**Lampiran 1 :**

**MATERI AJAR**

**Pertemuan 1**

**KONSEP DASAR JARINGAN KOMPUTER**

Seiring perkembangan komputer, jenis-jenis jaringan komputer pun juga mulai bervariasi. ada beberapa macam jenis jaringan komputer yang kita kenal sekarang, saya masih ingat dulu waktu saya sekolah SMK hanya ada 3 jaringan komputer yang saya kenal yakni jaringan LAN, MAN dan juga WAN. namun sepertinya sekarang sudah mulai ada tambahan jenis jaringan komputer baru.

**Jenis jaringan komputer yang ada sekarang**

1. **PAN (Personal Area Network)**

Merupakan jaringan antara dua atau lebih sistem komputer yang berjarak tidak terlalu jauh. Biasanya Jenis jaringan yang satu ini hanya berjarak 1 sampai 5 meter saja. Jenis jaringan ini sangat sering kita gunakan. misalnya pada saat kita menghubungkan komputer dengan HP, Heandset ataupun perangkat sejenis lainnya.

[](http://1.bp.blogspot.com/-0RfoZQjwul0/UaXQWkWfEeI/AAAAAAAAA8c/ucfF74pWIAs/s1600/jaringan+komputer+PAN.jpg)

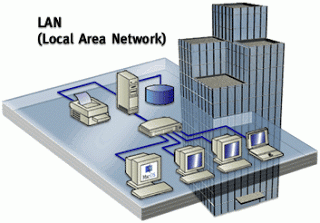
**Pertemuan 2**

1. **Local Area Network (LAN)**

Pada tahun 1940-an di Amerika ada sebuah penelitian yang ingin memanfaatkan sebuah perangkat komputer secara bersama. Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, karena mahalnya harga perangkat komputer maka ada tuntutan sebuah komputer mesti melayani beberapa terminal. Dari sinilah maka muncul konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System), bentuk pertama kali jaringan (network) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer.

Selanjutnya ketika harga-harga komputer kecil sudah mulai menurun dan konsep proses distribusi sudah matang, maka penggunaan komputer dan jaringannya sudah mulai beragam dari mulai menangani proses bersama maupun komunikasi antar komputer (Peer to Peer System) saja tanpa melalui komputer pusat. Untuk itu mulailah berkembang teknologi jaringan lokal yang dikenal dengan sebutan LAN (Local Area Network). Demikian pula ketika Internet mulai diperkenalkan, maka sebagian besar LAN yang berdiri sendiri mulai berhubungan dan terbentuklah jaringan raksasa ditingkat dunia yang disebut dengan istilah WAN (Word Area Network).

LAN merupakan jaringan komputer yang sering digunakan untuk menghubungkan komputer-komputer pribadi dan workstatioan dalam suatu kantor suatu perusahaan atau pabrik- pabrik untuk memakai sumber daya (resaource, misalnya printer) secara bersama-sama dan saling bertukar informasi yang masih dalam satu area.

[](http://3.bp.blogspot.com/-a_GEfhKy8eo/UaXQoXHJePI/AAAAAAAAA8k/gAr607nUKY0/s1600/jaringan+LAN.gif)

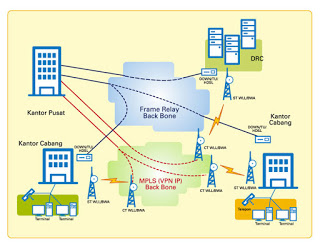
Ciri-ciri LAN:

* Bekerja di area geografis yang terbatas.
* Dapat digunakan multi-access hingga high-bandwidth.
* Administrasi dilakukan melalui administrator lokal.
* Koneksi secara Full-Time dan langsung (Directly Connected )

**Pertemuan 3**

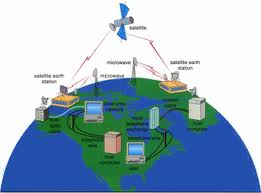
**3) Metropolitan Area Network (MAN)**

Hampir sama dengan LAN yang merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor- kantor perusahaan yang terletak berdekatan atau juga sebuah kota dan dapat di manfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang daya dan suara, bahkan dapat berhubungan dengan jaringan Televisi Kabel. biasanya MAN digunakan dalam area 1 kota, bukan hanya satu lokasi saja.

[](http://4.bp.blogspot.com/-GCXfPWnPXzM/UaXRKI19vkI/AAAAAAAAA8s/xCHyWOk9zqk/s1600/jaringan+MAN.jpg)

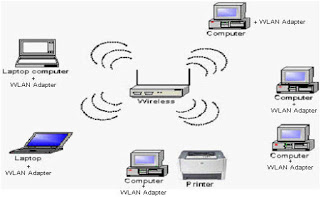
**Pertemuan 4**  
**4) Wide Area Network (WAN)**

Jaringan WAN merupakan jaringan yang mencakup daerah geografis yang lebih luas, seringkali mancakup sebuah negara bahkan antar benua. WAN terdiri dari kumpulan mesin- mesin yang bertujuan utuk menjalankan Program-program (Aplikasi) pemakai, bisa dikatakan jaringan WAN merupakan jaringan internet yang kita kenal saat ini.

[](http://2.bp.blogspot.com/-jkHOv_iQPT0/UaXVRBXZ7zI/AAAAAAAAA9M/TvNMkdkI6Qg/s1600/jaringan+WAN.jpg)

**5) Wireless ( Jaringan Tanpa Kabel )**

Jaringan Tanpa Kabel (wireless) merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan menggunkan kabel. Saat ini jaringan Tanpa Kabel atau wireless sudah marak di gunakan dengan memanfaatkan jasa satelit dan mampu memberi kecepatan akses yang lebih cepat di bandingkan dengan jaringan yang menggunakan kabel. dengan adanya jaringan wireless memudahkan penggunaan user untuk mengakses data yang di inginkan di tempat-tempat yang tidak terjangkau oleh jaringan kabel, misal pada saat mobile / bepergian.

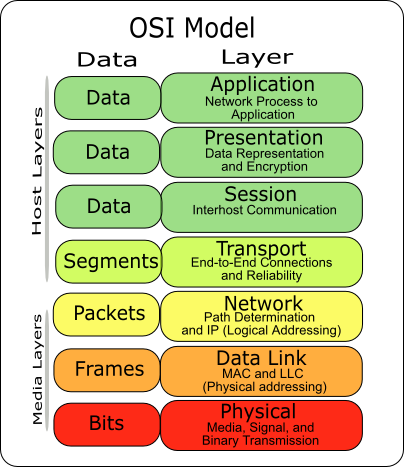
[](http://4.bp.blogspot.com/-dMqxYfg29Z8/UaXT-00IgOI/AAAAAAAAA88/So7nh_QHNus/s1600/jaringan+wireless.jpg)

**Pertemuan 5**

**MODEL OSI**

**MACAM-MACAM LAPISAN OSI**

**Model referensi jaringan terbuka OSI** atau ***OSI Reference Model for open networking*** adalah sebuah model arsitektural jaringan yang dikembangkan oleh badan [International Organization for Standardization](http://id.wikipedia.org/wiki/International_Organization_for_Standardization) (ISO) di [Eropa](http://id.wikipedia.org/wiki/Eropa) pada tahun [1977](http://id.wikipedia.org/wiki/1977). OSI sendiri merupakan singkatan dari ***Open System Interconnection***. Model ini disebut juga dengan model “**Model tujuh lapis OSI**” (*OSI seven layer model*).

[](http://imronayubi.files.wordpress.com/2008/01/osi-model-jb.png)

Struktur tujuh lapis model OSI, bersamaan dengan [*protocol data unit*](http://id.wikipedia.org/wiki/Protokol_jaringan) pada setiap lapisan

OSI Reference Model memiliki tujuh lapis, yakni sebagai berikut

|  |  |  |
| --- | --- | --- |
| **Lapisan ke-** | **Nama lapisan** | **Keterangan** |
| 7 | [*Application layer*](http://id.wikipedia.org/w/index.php?title=Lapisan_aplikasi&action=edit) | Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah [HTTP](http://id.wikipedia.org/wiki/HTTP), [FTP](http://id.wikipedia.org/wiki/FTP), [SMTP](http://id.wikipedia.org/wiki/SMTP), dan [NFS](http://id.wikipedia.org/wiki/Network_File_System). |
| 6 | [*Presentation layer*](http://id.wikipedia.org/wiki/Lapisan_presentasi) | Berfungsi untuk mentranslasikan [data](http://id.wikipedia.org/wiki/Data) yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* (dalam [Windows NT](http://id.wikipedia.org/wiki/Windows_NT)) dan juga [Network shell](http://id.wikipedia.org/w/index.php?title=Network_shell&action=edit) (semacam [*Virtual Network Computing*](http://id.wikipedia.org/w/index.php?title=Virtual_Network_Computing&action=edit) (VNC) atau [*Remote Desktop Protocol*](http://id.wikipedia.org/wiki/Remote_Desktop_Protocol) (RDP)). |
| 5 | [*Session layer*](http://id.wikipedia.org/wiki/Lapisan_sesi) | Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama. |
| 4 | [*Transport layer*](http://id.wikipedia.org/wiki/Lapisan_transport) | Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadp paket-paket yang hilang di tengah jalan. |
| 3 | [*Network layer*](http://id.wikipedia.org/wiki/Lapisan_jaringan) | Berfungsi untuk mendefinisikan [alamat-alamat IP](http://id.wikipedia.org/wiki/Pengalamatan_IP), membuat *header* untuk [paket-paket](http://id.wikipedia.org/wiki/Paket_jaringan), dan kemudian melakukan routing melalui *internetworking* dengan menggunakan [*router*](http://id.wikipedia.org/wiki/Router) dan [*switch layer-3*](http://id.wikipedia.org/w/index.php?title=Layer_3_switch&action=edit). |
| 2 | [*Data-link layer*](http://id.wikipedia.org/wiki/Lapisan_data-link) | Befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai ***frame***. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan [perangkat keras](http://id.wikipedia.org/wiki/Perangkat_keras) (seperti halnya [Media Access Control Address (MAC Address)](http://id.wikipedia.org/wiki/MAC_Address)), dan menetukan bagaimana perangkat-perangkat jaringan seperti [*hub*](http://id.wikipedia.org/w/index.php?title=Hub&action=edit), [*bridge*](http://id.wikipedia.org/wiki/Bridge), [*repeater*](http://id.wikipedia.org/w/index.php?title=Repeater&action=edit), dan [*switch layer 2*](http://id.wikipedia.org/wiki/Layer_2_switch) beroperasi. Spesifikasi IEEE 802, membagi *level* ini menjadi dua level anak, yaitu lapisan [*Logical Link Control*](http://id.wikipedia.org/wiki/Logical_Link_Control) (LLC) dan lapisan [*Media Access Control*](http://id.wikipedia.org/wiki/Media_Access_Control) (MAC). |
| 1 | [*Physical layer*](http://id.wikipedia.org/wiki/Lapisan_fisik) | Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya [Ethernet](http://id.wikipedia.org/wiki/Ethernet) atau [Token Ring](http://id.wikipedia.org/wiki/Token_Ring)), [topologi jaringan](http://id.wikipedia.org/wiki/Topologi_jaringan) dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana [*Network Interface Card*](http://id.wikipedia.org/wiki/Network_Interface_Card) (NIC) dapat berinteraksi dengan media [kabel](http://id.wikipedia.org/wiki/Kabel) atau [radio](http://id.wikipedia.org/wiki/Radio). |

 Layer-layer tersebut disusun sedemikian sehingga perubahan pada satu layer tidak membutuhkan perubahan pada layer lain. Layer teratas (5, 6 and 7) adalah lebih cerdas dibandingkan dengan layer yang lebih rendah; Layer Application dapat menangani protocol dan format data yang sama yang digunakan oleh layer lain, dan seterusnya. Jadi terdapat perbedaan yang besar antara layer Physical dan layer Application.

**II. FUNGSI LAYER**

1. Layer Physical

Ini adalah layer yang paling sederhana; berkaitan dengan electrical (dan optical) koneksi antar peralatan. Data biner dikodekan dalam bentuk yang dapat ditransmisi melalui media jaringan, sebagai contoh kabel, transceiver dan konektor yang berkaitan dengan layer Physical. Peralatan seperti repeater, hub dan network card adalah berada pada layer ini.

Network components:

* Repeater
* Multiplexer
* Hubs(Passive and Active)
* TDR
* Oscilloscope
* Amplifier

Protocols:

* IEEE 802 (Ethernet standard)
* IEEE 802.2 (Ethernet standard)
* ISO 2110
* ISDN

**Pertemuan 6**

1. Layer Data-link

 Layer ini sedikit lebih “cerdas” dibandingkan dengan layer physical, karena menyediakan transfer data yang lebih nyata. Sebagai penghubung antara media network dan layer protocol yang lebih high-level, layer data link bertanggung-jawab pada paket akhir dari data binari yang berasal dari level yang lebih tinggi ke paket diskrit sebelum ke layer physical. Akan mengirimkan frame (blok dari data) melalui suatu network. Ethernet (802.2 & 802.3), Tokenbus (802.4) dan Tokenring (802.5) adalah protocol pada layer Data-link.

Network components:

* Bridge
* Switch
* ISDN Router
* Intelligent Hub
* NIC
* Advanced Cable Tester

Protocols:

Media Access Control: Communicates with the adapter card and  Controls the type of media being used:

* 802.3 CSMA/CD (Ethernet)
* 802.4 Token Bus (ARCnet)
* 802.5 Token Ring
* 802.12 Demand Priority

Logical Link Control

* error correction and flow control
* manages link control and defines SAPs

1. Layer Network

Tugas utama dari layer network adalah menyediakan fungsi routing sehingga paket dapat dikirim keluar dari segment network lokal ke suatu tujuan yang berada pada suatu network lain. IP, Internet Protocol, umumnya digunakan untuk tugas ini. Protocol lainnya seperti IPX, Internet Packet eXchange. Perusahaan Novell telah memprogram protokol menjadi beberapa, seperti SPX (Sequence Packet Exchange) & NCP (Netware Core Protocol). Protokol ini telah dimasukkan ke sistem operasi Netware. Beberapa fungsi yang mungkin dilakukan oleh Layer Network

* Membagi aliran data biner ke paket diskrit dengan panjang tertentu
* Mendeteksi Error
* Memperbaiki error dengan mengirim ulang paket yang rusak
* Mengendalikan aliran

Network component

* Bridge
* Switch
* ISDN Router
* Intelligent Hub
* NIC
* Advanced Cable Tester

Protocols

* **IP**; ARP; RARP, ICMP; RIP; OSFP;
* IGMP;
* **IPX**
* NWLink
* NetBEUI
* OSI
* DDP
* DECnet

**Pertemuan 7**

1. Layer Transport

Layer transport data, menggunakan protocol seperti UDP, TCP dan/atau SPX (Sequence Packet eXchange, yang satu ini digunakan oleh NetWare, tetapi khusus untuk koneksi berorientasi IPX). Layer transport adalah pusat dari mode-OSI. Layer ini menyediakan transfer yang reliable dan transparan antara kedua titik akhir, layer ini juga menyediakan multiplexing, kendali aliran dan pemeriksaan error serta memperbaikinya.

Network components:

* Gateway
* Advanced Cable Tester
* Brouter

Protocols:

* TCP, ARP, RARP;
* SPX
* NWLink
* NetBIOS / NetBEUI
* ATP

1. Layer Session

Layer Session, sesuai dengan namanya, sering disalah artikan sebagai prosedur logon pada network dan berkaitan dengan keamanan. Layer ini menyediakan layananke dua layer diatasnya, Melakukan koordinasi komunikasi antara entiti layer yang diwakilinya. Beberapa protocol pada layer ini: NETBIOS: suatu session interface dan protocol, dikembangkan oleh IBM, yang menyediakan layanan ke layer presentation dan layer application. NETBEUI, (NETBIOS Extended User Interface), suatu pengembangan dari NETBIOS yang digunakan pada produk Microsoft networking, seperti Windows NT dan LAN Manager. ADSP (AppleTalk Data Stream Protocol). PAP (Printer Access Protocol), yang terdapat pada printer Postscript untuk akses pada jaringan AppleTalk.

Network components:

* Gateway

Protocols:

* NetBIOS
* Names Pipes
* Mail Slots
* RPC

**Pertemuan 8**

1. Layer Presentation

Layer presentation dari model OSI melakukan hanya suatu fungsi tunggal: translasi dari berbagai tipe pada syntax sistem. Sebagai contoh, suatu koneksi antara PC dan mainframe membutuhkan konversi dari EBCDIC character-encoding format ke ASCII dan banyak faktor yang perlu dipertimbangkan. Kompresi data (dan enkripsi yang mungkin) ditangani oleh layer ini.

Network components:

* Gateway
* Redirector

Protocols:

* None

1. Layer ApplicationLayer ini adalah yang paling “cerdas”, gateway berada pada layer ini. Gateway melakukan pekerjaan yang sama seperti sebuah router, tetapi ada perbedaan diantara mereka. Layer Application adalah penghubung utama antara aplikasi yang berjalan pada satu komputer dan resources network yang membutuhkan akses padanya. Layer Application adalah layer dimana user akan beroperasi padanya, protocol seperti FTP, telnet, SMTP, HTTP, POP3 berada pada layer Application.

Network components:

* Gateway

Protocols:

* DNS; FTP
* TFTP; BOOTP
* SNMP; RLOGIN
* SMTP; MIME;
* NFS; FINGER
* TELNET; NCP
* APPC; AFP
* SMB

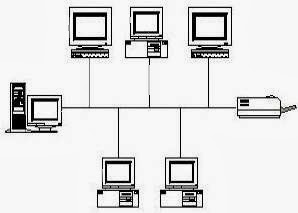
**Pertemuan 9**

**Pengertian topologi jaringan komputer**

**Pengertian topologi jaringan** adalah suatu tehnik untuk menghubungkan komputer yang satu dengan komputer lainnya yang merangkai menjadi sebuah jaringan, dimana penggunaan topologi jaringan didasarkan pada biaya, kecepatan akses data, ukuran maupun tingkat konektivitas yang akan mempengaruhi kualitas maupun efiensi suatu jaringan.  
  
Ada bermacam macam topologi jaringan komputer yang banyak di gunakan saat ini antara lain adalah Topologi Bus, Topologi Ring, Topologi Star, Topologi Mesh, Topologi Linear, masing-masing jenis topologi ini mempunyai kelebihan dan kekurangannnya sendiri.

**Macam-macam topologi jaringan komputer**

1. **Topologi Bus**

[](http://4.bp.blogspot.com/-1ab1CtHXVOw/UmnYq4FRQMI/AAAAAAAABUY/M2Br1ll02dQ/s1600/topologi+bus.jpg)

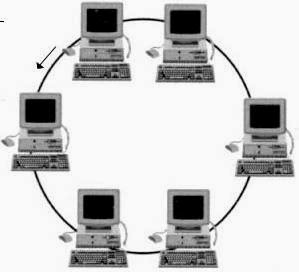
Jenis topologi bus ini menggunakan kabel tunggal, seluruh komputer saling berhubungan secara langsung hanya menggunakan satu kabel saja. Kabel yang menghubungkan jaringan ini adalah kabel koaksial dan dilekatkan menggunakan T-Connector. Untuk memaksimalkan penggunaan jaringan ini sebaiknya menggunakan kabel Fiber Optic karena kestabilan resistensi sehingga dapat mengirimkan data lebih baik.

Kelebihan Topologi Bus :

1. Mudah untuk dikembangkan
2. Tidak memerlukan kabel yang banyak
3. Hemat biaya pemasangan

Kelemahan topologi bus :

1. Tidak stabil, jika salah satu komputer terganggu maka jaringan akan terganggu
2. Tingkat deteksi kesalahan sangat kecil
3. Sulit mencari gangguan pada jaringan
4. Tingkat lalu lintas tinggi / sering terjadi antrian data
5. Untuk jarak jauh diperlukan repeater
6. **Topologi Ring**

[](http://3.bp.blogspot.com/-v0-Kz9o_MnA/UmnY3KEOdxI/AAAAAAAABUg/_jQcL7lt21I/s1600/topologi+ring.jpg)

Jenis topologi ring ini, seluruh komputer dihubungkan menjadi satu membentuk lingkaran (ring) yang tertutup dan dibantu oleh Token, Token berisi informasi yang berasal dari komputer sumber yang akan memeriksa apakah informasi tersebut digunakan oleh titik yang bersangkutan, jika ada maka token akan memberikan data yang diminta oleh titik jaringan dan menuju ke titik berikutnya. seluruh komputer akan menerima setiap signal informasi yang mengalir, informasi akan diterima jika memang sudah sesuai dengan alamat yang dituju, dan signal informasi akan diabaikan jika bukan merupakan alamatnya sendiri. Dengan kata lain proses ini akan berlanjut terus hingga sinyal data diterima ditujuan.

Kelebihan :

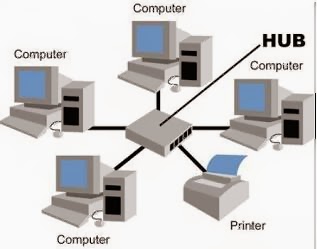
1. Tidak menggunakan banyak kabel
2. Tingkat kerumitan pemasangan rendah
3. Mudah instalasi
4. Tidak akan terjadi tabrak data
5. Mudah dirancang

Kekurangan :

1. peka kesalahan jaringan
2. Sulit untuk dikembangkan
3. Jika salah satu titik jaringan terganggu maka seluruh komunikasi data dapat terganggu

**Pertemuan 10**

1. **Topologi Star**

[](http://3.bp.blogspot.com/-1zuUFZoqvJY/UmnY-79S21I/AAAAAAAABUo/1fzxnb72FfU/s1600/topologi+star.jpg)

Pada topologi jenis star ini, setiap komputer langsung dihubungkan menggunakan Hub, dimana fungsi dari Hub ini adalah sebagai pengatur lalu lintas seluruh komputer yang terhubung. Karena menggunakan proses pengiriman dan penerimaan informasi secara langsung inilah yang menyebabkan biaya pemasangannya juga tinggi.

Kelebihan :

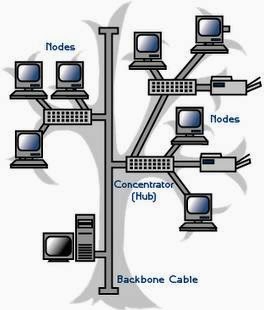
1. Deteksi kesalahan mudah dilakukan
2. Perubahan stasiun mudah dilakukan dan tidak mengganggu jaringan lain
3. Mudah melakukan control
4. Tingkat keamanan tinggi
5. Paling fleksibel

Kekurangan :

1. Menggunakan banyak kabel
2. Ada kemungkinan akan terjadi tabrakan data sehingga dapat menyebabkan jaringan lambat
3. Jaringan sangat tergantung kepada terminal pusat
4. Jaingan memakan biaya tinggi
5. Jika titik komputer pusat terjadi gangguan maka terganggu pula seluruh jaringan

**Pertemuan 11**

1. **Topologi Tree**

[](http://2.bp.blogspot.com/-QU_vNHUEvUI/UmnZFjrPsqI/AAAAAAAABUw/QdCSoJqu7t0/s1600/topologi+tree.jpg)

Topologi tree ini merupakan hasil pengembangan dari topologi star dan topologi bus yang terdiri dari kumpulan topologi star dan dihubungkan dengan 1 topologi bus. Topologi tree biasanya disebut juga topologi jaringan bertingkat dan digunakan interkoneksi antar sentral.  
Pada jaringan ini memiliki beberapa tingkatan simpul yang ditetapkan dengan suatu hirarki, gambarannya adalah semakin tinggi kedudukannya maka semakin tinggi pula hirarki-nya. Setiap simpul yang memiliki kedudukan tinggi dapat mengatur simpul yang memiliki kedudukan yang rendah. Data dikirim dari pusat simpul kemudian bergerak menuju simpul rendah dan menuju ke simpul yang lebih tinggi terlebih dahulu.

Topologi tree ini memiliki kelebihan dan kelemahan yang sama dengan topologi star antara lain:

Kelebihan :

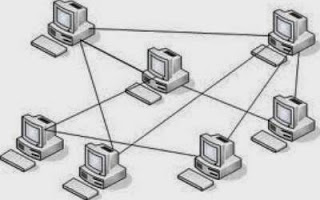
1. Deteksi kesalahan mudah dilakukan
2. Perubahan bentuk suatu kelompok mudah dilakukan dan tidak mengganggu jaringan lain
3. Mudah melakukan control

Kekurangan :

1. Menggunakan banyak kabel
2. Sering terjadi tabrakan data
3. Jika simpul yang lebih tinggi rusak maka simpul yang lebih rendah akan terganggu juga
4. Cara kerja lambat

**Pertemuan 12**

1. **Topologi  Mesh / Jala**

[](http://3.bp.blogspot.com/-s8WTpwOQrgc/UmnZLQ5hK3I/AAAAAAAABU4/uBS2BLs1ex8/s1600/topologi+mesh.jpg)

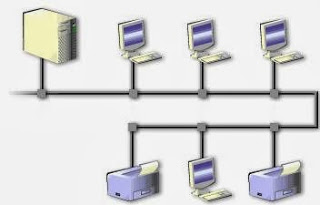
Topologi Mesh merupakan rangkaian jaringan yang saling terhubung secara mutlak dimana setiap perangkat komputer akan terhubung secara langsung ke setiap titik perangkat lainnya. Setiap titik komputer akan mempunyai titik yang siap untuk berkomunikasi secara langsung dengan titik perangkat komputer lain yang menjadi tujuannya.

Kelebihan :

1. Dinamis dalam memperbaiki setiap kerusakan titik jaringan komputer
2. Data langsung dikirimkan ke tujuan tanpa harus melalui komputer lain
3. Data lebih cepat proses pengiriman data
4. Jika terjadi kerusakan pada salah satu komputer tidak akan mengganggu komputer lainnya

Kekurangan :

1. Biaya untuk memasangnya sangat besar.
2. Perlu banyak kabel
3. Perlu banyak port I/O , setiap komputer diperlukan n-1 port I/O dan sebanyak n(n-1)/2 koneksi. Misalnya ada 4 komputer maka diperlukan kabel koneksi sebanyak 4(4-1)/2 =6 kabel dan memerlukan 4-1 = 3 port.
4. Proses instalasi sulit dan rumit
5. **Topologi linear**

[](http://2.bp.blogspot.com/-njAj5Drud5A/UmnZRpmoaBI/AAAAAAAABVA/bTpszGVfHrc/s1600/topologi+linear.jpg)

Topologi ini merupakan perluasan dari dari topologi bus dimana kabel utama harus dihubungkan ke tiap titik komputer menggunakan T-connector. Topologi tipe ini merupakan jenis yang sederhana menggunakan kabel RG-58.

Kelebihan :

1. Sederhana jaringannya
2. Hemat kabel
3. Mudah untuk dikembangkan

Kekurangan :

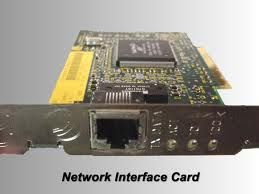
1. Deteksi kesalahan sangat kecil
2. Keamanan kurang terjamin
3. Lalu lintas data tinggi
4. Kecepatan transfer tergantung kepada jumlah pengguna, kecepatan turun jika jumlah pemakai bertambah

**Pertemuan 13**

**[Media Jaringan Komputer](http://www.it-artikel.com/2012/07/media-jaringan-komputer.html)**

Adapun media yang digunakan dalam jaringan komputer yang digunakan sebagai *workstation* atau *client* bisa bermacam-macam mesin tergantung kebutuhan dari pemakai dan dilengkapi dengan kartu jaringan atau minimal *ethernet* 10/100 Mbps.

1. *LAN Card/Network Interface Card (­Kartu jaringan)*

[](http://4.bp.blogspot.com/-_YiQCNRkjr4/T4fNUkDC0gI/AAAAAAAAAHQ/T923ioMIBg8/s1600/Nic.jpg)

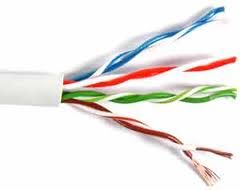
Sebuah kartu jaringan *(LAN Card)* yang terpasang pada sebuah komputer *server* maupun workstation sehingga komputer dapat dihubungkan ke dalam sistem jaringan. Apabila terjadi gangguan atau kerusakan pada kartu jaringan berakibat pada komputer tersebut tidak dapat masuk dalam sistem jaringan. Indikator yang dapat dilihat dalam kerusakan kartu jaringan adalah lampu indikator yang terdapat pada kartu jaringan tidak menyala dan lampu indikator di *hub/switch* saat komputer telah aktif dan konektifitas kabel dari kartu jaringan dan *hub/switch* telah baik.

1. *Twisted Pair Cable*

*Twisted* Pair *Cable* ini terdiri dari dua jenis yaitu [*shielded*](http://itartikel.blogspot.com/2012/07/media-jaringan-komputer.html) dan *unshielded*. *Shielded* adalah jenis kabel yang memiliki selubung pembungkus dan [*unshielded*](http://itartikel.blogspot.com/2012/07/media-jaringan-komputer.html) adalah jenis kabel yang tidak memiliki selubung pembungkus, untuk koneksinya kabel jenis ini menggunakan konektor *RJ-11* atau *RJ-45.*

[](http://4.bp.blogspot.com/-xbgToa73Su0/T7Wdt4vbQbI/AAAAAAAAAOY/pqNCBmy9chA/s1600/Konektor.png)

Saat ini ada beberapa *grate* atau kategori, dari kabel *twisted pair,* *Category* 5 adalah yang paling *realible* dan memiliki kompatibilitas yang tinggi, dan yang paling disarankan. Berjalan baik pada 10Mbps *network*, dan *fast Ethernet*. Suatu kabel category 5 memiliki 8 kabel kecil yang masing-masing memiliki kode warna di dalamnya dari ujung ke ujung. Hanya kabel kecil 1, 2, 3, dan 6 yang digunakan oleh *ethernet* *network* untuk komunikasi, walaupun hanya 4 kabel yang akan digunakan, tapi masing-masing 8 kabel semuanya terhubung ke *jack.*

[](http://4.bp.blogspot.com/-m9F2XrVyo9o/T4fSrzUmoTI/AAAAAAAAAII/zBToylQ0Gb8/s1600/utp.jpg)

Secara umum, pemasangan atau perakitan kabel *UTP* ada dua tipe, yaitu tipe *straight* dan tipe *cross*. Disebut tipe *straight* dikarenakan masing-masing kabel yang jumlahnya 8 terkorespondensi 1-1 (langsung), sedangkan disebut tipe *cross* dikarenakan adanya persilangan pada penyusunan kabelnya.

1. *Switch*

[](http://1.bp.blogspot.com/-Rdhrvh67Be0/T4fQVSsHJmI/AAAAAAAAAHo/pvz4eSoiOnw/s1600/swict.jpg)

*Switch* merupakan terminal bagi kartu jaringan (*Network Card*). Jika terminal mengalami kerusakan berarti seluruh jaringan juga tidak dapat berfungsi untuk berkomunikasi antar *workstation* atau komputer *workstation* dengan server. Apabila terjadi kerusakan pada *switch* dapat dilihat pada lampu indikator *power* dan lampu indikator untuk masing-masing *workstation*. Apabila lampu indikator *power switch* tidak menyala berarti kemungkinan besar *switch* tersebut rusak. Jika ada lampu indikator *workstation* yang tidak menyala menyatakan bahwa komputer *workstation* sedang tidak aktif atau ada gangguan pada komputer *workstation* tersebut.

1. Modem *ADSL*

[](http://1.bp.blogspot.com/-TiE-uRdeYDg/T4fR9nRnZTI/AAAAAAAAAIA/8IN-vLB6wFM/s1600/modem.jpg)

Modem adalah singkatan dari *modulator demodulator*. Komunikasi data  bisa berupa analog atau digital. *Modulasi* adalah suatu proses mengubah sinyal digital menjadi sinyal analog. Sinyal analog dikirim melalui saluran komunikasi ke ujung lain dari suatu jaringan. Di ujung lain sinyal tersebut dikembalikan ke bentuk asalnya yaitu bentuk digital yang bisa diinterpretasikan oleh komputer. Proses pengubahan ini dinamakan *demodulasi*.

*ADSL* adalah kependekan dari *Asymmetric Digital Subscriber Line*, sebuah teknologi yang memungkinan data kecepatan tinggi dikirim melalui kabel telepon. *ADSL* memungkinkan untuk menerima data sampai kecepatan 1.5-9Mbps (kecepatan *downstream*) dan mengirim data pada kecepatan 16-640Kbps (kecepatan *upstream)*.

*ADSL* membagi *frekuensi* dari sambungan yang digunakan dengan asumsi sebagian besar pengguna internet akan lebih banyak mengambil (*download*) data dari internet daripada mengirim (*upload*) ke internet*.* Oleh karena itu, kecepatan data dari internet biasa sekitar tiga sampai empat kali kecepatan ke internet. Karena kecepatan *upstream* dan *downstream* tidak sama digunakan istilah *Asymmetric*

**Pertemuan 14**

# Media Implementasi Jaringan

Perangkat keras (Hardware) yang dibutuhkan untuk membangun sebuah jaringan komputer yaitu, Komputer, kabel, Card Network, Hub, dan segala sesuatu yang berhubungan dengan koneksi jaringan seperti: Printer, CDROM, Scanner, Bridges, Router dan lainnya yang dibutuhkan untuk process transformasi data didalam jaringan. Berikut beberapa media jaringan yang biasa di gunakan di dalam membangun sebuah jaringan, yaitu

* 1. **Kabel**

Jaringan komputer pada dasaranya adalah jaringan kabel, menghubungkan satu sisi dengan sisi yang lain. Seiring dengan perkembangan teknologi, penghubung antar komputer pun mengalami perubahan serupa.Teknologi jaringan komputer bisa menggunakan teknologi kabel coaxial seperti 10BASE2 hingga fiber optik.

Setiap jenis kabel mempunyai kemampuan dan spesifikasi yang berbeda, ada dua jenis kabel yang dikenal secara umum twisted pair (UTP) dan coaxial kabel, sedangkan yang banyak digunakan KPPTI untuk membuat jaringan adalah UTP kabel (khususnya CAT 5) serta fiber optik kabel.

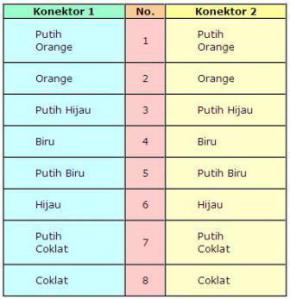
**1.1. Twisted Pair**

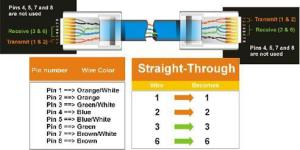
Twisted pair merupakan kabel yang di susun secara berpasangan (twist) di mana bertujuan untuk menghilangkan efek crosstalk, banyak di gunakan untuk jaringan LAN karena mampu mengirim bandwidth dalam jumlah besar. Kabel twisted pair terbagi menjadi dua jenis yaitu, Unshielded Twisted Pair (UTP) dan Shielded Twisted Pair (STP). Namun dari kedua jenis kabel twisted pair tersebut yang paling sering dan umum di gunakan dalam membangun jaringan adalah kabel UTP. Oleh karena itu di sini kami hanya akan membahas mengenai kabel UTP saja.

Sesuai dengan namanya kabel UTP tidak memiliki pelindung (Unshielded). UTP terdiri dari 4 pasang (twist). Kabel UTP yang umum di gunakan di dalam jaringan adalah UTP CAT 5 yang mampu melewatkan data dengan bandwidth 100 Mbps.

**Standar Internasional**

1. **Kabel Straight**

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/untitled-2/)

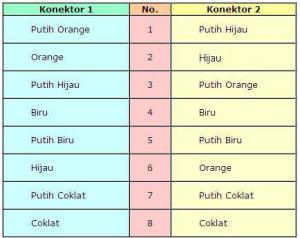
[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/straight/)

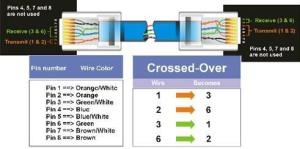
Straigh-Through cable digunakan untuk sambungan seperti berikut :

* Sambungan dari router kepada hub/switch.
* Sambungan dari server kepada hub/switch.
* Sambungan dari workstation kepada hub/switch.

1. **Kabel Crossover**

Tabel Kabel cross menurut standarisasi T586 adalah sebagai berikut:

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/table-crossover/)

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/crossover/)

Crossover cable pula digunakan untuk sambungan seperti berikut :

* Sambungan uplink antara switch.
* Sambungan hub kepada switch.
* Sambungan hub kepada hub lain.
* Sambungan network terus antara dua komputer (tanpa      hub/switch).
* Sambungan router interface kepada router interface yang lain.

**Category 1**

Kabel UTP Category 1 (Cat1) adalah kabel UTP dengan kualitas transmisi terendah, yang didesain untuk mendukung komunikasi suara analog saja. Kabel Cat1 digunakan sebelum tahun 1983 untuk menghubungkan telepon analog Plain Old Telephone Service (POTS). Karakteristik kelistrikan dari kabel Cat1 membuatnya kurang sesuai untuk digunakan sebagai kabel untuk mentransmisikan data digital di dalam jaringan komputer, dan karena itulah tidak pernah digunakan untuk tujuan tersebut.

**Category 2**

Kabel UTP Category 2 (Cat2) adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 1 (Cat1), yang didesain untuk mendukung komunikasi data dan suara digital. Kabel ini dapat mentransmisikan data hingga 4 megabit per detik. Seringnya, kabel ini digunakan untuk menghubungkan node-node dalam jaringan dengan teknologi Token Ring dari IBM. Karakteristik kelistrikan dari kabel Cat2 kurang cocok jika digunakan sebagai kabel jaringan masa kini. Gunakanlah kabel yang memiliki kinerja tinggi seperti Category 3, Category 4, atau Category 5.

**Category 3**

Kabel UTP Category 3 (Cat3) adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 2 (Cat2), yang didesain untuk mendukung komunikasi data dan suara pada kecepatan hingga 10 megabit per detik. Kabel UTP Cat3 menggunakan kawat-kawat tembaga 24-gauge dalam konfigurasi 4 pasang kawat yang dipilin (twisted-pair) yang dilindungi oleh insulasi. Cat3 merupakan kabel yang memiliki kemampuan terendah (jika dilihat dari perkembangan teknologi Ethernet), karena memang hanya mendukung jaringan 10BaseT saja. Seringnya, kabel jenis ini digunakan oleh jaringan IBM Token Ring yang berkecepatan 4 megabit per detik, sebagai pengganti Cat2.

**Category 4**

Kabel UTP Category 4 (Cat4) adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 3 (Cat3), yang didesain untuk mendukung komunikasi data dan suara hingga kecepatan 16 megabit per detik. Kabel ini menggunakan kawat tembaga 22-gauge atau 24-gauge dalam konfigurasi empat pasang kawat yang dipilin (twisted pair) yang dilindungi oleh insulasi. Kabel ini dapat mendukung jaringan Ethernet 10BaseT, tapi seringnya digunakan pada jaringan IBM Token Ring 16 megabit per detik.

**Category 5**

Kabel UTP Category 5 (Cat5) adalah kabel dengan kualitas transmisi yang jauh lebih baik dibandingkan dengan kabel UTP Category 4 (Cat4), yang didesain untuk mendukung komunikasi data serta suara pada kecepatan hingga 100 megabit per detik. Kabel ini menggunakan kawat tembaga dalam konfigurasi empat pasang kawat yang dipilin (twisted pair) yang dilindungi oleh insulasi. Kabel ini telah distandardisasi oleh Electronic Industries Alliance (EIA) dan Telecommunication Industry Association (TIA).

Kabel Cat5 dapat mendukung jaringan Ethernet (10BaseT), Fast Ethernet (100BaseT), hingga Gigabit Etheret (1000BaseT). Kabel ini adalah kabel paling populer, mengingat kabel serat optik yang lebih baik harganya hampir dua kali lipat lebih mahal dibandingkan dengan kabel Cat5. Karena memiliki karakteristik kelistrikan yang lebih baik, kabel Cat5 adalah kabel yang disarankan untuk semua instalasi jaringan.

**Enhanced Category 5**

Kabel ini merupakan versi perbaikan dari kabel UTP Cat5, yang menawarkan kemampuan yang lebih baik dibandingkan dengan Cat5 biasa. Kabel ini mampu mendukung frekuensi hingga 250 MHz, yang direkomendasikan untuk penggunaan dalam jaringan Gigabit Ethernet, meskipun menggunaan kabel UTP Category 6 lebih disarankan untuk mencapai kinerja tertinggi.

**Pertemuan 15**

**1.2   Coaxial**

Kabel Coaxial adalah jenis kabel yang memiliki bendwidth yang lebih lebar jika di bandingkan dengan kabel UTP, sehingga sering di gunakan pada instalasi jaringan broadband.

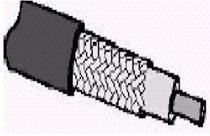
Untuk coaxial cable, dikenal dua jenis, yaitu thick coaxial cable (mempunyai diameter lumayan besar) dan thin coaxial cable (mempunyai diameter lebih kecil).

1. Thick coaxial cable (Kabel Coaxial “gemuk”)

Kabel coaxial jenis ini dispesifikasikan berdasarkan standar IEEE 802.3 10BASE5, dimana kabel ini mempunyai diameter rata-rata 12mm, dan biasanya diberi warna kuning; kabel jenis ini biasa disebut sebagai standard ethernet atau thick Ethernet, atau hanya disingkat ThickNet, atau bahkan cuman disebut sebagai yellow cable.

Kabel Coaxial ini (RG-6) jika digunakan dalam jaringan mempunyai spesifikasi dan aturan sebagai berikut:

1. Setiap ujung harus diterminasi dengan terminator 50-ohm (dianjurkan menggunakan terminator yang sudah dirakit, bukan menggunakan satu buah resistor 50-ohm 1 watt, sebab resistor mempunyai disipasi tegangan yang lumayan lebar).
2. Maksimum 3 segment dengan peralatan terhubung (attached devices) atau berupa populated segments.
3. Setiap kartu jaringan mempunyai pemancar tambahan (external transceiver).
4. Setiap segment maksimum berisi 100 perangkat jaringan, termasuk dalam hal ini repeaters.
5. Maksimum panjang kabel per segment adalah 1.640 feet (atau sekitar 500 meter).
6. f.. Maksimum jarak antar segment adalah 4.920 feet (atau sekitar 1500
7. meter).
8. Setiap segment harus diberi ground.
9. Jarang maksimum antara tap atau pencabang dari kabel utama ke perangkat (device) adalah 16 feet (sekitar 5 meter).
10. Jarang minimum antar tap adalah 8 feet (sekitar 2,5 meter).

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/kabel-thik/)

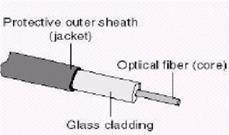
1. Thin coaxial cable (Kabel Coaxial “Kurus”)

Kabel coaxial jenis ini banyak dipergunakan di kalangan radio amatir, terutama untuk transceiver yang tidak memerlukan output daya yang besar. Untuk digunakan sebagai perangkat jaringan, kabel coaxial jenis ini harus memenuhi standar IEEE 802.3 10BASE2, dimana diameter rata-rata berkisar 5mm dan biasanya berwarna hitam atau warna gelap lainnya. Setiap perangkat (device) dihubungkan dengan BNC T-connector. Kabel jenis ini juga dikenal sebagai thin Ethernet atau ThinNet.Kabel coaxial jenis ini, misalnya jenis RG-58 A/U atau C/U, jika diimplementasikan dengan T-Connector dan terminator dalam sebuah jaringan, harus mengikuti aturan sebagai berikut:

1. Setiap ujung kabel diberi terminator 50-ohm.
2. Panjang maksimal kabel adalah 1,000 feet (185 meter) per  segment.
3. Setiap segment maksimum terkoneksi sebanyak 30 perangkat jaringan(devices)
4. Kartu jaringan cukup menggunakan transceiver yang onboard, tidak perlu tambahan transceiver, kecuali untuk repeater.
5. Maksimum ada 3 segment terhubung satu sama lain (populated segment).

Setiap segment sebaiknya dilengkapi dengan satu ground.

Panjang minimum antar T-Connector adalah 1,5 feet (0.5 meter). Maksimum panjang kabel dalam satu segment adalah 1,818 feet (555 meter). Setiap segment maksimum mempunyai 30 perangkat terkoneksi.

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/coaxcial/)

**Pertemuan 16**

* 1. **Fiber Optic**

Fiber optik adalah sebuah kaca murni yang panjang dan tipis serta berdiameter sebesar rambut manusia. Dan dalam pengunaannya beberapa fiber optik dijadikan satu dalam sebuah tempat yang dinamakan kabel optik dan digunakan untuk mengantarkan data digital yang berupa sinar dalam jarak yang sangat jauh.

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/fiber-optik/)

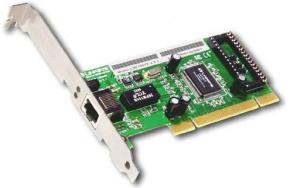
* 1. **Wirelless**

Merupakan teknologi baru dalam jaringan computer tanpa menggunakan kabel tapi menggunaln frekuensi radio dapat menghantarkan dat dengan kecepatan sampai dengan 512 Mbps pada produk – produk khusus (missal militer), tetepi pada produk-produk normal umumnya transfer data adalah 2 Mbps dengan jangkauan bervariasi tergantung produk umumnya jamgkauan maksimum 15 km. Keuntungan produk ini adalah tidak adanya instalasi kabel yang rumit sedangkan kerugiannya adalah diperlukan Line Of Sight (Jarak bebas pandang / LOS ) dari satu titik ke titik lainnya agar berfungsi serta harganya yang relative mahal.

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/belkin-n-wireless-router/)

* 1. **Network Interface Card (NIC)**

Sebuah perangkat yang menghubungkan sebuah titik koneksi jaringan seperti sebuah kompuetr atau sebuah printer jaringan ke sebuah kabel transmisi jaringan dinamakan Network Interface Units (NIU) atau Network Interface Card (NIC), sebuah NIU untuk sebuah komputer tunggal biasanya sebuah papan sirkuit tercetak, atau kartu terhubung secara langsung atau dimasukkan didalam sebuah slot dalam sistem bus. Sebuah perangkat drive sistem operasi mengontrol NIU dan menunjukkan aksi hardware yang memindahkan paket antara NIU dan penyimpanan utama. Sebuah NIU untuk sebuah perangkat pendukung seperti sebuah printer lebih kompleks karena tidak bisa meneruskan pada proses dan sumber penyimpanan dari sistem komputer secara lengkap dalam sebuah network bus, NIU memeriksa tujuan dari alamat dari semua paket dan mengindahkan yang tak teralamatkan.

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/nic/)

Ketika teralamatkan secara benar paket diterima, NIU menyimpan paket dalam sebuah buffer dan membuat sebuah interupt dalam bus sistem. NIU juga mengimplementasikan fungsi protokol Media Access Control, termasuk mendengarkan untuk aktivitas transmisi, mendekati collisions dan mengirim.

Ulang paket – paket data dalam jaringan CSMA/CD dan menerima lalu meneruskan token dalam jaringan token passing.

* 1. **HUB**

Hub merupakan titik knoeksi pertama antara sebuah titik koneksi jaringan dalam sebuah LAN. Variasi Hub sangat luas dalam fungsi dan kapabilitasnya. Hub yang paling sederhana tidak lebih dari koneksi pemasangan terpusat pada titik tunggal dan bisanya dinamakan Wiring Concentrators.

Jaringan hub sesuai dengan perkembangan teknik mutakhir lebih tidak dapat bekerja sama dengan fungsi routing, bridges dan switching. Hubs untuk token ring LAN lebih sophisticated dari hub untuk tipe LAN karena mereka harus mengenerate sebuah token ketika jaringan dimulai atau jika token asli hilang dan sekitar jalur transmisi ulang terputus atau gagal terhubung. Jalur transmisi yang dihubungkan ke sebuah NIU atau jaringan hub dengan standar konektor. Konektor RJ-45 seperti konektor telepon RJ-11 kecuali lebih besar dan menghubungkan 8 kabel, ada beberapa standard untuk konektor fiber optik termasuk ST, SC, LT, and MT-RJ. Standar MT-RJ telah mendukung peralatan vendor termasuk Cisco dan 3com.

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/hub/)

* 1. **Bridges**

Sebuah bridge, biasanya disebut sebagai sebuah repeater mengcopy atau mengulan paket dari satu segment jaringan ke yang lainnya. Kompleksitas dari sebuah bridges dan fungsi pasti bergantung pada perbedaan antara segement jaringan yang terkoneksi. Bridges yang sederhana mengkoneksi segment jaringan yang menggunakan identik kecepatan transmisi, tipe paket dan protokol. Bridge yang lebih komplek menghubungkan segment jaringan yang tidak sama dan menterjemaahkan format paket dan protokol jaringan .

Sebuah bridge memeriksa paket pada setiap jaringan untuk tujuan alamat dari titik koneksi pada jaringan lain dan mencopy paket tersebut kepada jaringan lain. Pada saat jaringan bridge memeriksa paket juga memeriksa pada sumber alamat dan mengupdate tabel internal dari alamat titik koneksi pada setiap segment jaringan. Bridge biasanya digunakan untuk :

* 1. Membangun sebuah virtual LAN dari dua LAN yang terpisah.
  2. Membagi sebuah LAN ke dalam segment untuk meminimalkan

kesempitan pada jaringan.

Design dari sebuah jaringan biasanya dibutuhkan untuk membangun sebuah LAN yang lebih besar dari standar design yang diperbolehkan. Sebagai contoh, 100-Mbps Ethernet LAN tidak bisa lebih panjang dari 210 meter. Jika 300-meter LAN dibutuhkan, maka 2 LAN yang lebih pendek bisa digabungkan dengan sebuah bridge. LAN bridge biasanya disebut Virtual LAN.

Jika sebuah LAN secara rutin dipenuhi dengan trafik, keluarannya bisa ditingkatkan dengan membagi LAN menjadi 2 atau lebih segment dan menggabungkan segmen dengan bridge. Titik koneksi yang mempunyai volume komunikasi yang tinggi satu dengan yang lainnya terhubung dalam satu segment jaringan dengan meminimalkan jumlah paket yang dibutuhkan untuk melewati bridge.

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/bridge/)

* 1. **Router**

Sebuah Router menjalankan fungsi yang sama spt sebuah bridge tapi dilakukannya pengartian yang lebih baik. Sebuah Router secara konstan memeriksa jaringan untuk memonitor pola dari traffic dan penambahan dari titik koneksi, modifikasi, dan penghapusan. Router mengunakan informasi ini untuk membangun sebuah “peta” internal dari jaringan. Router secara periodik menukar informasi dalam internal tabel dengan router lain untuk mendapatkan pengetahuan dari jaringan sesudahnya yang secara langsung terkoneksi. Mereka menggunakan informasi ini untuk meneruskan paket data dari titik koneksi lokal ke penerima yang jauh dan membuat keputusan yang terbaik ketika ada kemungkinan router yang ganda ke sebuah penerima.

Sebuah router yang berdiri sendiri intinya adalah spesial kegunaan komputer dengan prosessor dan penyimpanan. Fungsi routing dapat ditambahkan didalam perangkat lain seperti LAN Hub atau kegunaan computer secara umum.

Beberapa system komputer dengan NIU ganda yang terkoneksi ke segment yang berbeda atau jaringan bisa sebuah router jika software yang sesuai dipasang. Software routing biasanya adalah sebuah komponen system operasi jaringan yang standard dan mungkin atau tidak mungkin bisa difungsikan oleh server administrator. Fungsi routing biasanya diaktifkan pada server dalam LAN kecil untuk menghindari pengeluaran yang bertambah dari sebuah dedicated router.

Routing bukan sebuah tugas penghitungan yang komplek, tetapi membutuhkan kapabilitas I/O yang luas. Setiap paket jaringan hrs diperiksa dan diteruskan. Dalam sebuah jaringan yang sibuk, volume paket dapat menghabiskan kebanyakan atau semua dari kapasitas bus dari sebuah kegunaan kompuetr secara dasar. Seperti sebuah load yang besar bias meninggalkan ketidakcukupan bus atau kapasitas jaringan I/O untuk melakukan fiungsi server transfer file dan sharing printer.

* 1. **Switch**

Sebuah switch mengkombinasikan fungsi dari sebuah bridge dan sebuah hub. Seperti sebuah hub, sebuah switch umumnya mempunyai selusin atau lebih koneksi input untuk komputerdan titik koneksi jaringan lainnya. Setiap koneksi input diberlakukan sebagai sebuah LAN yang terpisah. Sebuah switch memeriksa alamat tujuan dari setiap paket yang datang dan menghubungkan jalur transmisi pada pengirim ke jalur transmisi ke penerima.

Switch menciptakan sebuah virtual LAN yang baru untuk setiap paket dan menghancurkan virtual LAN setelah paket mencapai tujuannya. Switch secara dramatis meningkatkan performance jaringan karena :

1. Switching dilakukan didalam hardware
2. Setiap virtual LAN hanya mempunyai satu titik koneksi    pengiriman dan penerimaan, oleh karena itu menghilangkan kepadatan.

Switching biasanya berguna untuk LAN yang menggunakan CSMA/CD. Switch pada internal segment LAN, mengurangi atau menghilangkan collisions dan transmisi ulang. Switch juga bisa digunakan pada bridge menggabungkan LAN dengan segmen ganda. Seperti bridge, design jaringan harus menggabungkan jaringan titik koneksi ke dalam LAN berdasarkan pada

pembagian traffik dalam meminimalkan jumlah dari paket yang harus direplikasi melewati LAN. Tidak seperti briges, switch bisa berkoneksi lebih dari 2 LAN, menciptakan virtual LAN yang lebih besar.

[](http://1nuy4s4.wordpress.com/media-implementasi-jaringan/switch/)

**Pertemuan 17**

**PROTOKOL JARINGAN KOMPUTER**

* 1. Pengertian protokol jaringan komputer

Protokol adalah sebuah aturan yang mendefinisikan beberapa fungsi yang ada dalam sebuah jaringan komputer, misalnya mengirim pesan, data, informasi dan fungsi lain yang harus dipenuhi oleh sisi pengirim (transmitter) dan sisi penerima (receiver) agar komunikasi berlangsung dengan benar. Selain itu protokol juga berfungsi untuk memungkinkan dua atau lebih komputer dapat berkomunikasi dengan bahasa yang sama.

Hal –hal yang harus diperhatikan :

* + Syntax, Merupakan format data dan cara pengkodean yang digunakan untuk mengkodekan sinyal.
  + semantix, Digunakan untuk mengetahui maksud dari informasi yang dikirim dan mengoreksi kesalahan yang terjadi dari informasi tadi.
  + Timing, Digunakan untuk mengetahui kecepatan transmisi data.

**Fungsi Protokol :**

* + Fragmentasi dan Reassembly, Membagi informasi yang dikirim menjadi beberapa paket data pada saat sisi pengirim mengirimkan informasi tadi dan setelah diterima maka sisi penerima akan menggabungkan lagi menjadi paket berita yang lengkap.
  + Encaptulation, Fungsi dari encaptulation adalah melengkapi berita yang dikirimkan dengan address, kode-kode koreksi dan lain-lain
  + Connection Control, Fungsi dari connection control adalah membangun hubungan komunikasi dari transmitter dan receiver.
  + Flow Control, Fungsi dari flow control adalah mengatur perjalanan data dari transmitter ke receiver.
  + Error Control, Fungsi dari error control adalah mengontrol terjadinya kesalahan yang terjadi pada waktu data dikirimkan.
  + Transmission Service, Fungsi dari transmission service adalah memberi pelayanan komunikasi data khususnya yang berkaitan dengan prioritas dan keamanan serta perlindungan data.

**Standarisasi protokol**

Beberapa perusahaan yang berperan dalam usaha komunikasi, antara lain :

* + Electronic Industries Association (EIA)
  + Committee Consultative Internationale de Telegrapque et Telephonique (CCITT)
  + International Standards Organization (ISO)
  + American National Standard Institute (ANSI)
  + Institute of Electrical and Electronic Engineers (IEEE)
  + Alasan di perlukan standarisasi dalam komunikasi data pada suatu jaringan komputer :
  + Standarisasi memberikan jaminan kepada produsen hardware dan software bahwa produknya akan banyak digunakan oleh pemakai dengan kata lain potensi pasar menjadi lebih besar.
  + Standarisasi menjadikan produk dari para produsen komputer dapat saling berkomunikasi, sehingga pembeli menjadi lebih leluasa dalam memilih peralatan dan menggunakanya.
  + Dengan standarisasi maka produsen tidak dapat melakukan monopoli pasar sehingga harga produk menjadi lebih murah karena terjadi persaingan sehat antar para produsen dalam menjual produknya.
  1. Jenis-jenis protokol
     1. TCP

Transmission Control Protocol (TCP) adalah suatu protokol yang berada di lapisan transpor (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (connection-oriented) dan dapat diandalkan (reliable). TCP dispesifikasikan dalam RFC 793.

TCP memiliki karakteristik sebagai berikut:

* Berorientasi sambungan (connection-oriented): Sebelum data dapat ditransmisikan antara dua host, dua proses yang berjalan pada lapisan aplikasi harus melakukan negosiasi untuk membuat sesi koneksi terlebih dahulu. Koneksi TCP ditutup dengan menggunakan proses terminasi koneksi TCP (TCP connection termination).
* Full-duplex: Untuk setiap host TCP, koneksi yang terjadi antara dua host terdiri atas dua buah jalur, yakni jalur keluar dan jalur masuk. Dengan menggunakan teknologi lapisan yang lebih rendah yang mendukung full-duplex, maka data pun dapat secara simultan diterima dan dikirim. Header TCP berisi nomor urut (TCP sequence number) dari data yang ditransmisikan dan sebuah acknowledgment dari data yang masuk.
* Dapat diandalkan (reliable): Data yang dikirimkan ke sebuah koneksi TCP akan diurutkan dengan sebuah nomor urut paket dan akan mengharapkan paket positive acknowledgment dari penerima. Jika tidak ada paket Acknowledgment dari penerima, maka segmen TCP (protocol data unit dalam protokol TCP) akan ditransmisikan ulang. Pada pihak penerima, segmen-segmen duplikat akan diabaikan dan segmen-segmen yang datang tidak sesuai dengan urutannya akan diletakkan di belakang untuk mengurutkan segmen-segmen TCP. Untuk menjamin integritas setiap segmen TCP, TCP mengimplementasikan penghitungan TCP Checksum.
* Byte stream: TCP melihat data yang dikirimkan dan diterima melalui dua jalur masuk dan jalur keluar TCP sebagai sebuah byte stream yang berdekatan (kontigu). Nomor urut TCP dan nomor acknowlegment dalam setiap header TCP didefinisikan juga dalam bentuk byte. Meski demikian, TCP tidak mengetahui batasan pesan-pesan di dalam byte stream TCP tersebut. Untuk melakukannya, hal ini diserahkan kepada protokol lapisan aplikasi (dalam DARPA Reference Model), yang harus menerjemahkan byte stream TCP ke dalam "bahasa" yang ia pahami.
* Memiliki layanan flow control: Untuk mencegah data terlalu banyak dikirimkan pada satu waktu, yang akhirnya membuat "macet" jaringan internetwork IP, TCP mengimplementasikan layanan flow control yang dimiliki oleh pihak pengirim yang secara terus menerus memantau dan membatasi jumlah data yang dikirimkan pada satu waktu. Untuk mencegah pihak penerima untuk memperoleh data yang tidak dapat disangganya (buffer), TCP juga mengimplementasikan flow control dalam pihak penerima, yang mengindikasikan jumlah buffer yang masih tersedia dalam pihak penerima.
* Melakukan segmentasi terhadap data yang datang dari lapisan aplikasi (dalam DARPA Reference Model)
* Mengirimkan paket secara "one-to-one": hal ini karena memang TCP harus membuat sebuah sirkuit logis antara dua buah protokol lapisan aplikasi agar saling dapat berkomunikasi. TCP tidak menyediakan layanan pengiriman data secara one-to-many.

TCP umumnya digunakan ketika protokol lapisan aplikasi membutuhkan layanan transfer data yang bersifat andal, yang layanan tersebut tidak dimiliki oleh protokol lapisan aplikasi tersebut. Contoh dari protokol yang menggunakan TCP adalah HTTP dan FTP.

**Segmen TCP**

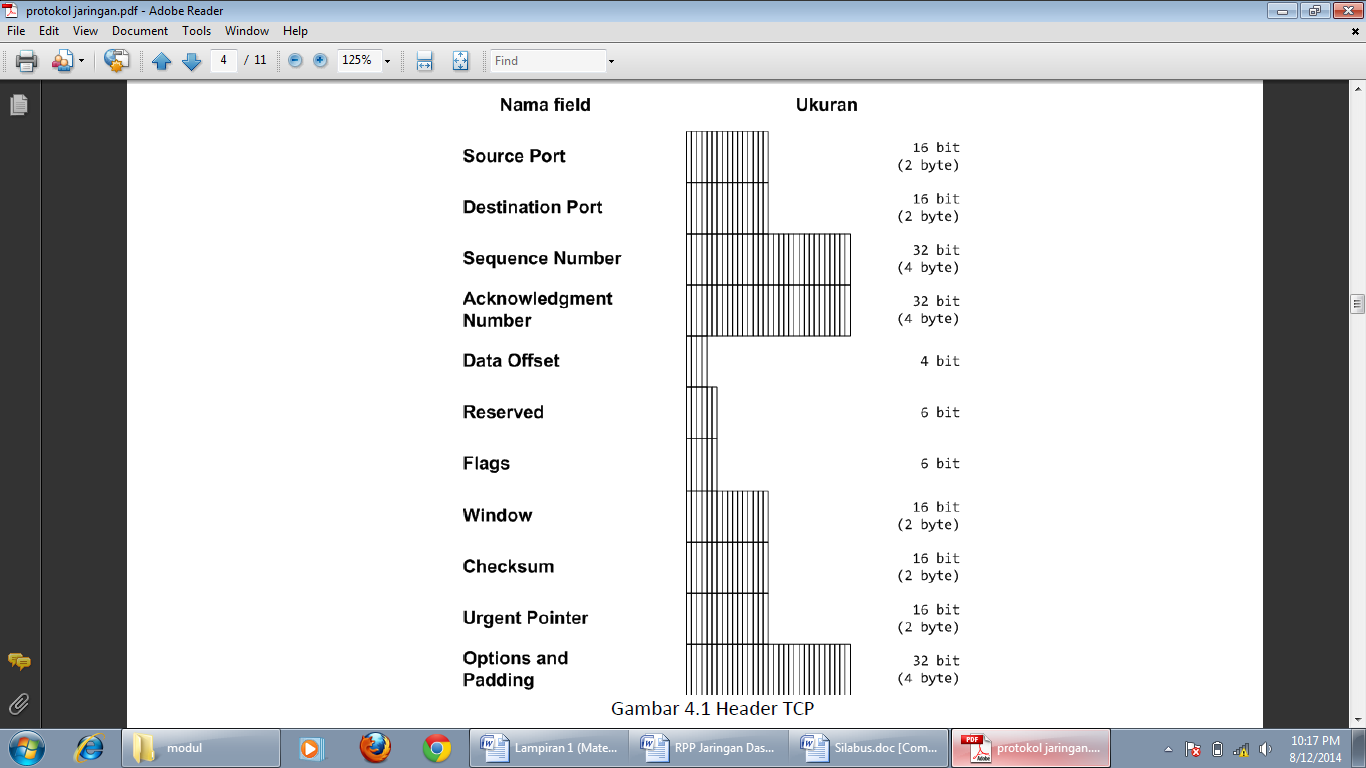
Segmen-segmen TCP akan dikirimkan sebagai datagram-datagram IP (datagram merupakan satuan protocol data unit pada lapisan internetwork). Sebuah segmen TCP terdiri atas sebuah header dan segmen data (payload), yang dienkapsulasi dengan menggunakan header IP dari protokol IP.

Sebuah segmen dapat berukuran hingga 65495 byte: 216-(ukuran header IP terkecil (20 byte)+ukuran header TCP terkecil (20 byte)). Datagram IP tersebut akan dienkapsulasi lagi dengan menggunakan header protokol network interface (lapisan pertama dalam DARPA Reference Model) menjadi frame lapisan Network Interface. Gambar berikut mengilustrasikan data yang dikirimkan ke sebuah host.

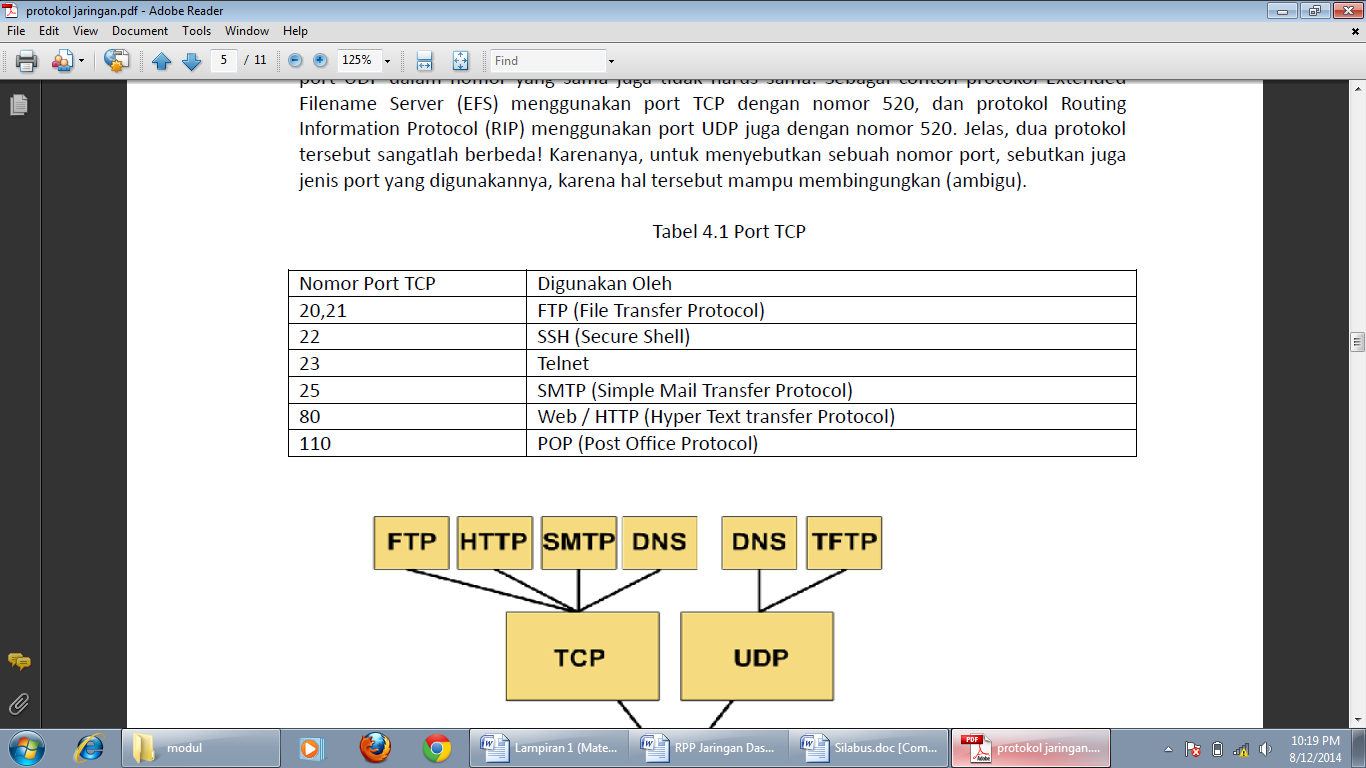
Di dalam header IP dari sebuah segmen TCP, field Source IP Address diatur menjadi alamat unicast dari sebuah antarmuka host yang mengirimkan segmen TCP yang bersangkutan. Sementara itu, field Destination IP Address juga akan diatur menjadi alamat unicast dari sebuah antarmuka host tertentu yang dituju. Hal ini dikarenakan, protokol TCP hanya mendukung transmisi one-to-one.

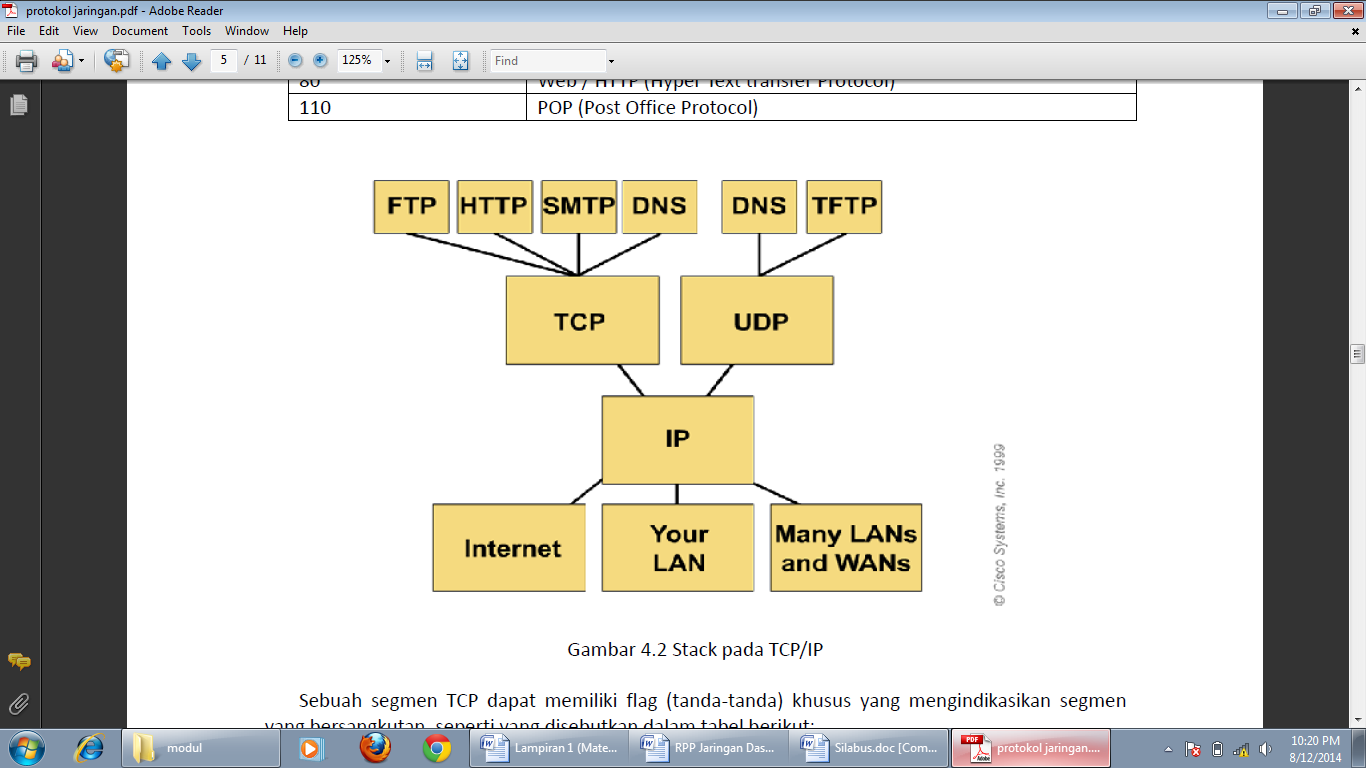
Ukuran dari header TCP adalah bervariasi, yang terdiri atas beberapa field yang ditunjukkan dalam gambar berikut. Ukuran TCP header paling kecil (ketika tidak ada tambahan opsi TCP) adalah 20 byte.

* **Source Port**, Mengindikasikan sumber protokol lapisan aplikasi yang mengirimkan segmen TCP yang bersangkutan. Gabungan antara field Source IP Address dalam header IP dan field Source Port dalam field header TCP disebut juga sebagai socket sumber, yang berarti sebuah alamat global dari mana segmen dikirimkan.
* **Destination Port**, Mengindikasikan tujuan protokol lapisan aplikasi yang menerima segmen TCP yang bersangkutan. Gabungan antara field Destination IP Address dalam header IP dan field Destination Port dalam field header TCP disebut juga sebagai socket tujuan, yang berarti sebuah alamat global ke mana segmen akan dikirimkan.
* **Sequence Number**, Mengindikasikan nomor urut dari oktet pertama dari data di dalam sebuah segmen TCP yang hendak dikirimkan. Field ini harus selalu diset, meskipun tidak ada data (payload) dalam segmen. Ketika memulai sebuah sesi koneksi TCP, segmen dengan flag SYN (Synchronization) diset ke nilai 1, field ini akan berisi nilai Initial Sequence Number (ISN). Hal ini berarti, oktet pertama dalam aliran byte (byte stream) dalam koneksi adalah ISN+1.
* **Acknowledgment Number**, Mengindikasikan nomor urut dari oktet selanjutnya dalam aliran byte yang diharapkan oleh untuk diterima oleh pengirim dari si penerima pada pengiriman selanjutnya. Acknowledgment number sangat dipentingkan bagi segmen-segmen TCP dengan flag ACK diset ke nilai 1.
* **Data Offset,** Mengindikasikan di mana data dalam segmen TCP dimulai. Field ini juga dapat berarti ukuran dari header TCP. Seperti halnya field Header Length dalam header IP, field ini merupakan angka dari word 32-bit dalam header TCP. Untuk sebuah segmen TCP terkecil (di mana tidak ada opsi TCP tambahan), field ini diatur ke nilai 0x5, yang berarti data dalam segmen TCP dimulai dari oktet ke 20 dilihat dari permulaan segmen TCP. Jika field Data Offset diset ke nilai maksimumnya (24=16) yakni 15, header TCP dengan ukuran terbesar dapat memiliki panjang hingga 60 byte.
* **Reserved**, Direservasikan untuk digunakan pada masa depan. Pengirim segmen TCP akan mengeset bit-bit ini ke dalam nilai 0.
* **Flags,** Mengindikasikan flag-flag TCP yang memang ada enam jumlahnya, yang terdiri atas: URG (Urgent), ACK (Acknowledgment), PSH (Push), RST (Reset), SYN (Synchronize), dan FIN (Finish).
* **Window,** Mengindikasikan jumlah byte yang tersedia yang dimiliki oleh buffer host penerima segmen yang bersangkutan. Buffer ini disebut sebagai Receive Buffer, digunakan untuk menyimpan byte stream yang datang. Dengan mengimbuhkan ukuran window ke setiap segmen, penerima segmen TCP memberitahukan kepada pengirim segmen berapa banyak data yang dapat dikirimkan dan disangga dengan sukses. Hal ini dilakukan agar si pengirim segmen tidak mengirimkan data lebih banyak dibandingkan ukuran Receive Buffer. Jika tidak ada tempat lagi di dalam Receive buffer, nilai dari field ini adalah 0. Dengan nilai 0, maka si pengirim tidak akan dapat mengirimkan segmen lagi ke penerima hingga nilai field ini berubah (bukan 0). Tujuan hal ini adalah untuk mengatur lalu lintas data atau flow control.
* **Checksum,** Mampu melakukan pengecekan integritas segmen TCP (header-nya dan payload-nya). Nilai field Checksum akan diatur ke nilai 0 selama proses kalkulasi checksum.
* **Urgent Pointer,** Menandakan lokasi data yang dianggap "urgent" dalam segmen.
* **Options,** Berfungsi sebagai penampung beberapa opsi tambahan TCP. Setiap opsi TCP akan memakan ruangan 32 bit, sehingga ukuran header TCP dapat diindikasikan dengan menggunakan field Data offset.



Port TCP mampu mengindikasikan sebuah lokasi tertentu untuk menyampaikan segmen-segmen TCP yang dikirimkan yang diidentifikasi dengan TCP Port Number. Nomor-nomor di bawah angka 1024 merupakan port yang umum digunakan dan ditetapkan oleh \*\*IANA|IANaplikasi, sementara port UDP merepresentasikan sebuah antrean pesan UDP untuk protokol lapisan aplikasi. Selain itu, protokol lapisan aplikasi yang menggunakan port TCP dan port UDP dalam nomor yang sama juga tidak harus sama. Sebagai contoh protokol Extended Filename Server (EFS) menggunakan port TCP dengan nomor 520, dan protokol Routing Information Protocol (RIP) menggunakan port UDP juga dengan nomor 520. Jelas, dua protokol tersebut sangatlah berbeda! Karenanya, untuk menyebutkan sebuah nomor port, sebutkan juga jenis port yang digunakannya, karena hal tersebut mampu membingungkan (ambigu).





Sebuah segmen TCP dapat memiliki flag (tanda-tanda) khusus yang mengindikasikan segmen yang bersangkutan, seperti yang disebutkan dalam tabel berikut:

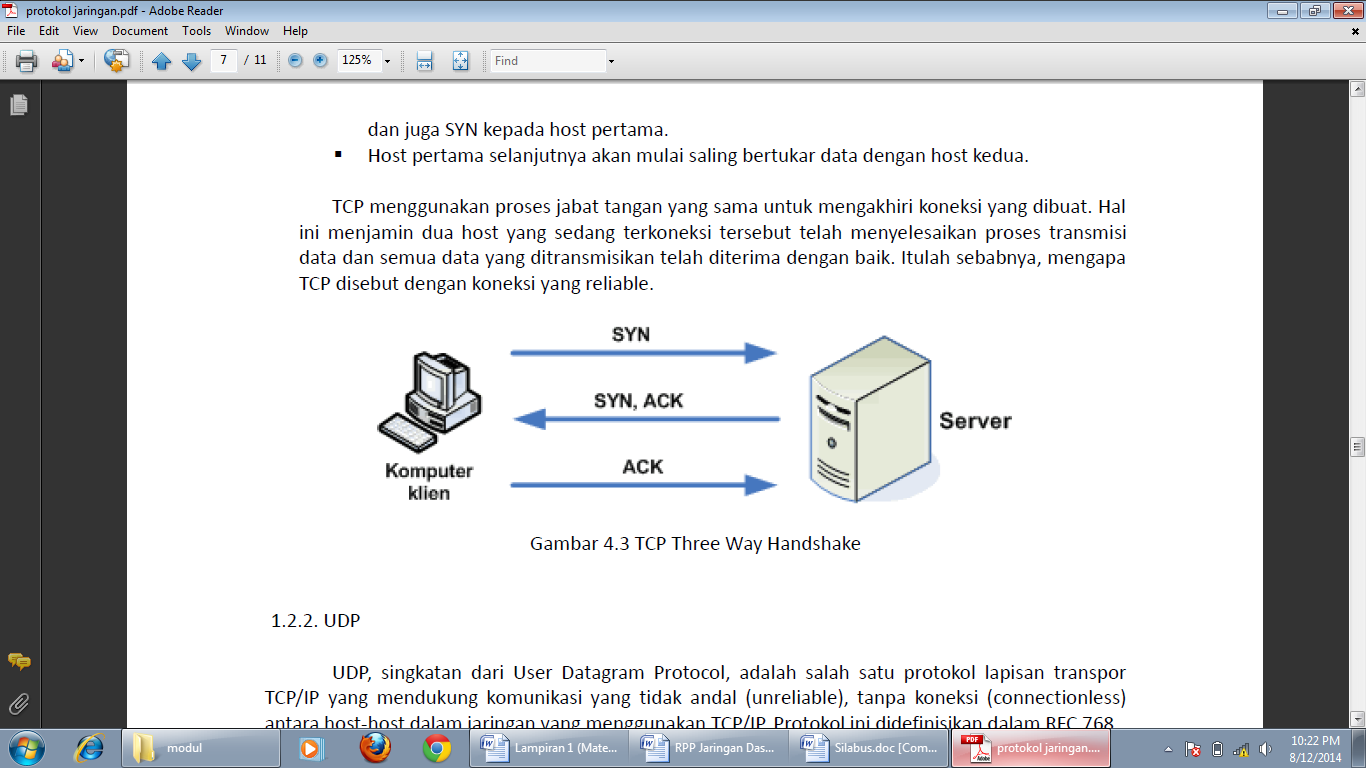
* **URG,** Mengindikasikan bahwa beberapa bagian dari segmen TCP mengandung data yang sangat penting, dan field Urgent Pointer dalam header TCP harus digunakan untuk menentukan lokasi di mana data penting tersebut berada dalam segmen.
* **ACK,** Mengindikasikan field Acknowledgment mengandung oktet selanjutnya yang diharapkan dalam koneksi. Flag ini selalu diset, kecuali pada segmen pertama pada pembuatan sesi koneksi TCP.
* **PSH,** Mengindikasikan bahwa isi dari TCP Receive buffer harus diserahkan kepada protokol lapisan aplikasi. Data dalam receive buffer harus berisi sebuah blok data yang berurutan (kontigu), dilihat dari ujung paling kiri dari buffer. Dengan kata lain, sebuah segmen yang memiliki flag PSH diset ke nilai 1, tidak bolah ada satu byte pun data yang hilang dari aliran byte segmen tersebut; data tidak dapat diberikan kepada protokol lapisan aplikasi hingga segmen yang hilang tersebut datang. Normalnya, TCP Receive buffer akan dikosongkan (dengan kata lain, isi dari buffer akan diteruskan kepada protokol lapisan aplikasi) ketika buffer tersebut berisi data yang kontigu atau ketika dalam "proses perawatan". Flag PSH ini dapat mengubah hal seperti itu, dan membuat akan TCP segera mengosongkan TCP Receive buffer. Flag PSH umumnya digunakan dalam protokol lapisan aplikasi yang bersifat interaktif, seperti halnya Telnet, karena setiap penekanan tombol dalam sesi terminal virtual akan dikirimkan dengan sebuah flag PSH diset ke nilai 1. Contoh dari penggunaan lainnya dari flag ini adalah pada segmen terakhir dari berkas yang ditransfer dengan menggunakan protokol FTP. Segmen yang dikirimkan dengan flag PSH aktif tidak harus segera di-acknowledge oleh penerima.
* **RST,** Mengindikasikan bahwa koneksi yang dibuat akan digagalkan. Untuk sebuah koneksi TCP yang sedang berjalan (aktif), sebuah segmen dengan flag RST diset ke nilai 1 akan dikirimkan sebagai respons terhadap sebuah segmen TCP yang diterima yang ternyata segmen tersebut bukan yang diminta, sehingga koneksi pun menjadi gagal. Pengiriman segmen dengan flag RST diset ke nilai 1 untuk sebuah koneksi aktif akan menutup koneksi secara paksa, sehingga data yang disimpan dalam buffer akan dibuang (dihilangkan). Untuk sebuah koneksi TCP yang sedang dibuat, segmen dengan flag RST aktif akan dikirimkan sebagai respons terhadap request pembuatan koneksi untuk mencegah percobaan pembuatan koneksi.
* **SYN,** Mengindikasikan bahwa segmen TCP yang bersangkutan mengandung Initial Sequence Number (ISN). Selama proses pembuatan sesi koneksi TCP, TCP akan mengirimkan sebuah segmen dengan flag SYN diset ke nilai 1. Setiap host TCP lainnya akan memberikan jawaban (acknowledgment) dari segmen dengan flag SYN tersebut dengan menganggap bahwa segmen tersebut merupakan sekumpulan byte dari data. Field Acknowledgment Number dari sebuah segmen SYN diatur ke nilai ISN + 1.
* **FIN,** Menandakan bahwa pengirim segmen TCP telah selesai dalam mengirimkan data dalam sebuah koneksi TCP. Ketika sebuah koneksi TCP akhirnya dihentikan (akibat sudah tidak ada data yang dikirimkan lagi), setiap host TCP akan mengirimkan sebuah segmen TCP dengan flag FIN diset ke nilai 1. Sebuah host TCP tidak akan mengirimkan segmen dengan flag FIN hingga semua data yang dikirimkannya telah diterima dengan baik (menerima paket acknowledgment) oleh penerima. Setiap host akan menganggap sebuah segmen TCP dengan flag FIN sebagai sekumpulan byte dari data. Ketika dua host TCP telah mengirimkan segmen TCP dengan flag FIN dan menerima acknowledgment dari segmen tersebut, maka koneksi TCP pun akan dihentikan.

**TCP Three-way handshake**

Proses pembuatan koneksi TCP disebut juga dengan "Three-way Handshake". Tujuan metode ini adalah agar dapat melakukan sinkronisasi terhadap nomor urut dan nomor acknowledgement yang dikirimkan oleh kedua pihak dan saling bertukar ukuran TCP Window. Prosesnya dapat digambarkan sebagai berikut:

* Host pertama (yang ingin membuat koneksi) akan mengirimkan sebuah segmen TCP dengan flag SYN diaktifkan kepada host kedua (yang hendak diajak untuk berkomunikasi).
* Host kedua akan meresponsnya dengan mengirimkan segmen dengan acknowledgment dan juga SYN kepada host pertama.
* Host pertama selanjutnya akan mulai saling bertukar data dengan host kedua.

TCP menggunakan proses jabat tangan yang sama untuk mengakhiri koneksi yang dibuat. Hal ini menjamin dua host yang sedang terkoneksi tersebut telah menyelesaikan proses transmisi data dan semua data yang ditransmisikan telah diterima dengan baik. Itulah sebabnya, mengapa TCP disebut dengan koneksi yang reliable.



**Pertemuan 18-19**

**Jenis Jenis Protocol dan Fungsinya Pada Jaringan Komputer**

**TCP/IP (Transmission Control Protocol/Internet Protocol)**

Adalah 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 (software) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP stack. Pada TCP/IP terdapat beberapa protokol sub yang menangani masalah komunikasi antar komputer. TCP/IP mengimplemenasikan arsitektur berlapis yang terdiri atas empat lapis, diantaranya adalah :

1. Protokol lapisan aplikasi
2. Protokol lapisan antar-host
3. Protokol lapisan internetwork
4. Protokol lapisan antarmuka jaringan

**UDP ( User Datagram Protokol)**

UDP, singkatan dari User Datagram Protocol, adalah salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP.

* Connectionless (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak berukar informasi.
* Unreliable (tidak andal): Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan acknowledgment. Protokol lapisan aplikasi yang berjalan di atas UDP harus melakukan pemulihan terhadap pesan-pesan yang hilang selama transmisi.
* UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi atau proses tertentu di dalam sebuah host dalam jaringan yang menggunakan TCP/IP. Header UDP berisi field Source Process Identification dan Destination Process Identification.
* UDP menyediakan penghitungan checksum berukuran 16-bit terhadap keseluruhan pesan UDP.

**Domain Name System (DNS)**

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

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.

**Point-to-Point Protocol**

Point-to-Point Protocol (sering disingkat menjadi PPP) adalah sebuah protokol enkapsulasi paket jaringan yang banyak digunakan pada wide area network (WAN). Protokol ini merupakan standar industri yang berjalan pada lapisan data-link dan dikembangkan pada awal tahun 1990-an sebagai respons terhadap masalah-masalah yang terjadi pada protokol Serial Line Internet Protocol (SLIP), yang hanya mendukung pengalamatan IP statis kepada para kliennya. Dibandingkan dengan pendahulunya (SLIP), PPP jauh lebih baik, mengingat kerja protokol ini lebih cepat, menawarkan koreksi kesalahan, dan negosiasi sesi secara dinamis tanpa adanya intervensi dari pengguna. Selain itu, protokol ini juga mendukung banyak protokol-protokol jaringan secara simultan.

**Serial Line Internet Protocol**

Serial Line Internet Protocol dianggap berkaitan erat dengan pengertian berikut  
Disingkat dengan SLIP. Sebuah protokol yang memungkinkan pemindahan data IP melalui saluran telepon. Alat bantu lainnya dalam SLIP adalah PPP yang mendeteksi kesalahan dan konfigurasi. Sistem ini memerlukan satu komputer server sebagai penampungnya, dan secara perlahan-lahan akan digantikan oleh standar PPP yang memiliki kecepatan proses lebih tinggi.

**Internet Control Message Protocol (ICMP)**

adalah salah satu protokol inti dari keluarga. ICMP berbeda tujuan dengan TCP dan UDP dalam hal ICMP tidak digunakan secara langsung oleh aplikasi jaringan milik pengguna. salah satu pengecualian adalah aplikasi ping yang mengirim pesan ICMP Echo Request (dan menerima Echo Reply) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan. protokol internet. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau.

**POP3 (Post Office Protocol)**

POP3 adalah kepanjangan dari Post Office Protocol version 3, yakni protokol yang digunakan untuk mengambil email dari email server. Protokol POP3 dibuat karena desain dari sistem email yang mengharuskan adanya email server yang menampung email untuk sementara sampai email tersebut diambil oleh penerima yang berhak. Kehadiran email server ini disebabkan kenyataan hanya sebagian kecil dari komputer penerima email yang terus-menerus melakukan koneksi ke jaringan internet.

**IMAP (Internet Message Access Protocol)**

IMAP (Internet Message Access Protocol) adalah protokol standar untuk mengakses/mengambil e-mail dari server. IMAP memungkinkan pengguna memilih pesan e-mail yang akan ia ambil, membuat folder di server, mencari pesan e-mail tertentu, bahkan menghapus pesan e-mail yang ada. Kemampuan ini jauh lebih baik daripada POP (Post Office Protocol) yang hanya memperbolehkan kita mengambil/download semua pesan yang ada tanpa kecuali.

adalah suatu  protokol yang umum digunakan untuk pengiriman surat elektronik atau email di Internet. Protokol ini gunakan untuk mengirimkan data dari komputer pengirim surat elektronik ke server surat elektronik penerima. Untuk menggunakan SMTP bisa dari Microsoft Outlook. biasanya untuk menggunakan SMTP di perlukan settingan :

* 1. Email Address : contoh —> [anda@domainanda.com](mailto:anda@domainanda.com)
  2. Incoming Mail (POP3, IMAP or HTTP) server : mail.doaminanda.com
  3. Outgoing (SMTP) server : mail.domainanda.com
  4. Account Name : [anda@domainanda.com](mailto:anda@domainanda.com)
  5. Password : password yang telah anda buat sebelumnya

**HTTP (Hypertext Transfer Protocol)**

HTTP (Hypertext Transfer Protocol) suatu protokol yang digunakan oleh WWW (World Wide Web). HTTP mendefinisikan bagaimana suatu pesan bisa diformat dan dikirimkan dari server ke client. HTTP juga mengatur aksi-aksi apa saja yang harus dilakukan oleh web server dan juga web browser sebagai responatas perintah-perintah yang ada pada protokol HTTP ini.

Contohnya bila kita mengetikkan suatu alamat atau URL pada internet browser maka web browser akan mengirimkan perintah HTTP ke web server. Web server kemudian akan menerima perintah ini dan melakukan aktivitas sesuai dengan perintah yang diminta oleh web browser. Hasil aktivitas tadi akan dikirimkan kembali ke web browser untuk ditampilkan kepada kita.

**HTTPS**  
https adalah versi aman dari HTTP, protokol komunikasi dari World Wide Web. Ditemukan oleh Netscape Communications Corporation untuk menyediakan autentikasi dan komunikasi tersandi dan penggunaan dalam komersi elektris. Selain menggunakan komunikasi plain text, HTTPS menyandikan data sesi menggunakan protokol SSL (Secure Socket layer) atau protokol TLS (Transport Layer Security). Kedua protokol tersebut memberikan perlindungan yang memadai dari serangan eavesdroppers, dan man in the middle attacks. Pada umumnya port HTTPS adalah 443.

Tingkat keamanan tergantung pada ketepatan dalam mengimplementasikan pada browser web dan perangkat lunak server dan didukung oleh algorithma penyandian yang aktual.  
Oleh karena itu, pada halaman web digunakan HTTPS, dan URL yang digunakan dimulai dengan ‘https://’ bukan dengan ‘http://’

**SSH (Sucure Shell)**

SSH adalah protocol jaringan yang memungkinkan pertukaran data secara aman antara dua komputer. SSH dapat digunakan untuk mengendalikan komputer dari jarak jauh mengirim file, membuat Tunnel yang terrenkripsi dan lain-lain. Protocol ini mempunyai kelebihan disbanding protocol yang sejenis seperti Telnet, FTP, Danrsh, karena SSH memiliki system Otentikasi,Otorisasi, dan ekripsinya sendiri. Dengan begitu keamanan sebuah sesi komunikasi melalui bantuan SSH ini menjadi lebih terjamin.

**Telnet (Telecommunication network)**

Adalah sebuah protokol jaringan yang digunakan di koneksi Internet atau Local Area Network. TELNET dikembangkan pada 1969 dan distandarisasi sebagai IETF STD 8, salah satu standar Internet pertama. TELNET memiliki beberapa keterbatasan yang dianggap sebagai risiko keamanan.

**FTP ( File Transfer Protocol )**

FTP ( File Transfer Protocol ) adalah sebuah protocol internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas (file) computer antar mesin-mesin dalam sebuah internetwork. FTP atau protocol Transmission Control Protocol (TCP) untuk komunikasi data antara klien dan server, sehingga diantara kedua komponen tersebut akan dibuatlah sebuah sesi komunikasi sebelum transfer data dimulai. FTP hanya menggunakan metode autentikasi standar, yakni menggunakan User name dan paswordnya yang dikirim dalam bentuk tidak terenkripsi. Pengguana terdaftar dapat menggunakan username dan password-nya untuk mengakses ,men-dawnload ,dan meng- updlot berkas- berkas yang ia kehenaki. Umumnya, para pengguna daftar memiliki akses penuh terdapat berapa direkotri , sehingga mereka dapat berkas , memuat dikotri dan bahkan menghapus berkas. Pengguna yang belum terdaftar dapat juga menggunakan metode anonymous login,yakni dengan menggunakan nama pengguna anonymous & password yang diisi dengan menggunakan alamat e-mail. Sebuah server FTP diakses dengan menggunakan Universal Resource Identifier (URI) dengan menggunakan format ftp://namaserver. Klien FTP dapat menghubungi server FTP dengan membuka URI tersebut.

Tujuan FTP server adalah sebagai beikut :

1. Untuk men-sharing data.
2. Untuk menyediakan indirect atau implicit remote computer.
3. Untuk menyediakan tempat penyimpanan bagi User.
4. Untuk menyediakan tranper data yang reliable dan efisien.

**LDAP**  
LDAP (Lightweight Directory Access Protocol) adalah protokol perangkat lunak untuk memungkinkan semua orang mencari resource organisasi, perorangan dan lainnya, seperti file atau printer di dalam jaringan baik di internet atau intranet. Protokol LDAP membentuk sebuah direktori yang berisi hirarki pohon yang memiliki cabang, mulai dari negara (countries), organisasi, departemen sampai dengan perorangan. Dengan menggunakan LDAP, seseorang dapat mencari informasi mengenai orang lain tanpa mengetahui lokasi orang yang akan dicari itu.

**SSL (Secure Socket Layer)**

SSL (Secure Socket Layer) adalah arguably internet yang paling banyak digunakan untuk enkripsi. Ditambah lagi, SSL digunakan tidak hanya keamanan koneksi web, tetapi untuk berbagai aplikasi yang memerlukan enkripsi jaringan end-to-end.

Secure Sockets Layer (SSL) merupakan sistem yang digunakan untuk mengenkripsi  
pengiriman informasi pada internet, sehingga data dapat dikirim dengan aman. Protokol SSL mengatur keamanan dan integritas menggunakan enkripsi, autentikasi, dan kode autentikasi pesan. SSL protocol menyedian privasi komunikasi di internet. SSL tidak mendukung fileencryption, access-control, atau proteksi virus, jadi SSL tidak dapat membantu mengatur data sensitif setelah dan sebelum pengiriman yang aman.

**Berikut adalah Jenis-Jenis dari Protocol Jaringan :**

1. **Ethernet**

**Protokol Ethernet** paling banyak di gunakan dalam sistem jaringan. Ethernet menggunakan metode akses yang disebut dengan *CSMA/CD (Carrier Sense Multiple Access/Collision Detection)* dalam mengkomunikasikan data. **Protocol Ethernet** bekerja dengan memperhatikan network atau jaringan sebelum di lakukan transformasi atau transmisi data . Apabila jalur masih sibuk maka akan dia akan menunggu melakukkan pengiriman data hingga jalur bersih dari data.

Topologi : Topologi BUS dan Topologi Star  
Kabel : Coaxial, Fiber Optic dan Twisted Pair  
Kecepatan : 10 Mbps.

1. **Local Talk**

**Local Talk** merupakan protokol jaringan dengan menggunakan metode akses yang disebut *CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)* dalam mengkomunikasikan data. **Protocol Local Talk** di Populerkan oleh Machintos atau Apple Computer. Protocol Local Talk bekerja dengan menghindari dari tabrakan saat pengiriman data. Adapter Local Talk dan Kabel Twisted Pair khusus di gunakan dalam jaringan ini melalui serial port.

Topologi : Topologi Bus  
Kabel : Twisted Pair  
Kecepatan : 230 Kbps

1. **Token Ring**

**Protokol Token Ring** di populerkan oleh IBM pada tahun 1980. Metode akses protokol Token Ring adalah melalui sebuah Token dalam sebuah lingkaran seperti cincin. Sinyal Token bergerak berputar dalam sebuah lingkaran (cincin) dalam sebuah jaringan dan bergerak dari satu komputer menuju ke komputer lainnya. Jika pada persinggahan di salah satu komputer terdapat data yang ingin ditransmisikan, Token akan mengirimkan data ke tempat yang di inginkan tersebut. Selanjutnya, Token bergerak untuk saling mengkoneksikan di antara masing-masing komputer.

Topologi : Topologi Star  
Kabel : Twisted Pair dan Fiber Optic  
Kecepatan : 4 Mbps – 11 Mbps

1. **FDDI (Fiber Distributted Data Interface)**

**FDDI** merupakan protokol jaringan dengan metode akses model Token. **FDDI** menghubungkan beberapa komputer sampai jarak yang jauh. Topologi ini bentuknya sama dengan Token Ring tetapi menggunakan 2 buah ring. Dengan Maksud apabila ring 1 ada masalah maka secara otomatis akan berpindah ke ring 2.

Topologi : Topologi Star  
Kabel : Fiber Optic  
Kecepatan : 100 Mbps

Dari ke empat macam Protocol di atas, Protocol yang paling populer atau berkembang adalah Protocol Ethernet karena Protocol Ethernet Cara Instalasi nya yang mudah dan Alat yang di pergunakan mudah untuk di cari di pasaran.

1. **TCP/IP** (singkatan dari ***Transmission Control*** *Protocol***/*Internet Protocol***) adalah standar [komunikasi](http://id.wikipedia.org/wiki/Komunikasi) [data](http://id.wikipedia.org/wiki/Data) yang digunakan oleh komunitas [internet](http://id.wikipedia.org/wiki/Internet) dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. [Protokol](http://id.wikipedia.org/wiki/Protokol_jaringan) ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol ([*protocol suite*](http://id.wikipedia.org/w/index.php?title=Protocol_suite&action=edit)). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk [perangkat lunak](http://id.wikipedia.org/wiki/Perangkat_lunak) ([software](http://id.wikipedia.org/wiki/Software)) di [sistem operasi](http://id.wikipedia.org/wiki/Sistem_operasi). Istilah yang diberikan kepada perangkat lunak ini adalah [TCP/IP stack](http://id.wikipedia.org/w/index.php?title=TCP/IP_stack&action=edit)

TCP/IP pun mempunyai beberapa layer, layer-layer itu adalah :

1. IP (internet protocol) yang berperan dalam pentransmisian paket data dari node ke node. IP mendahului setiap paket data berdasarkan 4 byte (untuk versi IPv4) alamat tujuan (nomor IP). Internet authorities menciptakan range angka untuk organisasi yang berbeda. Organisasi menciptakan grup dengan nomornya untuk departemen. IP bekerja pada mesin gateaway yang memindahkan data dari departemen ke organisasi kemudian ke region dan kemudian ke seluruh dunia.
2. TCP (transmission transfer protocol) berperan didalam memperbaiki pengiriman data yang benar dari suatu klien ke server. Data dapat hilang di tengah-tengah jaringan. TCP dapat mendeteksi error atau data yang hilang dan kemudian melakukan transmisi ulang sampai data diterima dengan benar dan lengkap.
3. Sockets yaitu merupakan nama yang diberikan kepada subrutin paket yang menyediakan akses ke TCP/IP pada kebanyakan sistem.

**Pengertian IP address**

Internet Protocol Address merupakan singkatan dari IP address. [Pengertian IP address](http://belajar-komputer-mu.com/memahami-pengertian-ip-address/) adalah suatu identitas numerik yang dilabelkan kepada suatu alat seperti komputer, router atau printer yang terdapat dalam suatu jaringan komputer yang menggunakan internet protocol sebagai sarana komunikasi. IP address memiliki dua fungsi, yakni:

1. Sebagai alat identifikasi host atau antarmuka pada jaringan.

Fungsi ini diilustrasikan seperti nama orang sebagai suatu metode untuk mengenali siapa orang tersebut. dalam jaringan komputer berlaku hal yang sama.

1. Sebagai alamat lokasi jaringan.

Fungsi ini diilustrasikan seperti alamat rumah kita yang menunjukkan lokasi kita berada. Untuk memudahkan pengiriman paket data, maka IP address memuat informasi keberadaannya. Ada rute yang harus dilalui agar data dapat sampai ke komputer yang dituju.

IP address menggunakan bilangan 32 bit. Sistem ini dikenal dengan nama Internet Protocol version 4 atau IPv4. Saat ini IPv4 masih digunakan meskipun sudah ada IPv6 yang diperkenalkan pada tahun 1995. Hal ini dikarenakan tingginya pertumbuhan jumlah komputer yang terkoneksi ke internet. Maka dibutuhkan alamat yang lebih banyak yang mampu mengidentifikasi banyak anggota jaringan.

**Format IP address**

Sebenarnya pengalamatan IP address menggunakan bilangan biner. Namun supaya lebih mudah ditulis dan dibaca oleh manusia, maka IP address ditulis dengan bilangan 4 desimal yang masing-masing dipisahkan oleh titik. Format penulisan ini disebut sebagai *dotted-decimal notation*. Setiap bilangan desimal merupakan nilai dari satu oktet atau delapan bit alamat IP. Sebagai contoh adalah sebagai berikut:

192.168.1.1

Jika dikonversi menjadi bilangan biner adalah sebagai berikut:

11000000.10101000.1.1