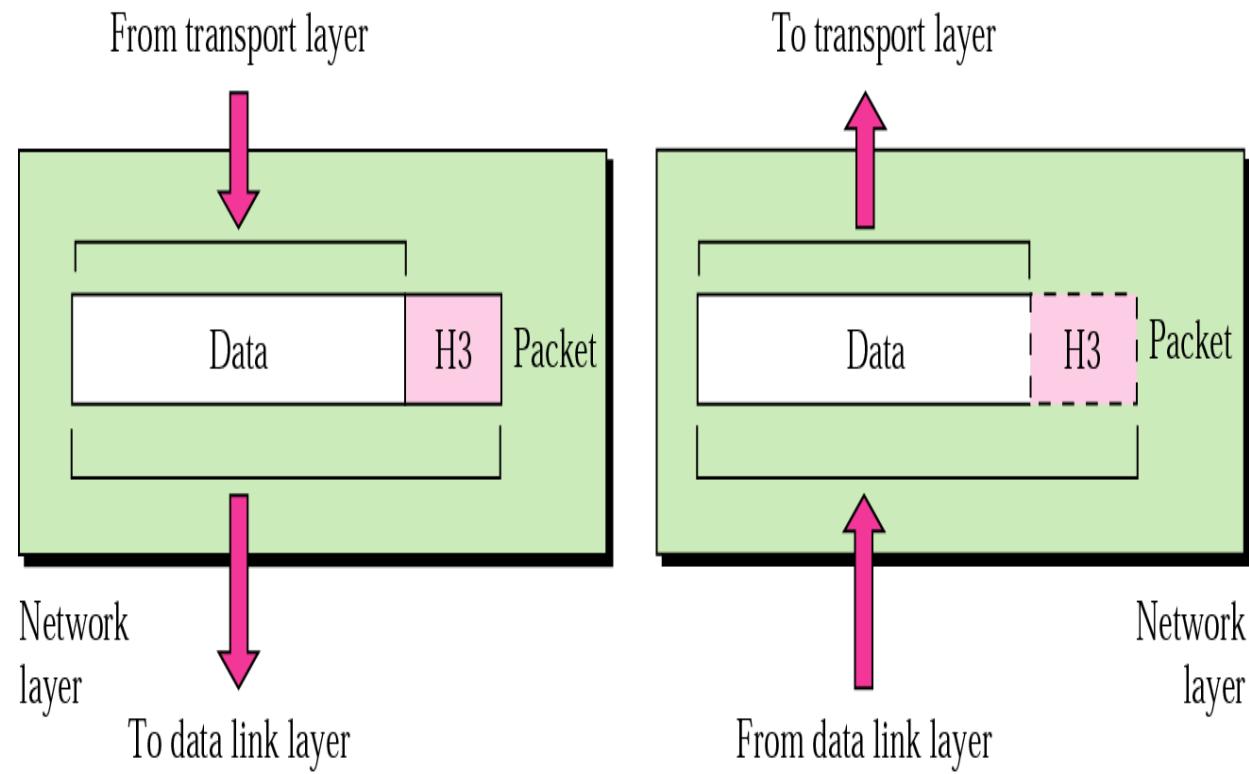
Lapisan Data Link



Lapisan Jaringan

- Bertanggung jawab pada pengantaran/delivery paket data dari sumber ke tujuan
- Tugas lapisan ini berkaitan dengan :
 - Pengalaman logika
 - Routing

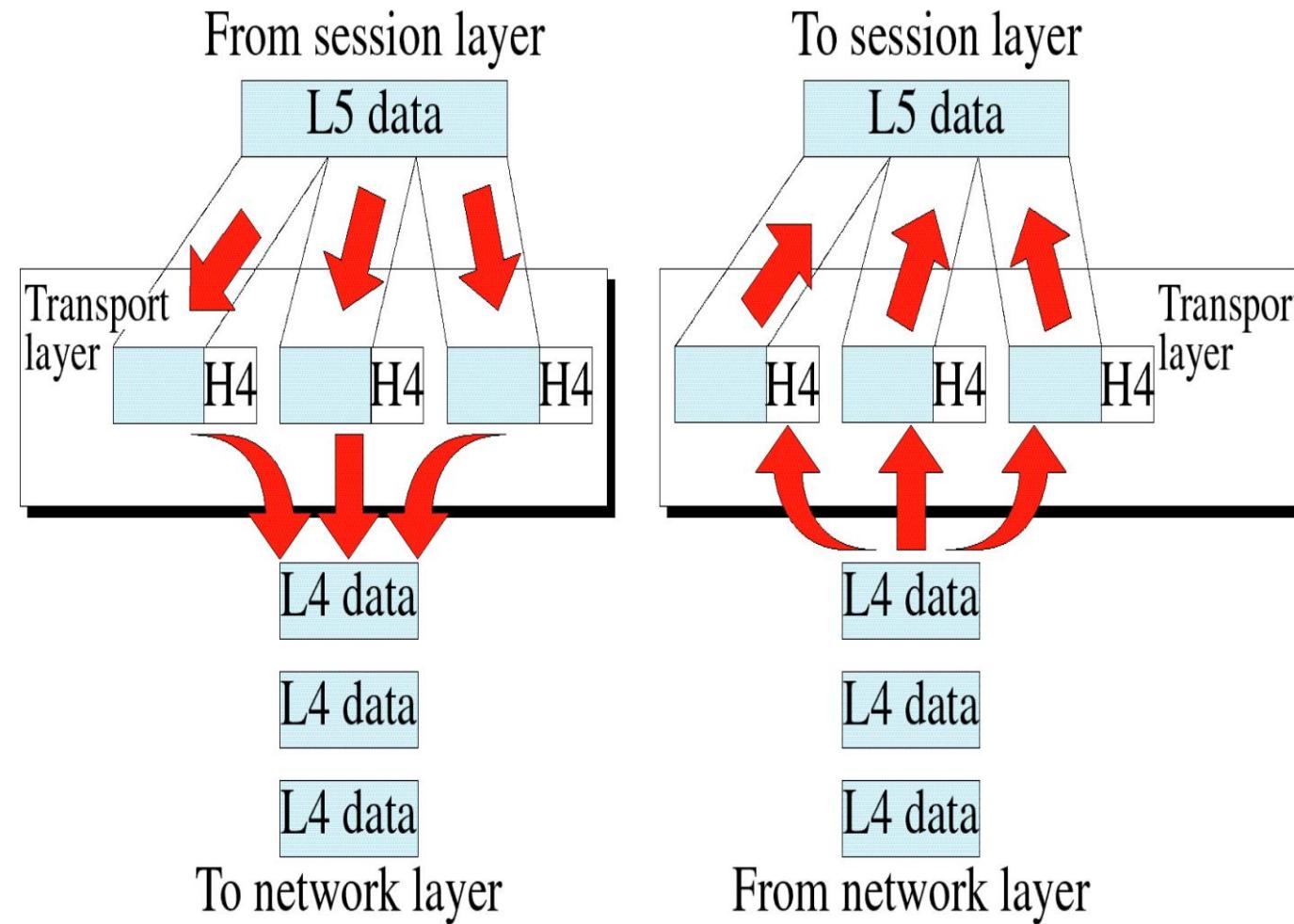
Lapisan Jaringan



Lapisan Transport

- Bertanggung jawab pada pengantaran seluruh pesan (meyakinkan paket sampai dengan urutan yang benar)
- Tugasnya berkaitan dengan :
 - Service-point addressing
 - Segmentation and reassembly
 - Connection control
 - Flow control
 - Error control

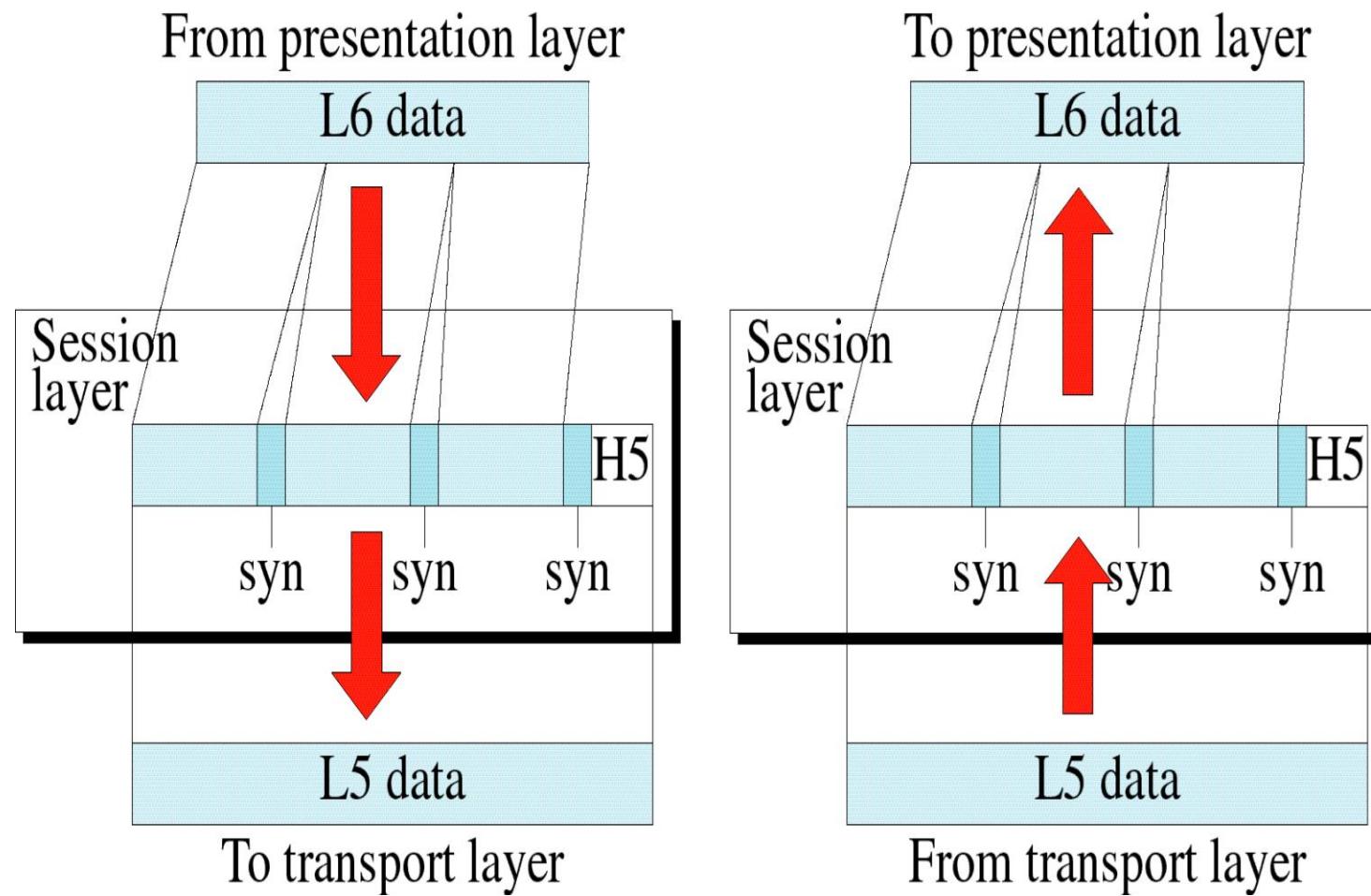
Lapisan Transport



Lapisan Session

- Bertanggung jawab: network dialog controller (membangun, merawat dan mensinkronkan interaksi antara sistem yang berkomunikasi)
- Tugas lapisan ini berkaitan dengan :
 - Kendali dialog
 - Sinkronisasi

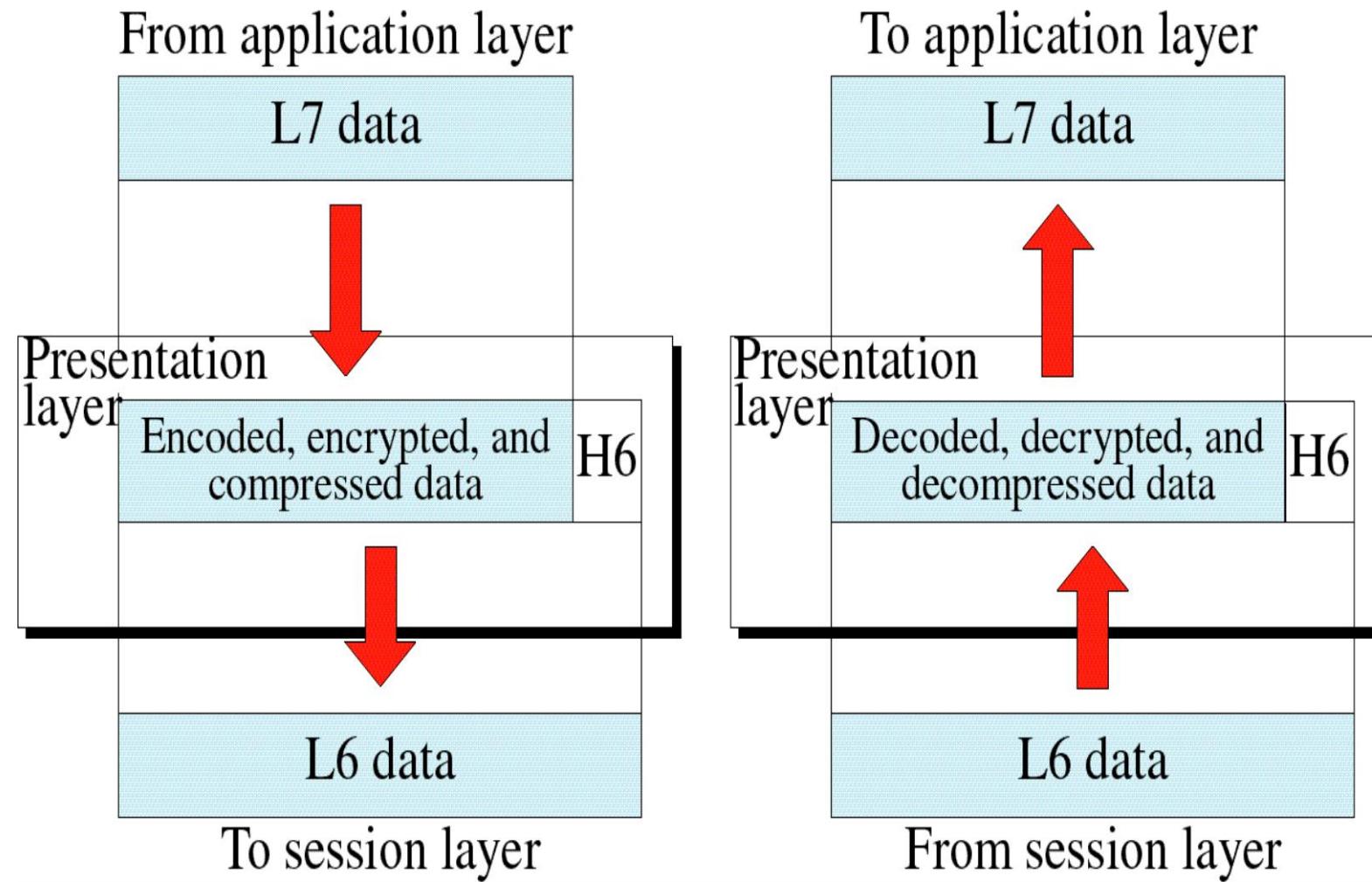
Lapisan Session



Lapisan Presentasi

- Berkaitan erat dengan sintaks dan semantik dari pertukaran informasi antara dua sistem
- Tugas lapisan ini berkaitan dengan :
 - Translasi
 - Enkripsi
 - Kompresi

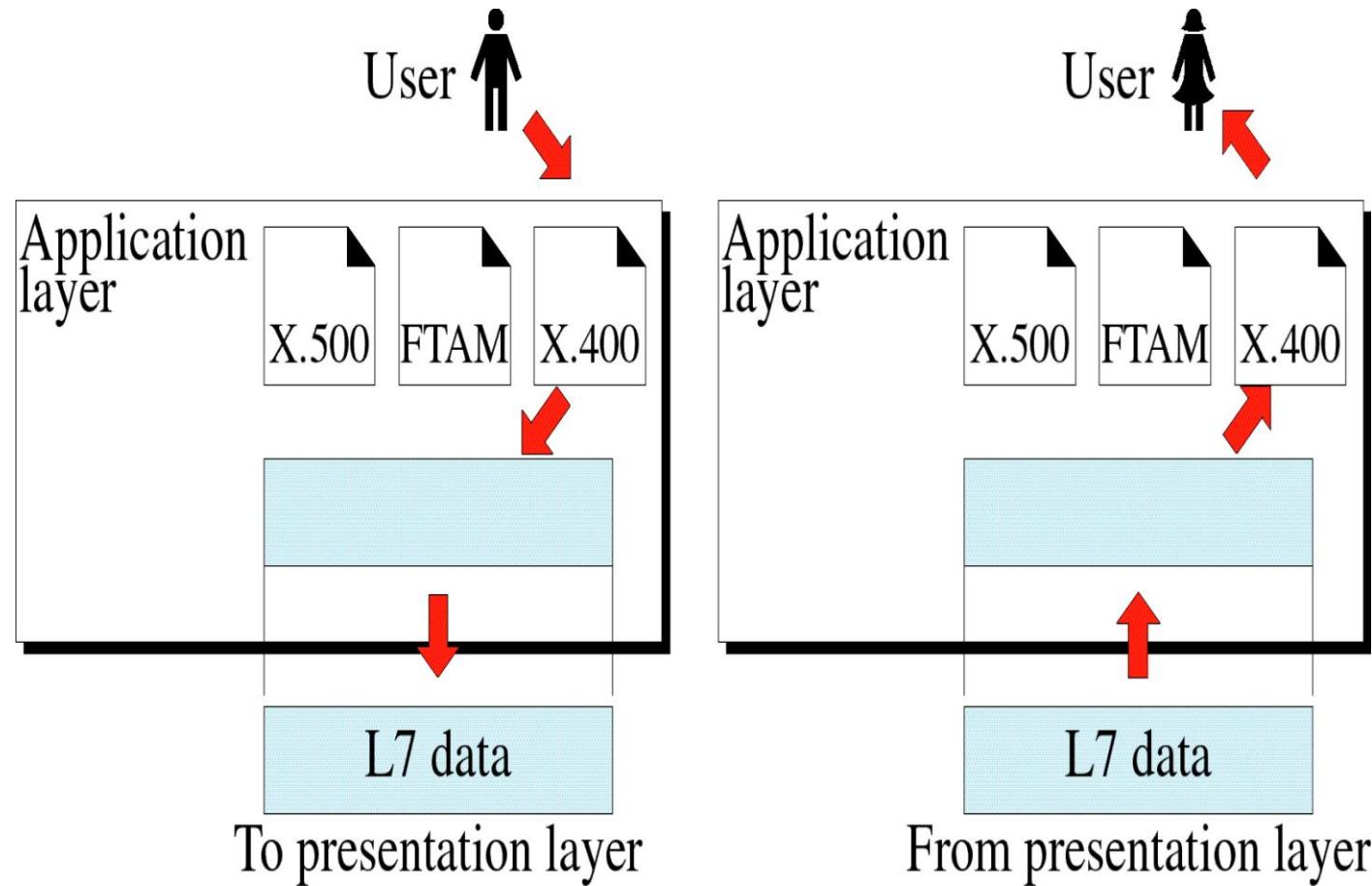
Lapisan Presentasi



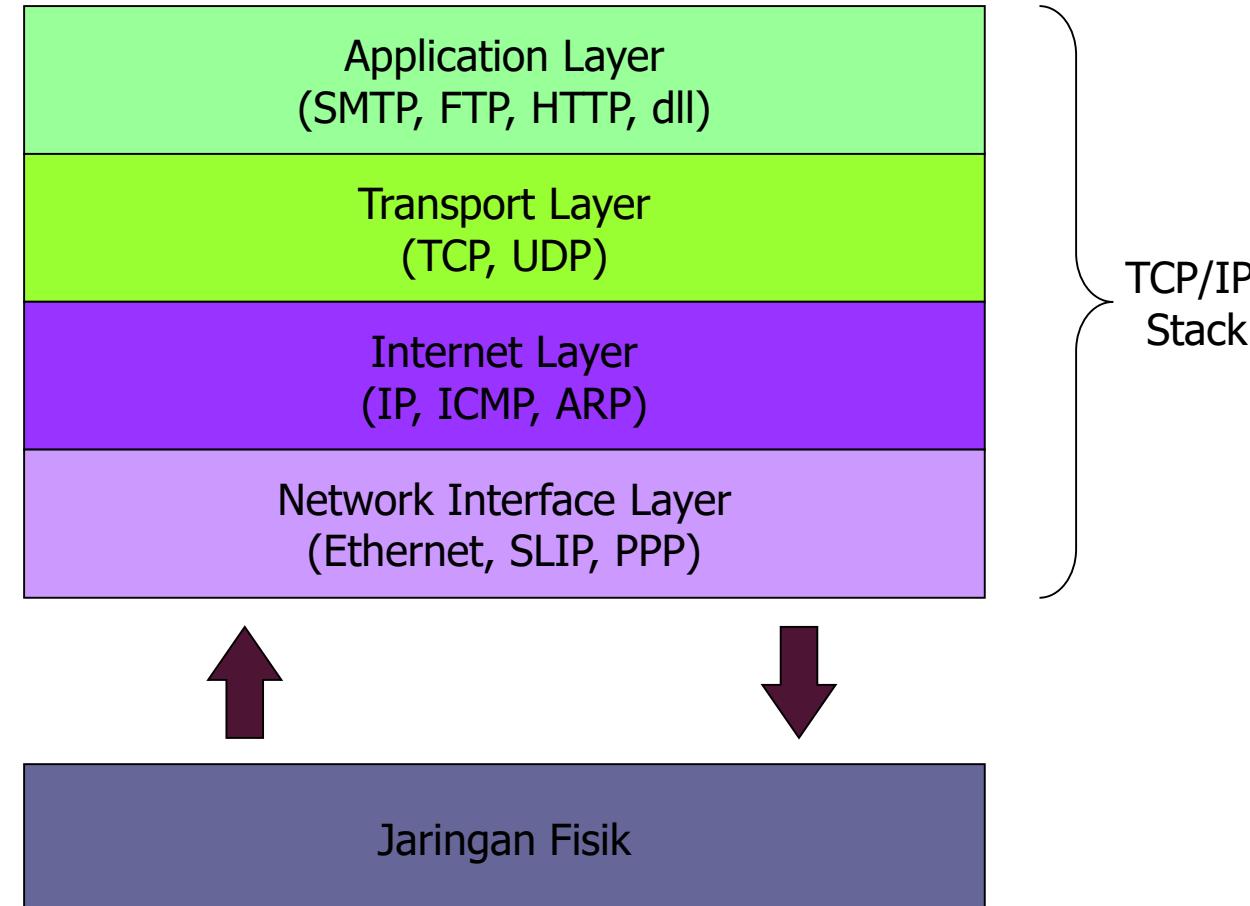
Lapisan Aplikasi

- Lapisan aplikasi memungkinkan user (manusia atau software) untuk mengakses jaringan.
- Tugas lapisan ini berkaitan dengan :
 - Network virtual terminal
 - File transfer and management
 - Mail services
 - Directory services

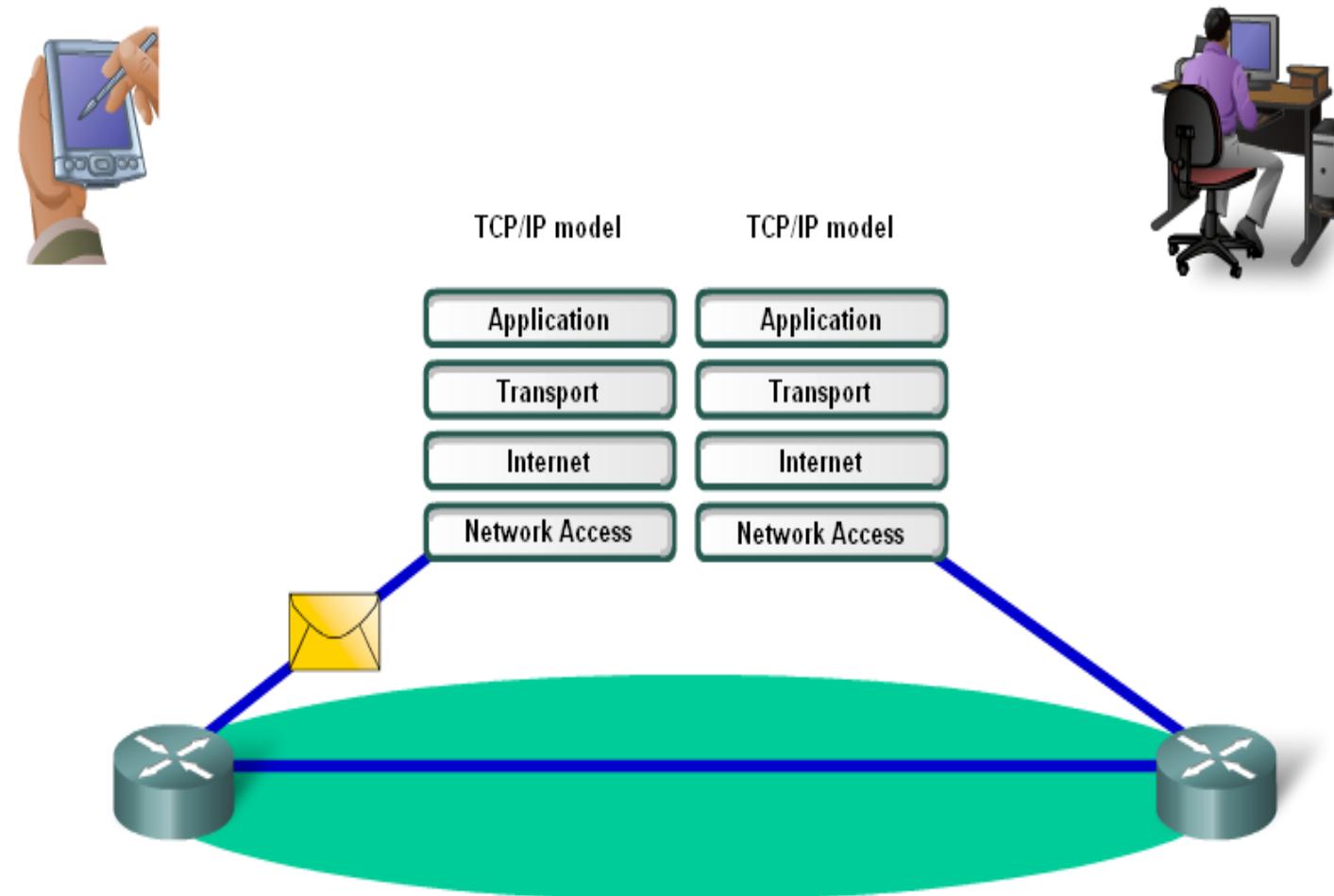
Lapisan Aplikasi



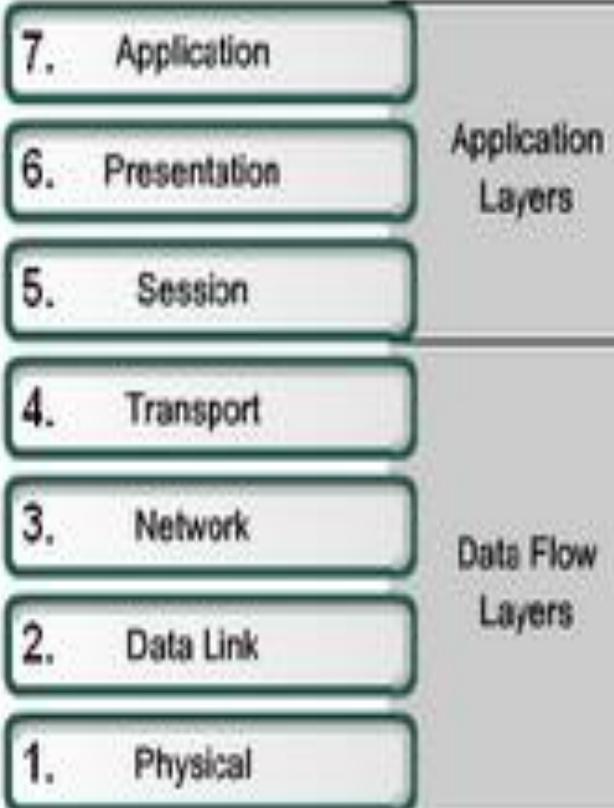
Arsitektur TCP/IP



Arsitektur TCP/IP



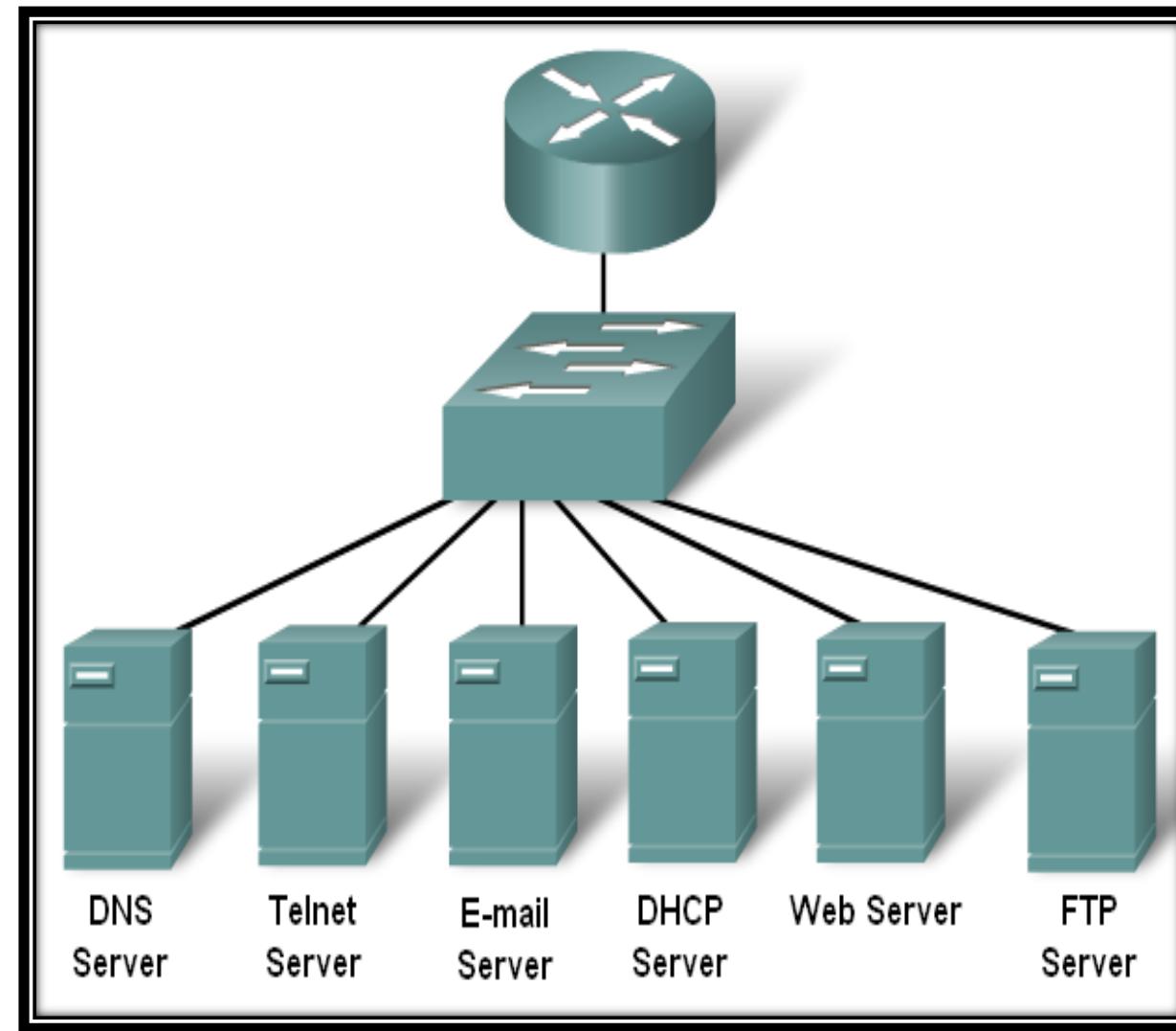
OSI Model



TCP/IP Model

Domain Name System
HyperText Transfer Protocol
Simple Mail Transfer Protocol
Post Office Protocol
Dynamic Host Configuration Protocol

TCP/IP Protokol





KEAMANAN JARINGAN

Pendekatan keamanan komputer yang umum dilakukan meliputi:

1. Identifikasi apa yang ingin diproteksi
2. Tentukan dari apakah ia diproteksi
3. Tentukan seperti apakah serangan yang akan terjadi
4. Tentukan ukuran proteksi keseluruhan aset dalam bentuk ukuran biaya yang efektif
5. Amati keseluruhan proses secara terus menerus dan perbaiki bila ditemukan kelemahan

Dalam merancang keamanan komputer seringkali perlu dipertimbangkan beberapa pilihan-pilihan berikut:

1. **Pilih service atau keamanan service.** Setiap service mempunyai resiko keamanan. Bila keuntungan yang diperoleh dari adanya service tersebut lebih kecil dari resiko keamanannya maka lebih baik service itu tidak dipergunakan daripada harus memproteksi service.
2. **Pilih kemudahan atau keamanan.** Sistem komputer yang paling mudah digunakan adalah yang memberikan akses apasaja bagi penggunanya tanpa penggunaan password. Penggunaan password memang akan sedikit menyulitkan namun akan meningkatkan keamanan. Penggunaan one-time password akan lebih menyulitkan namun akan lebih meningkatkan keamanan
3. **Pilih biaya keamanan atau resiko kehilangan.** Biaya yang dipertimbangkan misalnya biaya dalam pengertian sebenarnya (untuk pembelian firewall dsb), kinerja (penambahan fitur keamanan akan menambah waktu proses dan mengurangi kinerja), dan kemudahan pemakaian. Sedangkan dari sisi resiko kehilangan adalah kehilangan privacy, data, dan service.

Analisis Resiko (*Risk Analysis*)

Langkah pertama dalam melakukan analisis resiko adalah **identifikasi aset**. Aset tidak terbatas hanya pada perangkat keras dan lunak serta data, namun juga dokumentasi, suplies, dan bahkan orang yang terlibat dalam lingkungan jaringan komputer. Tujuan keamanan untuk setiap aset di atas adalah ketersediaan (availability), confidentiality (kerahasiaan), dan kesatuan (integrity).

Setelah identifikasi aset dilakukan kemudian ditentukan jenis gangguan keamanan yang mungkin pada setiap aset tersebut.

Secara umum terdapat tiga hal yang perlu diperhatikan, yaitu **akses yang tidak sah (unauthorized access)** terhadap **informasi**, **pengungkapan informasi yang tidak sah (unauthorized disclosure)**, serta **denial of service**.

Security Policy

Tujuan utama dari security policy adalah memberitahukan pengguna tentang kewajiban apa saja yang harus ditaati mereka untuk melindungi aset sesuai dengan tingkatan masing-masing pengguna. Selain itu security policy digunakan sebagai dasar untuk membangun, mengkonfigurasi dan mengaudit jaringan komputer yang sesuai dengan kebutuhan keamanan.

Sebuah security policy yang baik berisikan pembagian tanggung jawab yang jelas antara pengguna, administrator, dan manager serta dapat diimplementasikan oleh administrator dan diberitahukan kepada pengguna sebagai sebuah user guideline. Selain itu juga dimungkinkan untuk ditambahkan dengan perangkat dan aturan keamanan tambahan jika diperlukan.

Fleksibilitas sebuah security policy sangat diperlukan karena perubahan teknologi harus selalu dapat diantisipasi. Karena itu security policy tidak boleh tergantung pada penggunaan perangkat keras dan lunak tertentu. Selain fleksibel security policy juga berisikan hal-hal yang bersifat pengecualian.

PROTEKSI DAN *SECURITY SERVICE*

Proteksi

Pada lingkup jaringan komputer proteksi yang harus dilakukan adalah proteksi infrastruktur, jaringan, dan service. Infrastruktur yang dicakup di sini tidak hanya perangkat keras, namun juga network management, dan security (user authentication misalnya).

Dengan alasan di atas sebagian besar administrator lebih memilih mengamankan komputer yang berisikan data dibandingkan harus mengamankan jaringannya. Pilihan itu semakin ditambah karena lebih mudahnya mengamankan komputer dari pada infrastruktur dan jaringannya. Proteksi pada jaringan dilakukan untuk mencegah adanya serangan yang spesifik ditujukan untuk jaringan. Di antaranya yang umum dikenal adalah denial of service.

SECURITY SERVICE

Autentikasi merupakan salah satu contoh security service. Hal yang berhubungan dengan autentikasi adalah penggunaan password. Beberapa jenis dan metode pe-password-an diperkenalkan, misalnya reusable password dan one-time-password.

One-time-password diaplikasikan dengan penggunaan peralatan tambahan.

Security service lainnya adalah Integrity yang digunakan untuk memastikan bahwa informasi (file, data, atau paket) tidak dirubah oleh orang yang tidak berhak. Autorisasi, Audit, dan Pengaturan Akses merupakan jenis security service lainnya. Autorisasi berhubungan dengan apa sajakah yang bisa dilakukan seorang user sesuai dengan hak yang dimiliki. Sedangkan Audit berhubungan dengan pengumpulan data aktifitas jaringan. Pengumpulan data dapat dilakukan melalui audit log file, maupun dengan menggunakan aplikasi tertentu.

SECURITY INCIDENT HANDLING

Penanganan insiden (security incident handling) diperlukan sebelum, saat, dan setelah terjadinya gangguan keamanan dan masih berhubungan dengan security policy. Hal ini diperlukan karena seringkali terjadi kepanikan yang berlebihan pada saat terjadinya gangguan keamanan. Selain timbul kepanikan, pada saat tersebut bahkan dibutuhkan staf yang lebih banyak untuk mengatasi gangguan keamanan. Dengan perencanaan dan langkah yang tepat akan dimungkinkan untuk menghindari hal-hal tersebut.

Langkah-langkah yang diperlukan dalam security incident handling adalah persiapan dan perencanaan, pemberitahuan, identifikasi insiden (apakah benar dan seberapa parah), penanganan, dan langkah setelah insiden.



TERIMA KASIH