

PERCOBAAN I

Pengenalan

JARINGAN KOMPUTER

1.1. Tujuan

- Mengetahui jaringan komputer yang sering digunakan saat ini
- Mengetahui *communication model (reference model) OSI (Open System Interconnection)* dasar pada sistem komputer yang menyediakan komunikasi satu dengan lainnya serta hubungannya dengan *communication model TCP/IP*

1.2. Peralatan Yang Digunakan

- Perangkat komputer yang menggunakan sistem operasi OpenBSD
- Perangkat komputer disertai perangkat tambahan *keyboard*
- Perangkat jaringan yang menggunakan kabel UTP dengan konektor RC45, NIC, HUB, atau *switch*

1.3. Teori Dasar

Jaringan komputer dibentuk dengan menghubungkan beberapa komputer (*host*) dan perangkat jaringan (*bridge, router, gateway, firewall*) sehingga menjadi suatu jaringan komputer lokal. Komputer dan perangkat jaringan ini secara umum disebut sebagai *node*. Media penghubung antar *node-node* pada jaringan komputer dapat berupa kabel, gelombang mikro maupun fiber [Comer, D. E., 1997][Shay, W. A., 1995].

1.3.1. Model Internetworking

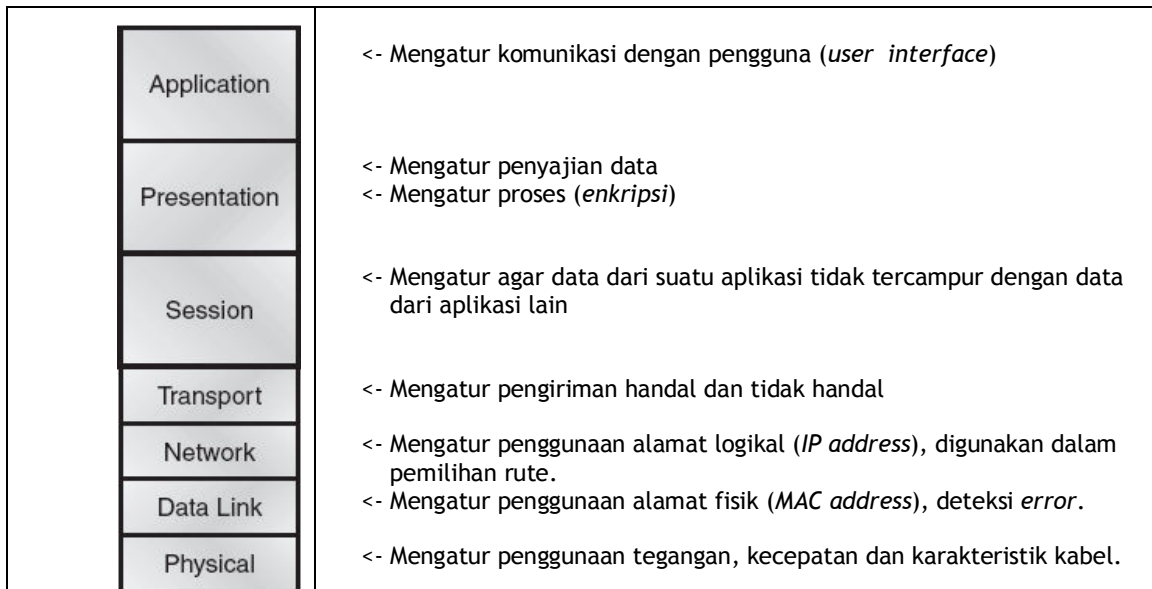
Ada dua arsitektur utama *network*, model OSI dan model TCP/IP. Model OSI kini mulai jarang digunakan, namun memiliki model yang lengkap dan detail. TCP/IP sebaliknya, memiliki model yang kurang detail, namun digunakan secara luas. OSI merupakan model referensi *de jure*, sementara TCP merupakan model *de facto*.

❖ Model OSI

Untuk menyelenggarakan komunikasi berbagai macam *vendor* komputer, diperlukan sebuah aturan baku yang standar dan disetujui berbagai pihak. Seperti halnya dua orang yang berlainan bangsa, maka untuk berkomunikasi memerlukan penerjemah/*interpreter* atau satu bahasa yang dimengerti kedua belah pihak. Dalam dunia komputer dan telekomunikasi, *interpreter* identik dengan protokol. Untuk itu maka badan dunia yang menangani masalah standardisasi ISO (*International Standardization Organization*) pada akhir 70an, membuat aturan baku yang dikenal dengan nama model referensi OSI (*Open System Interconnection*). Dengan demikian diharapkan semua *vendor* perangkat telekomunikasi harus berpedoman pada model referensi ini dalam mengembangkan protokolnya.

Model referensi OSI terdiri dari 7 lapisan, mulai dari lapisan fisik hingga aplikasi. Model referensi ini tidak hanya berguna untuk produk-produk LAN saja, tetapi juga sangat diperlukan dalam membangun jaringan Internet. OSI menjelaskan bagaimana data dan informasi jaringan berkomunikasi dari sebuah aplikasi pada sebuah komputer berjalan melalui jaringan, menuju ke aplikasi di komputer lain. OSI menjelaskan melalui pendekatan pemecahan menjadi lapisan-lapisan (*layer*). Analogi konsep *layer* adalah seperti dalam departemen / bidang dalam sebuah perusahaan, setiap departemen memiliki tugas yang berbeda, dan hanya terfokus pada hal tertentu sesuai pembagian tugas. Hubungan antara model referensi OSI dengan protokol Internet dapat dilihat pada Tabel 1.1. Setiap *layer* mewakili suatu abstraksi yang berbeda dengan lainnya dan melaksanakan suatu fungsi yang telah didefinisikan [Tanenbaum, 1996].

OSI memiliki 7 *layer*, dimana dapat dibagi menjadi 2 group. Tiga layer teratas mendefinisikan bagaimana antara aplikasi dalam jaringan dapat berkomunikasi, juga antara aplikasi dengan pengguna. Empat layer terbawah mendefinisikan bagaimana data ditransmisikan dalam jaringan.



Gambar 1. 1 Fungsi tiap-tiap layer secara umum

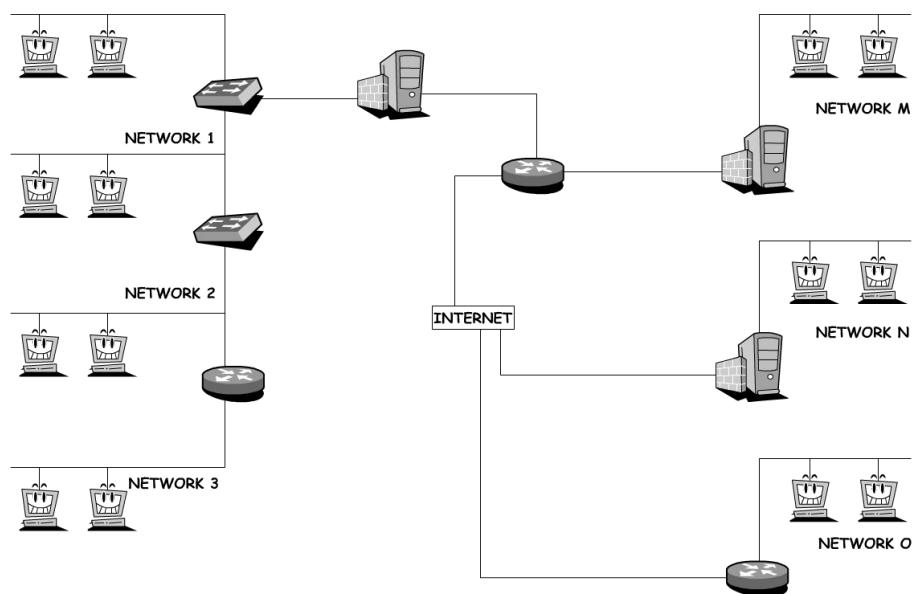
Tabel 1.1 Perbandingan Referensi Model OSI, Model TCP/IP, dan Protokol.

OSI	Protocol OSI	TCP/IP	Protokol TCP/IP	
Lapisan	Nama Protokol	Lapisan	Nama Protokol	Kegunaan
Aplikasi	File transfer, email dan akses ke database	Aplikasi	DHCP (Dynamic Host Configuration Protocol)	Protokol untuk distribusi IP pada jaringan secara otomatis
Presentasi	ASCII, EBCDIC, MIDI, MPEG, TIFF, JPEG, PICT, Quick Time			
Sessi	SQL, NetBEUI, RPC, Xwindows		DNS (Domain Name Server)	Database nama domain mesin dan nomer IP
			FTP (File Transfer Protocol)	Protokol untuk transfer <i>file</i>
			HTTP (HyperText Transfer Protocol)	Protokol untuk transfer <i>file</i> HTML (<i>web</i>)
		MIME (Multipurpose Internet Mail Extention)	Protokol untuk mengirim <i>file binary</i> dalam bentuk teks	
		NNTP (Network News Transfer Protocol)	Protokol untuk menerima dan mengirim <i>newsgroup</i>	

			POP (Post Office Protocol)	Protokol untuk mengambil <i>mail</i> dari <i>server</i>
			SMB (Server Message Block)	Protokol untuk transfer berbagai <i>server</i> file DOS dan Windows
			SMTP (Simple Mail Transfer Protocol)	Protokol untuk mengirim mail ke client
			SNMP (Simple Network Management Protocol)	Protokol untuk manajemen jaringan
			Telnet (Telephone Networking)	Protokol untuk akses dari jarak jauh
			NETBIOS (Network Basic Input Output System)	BIOS jaringan standar. Digunakan pada <i>file sharing</i>
			RPC (Remote Procedure Call)	Prosedur pemanggilan jarak jauh
			SOCKET	Input Output untuk <i>network</i> jenis BSD-UNIX
Transport	TCP, UDP, SPX	Transport	TCP (Transmission Control Protocol)	Protokol pertukaran data berorientasi (<i>connection oriented</i>)
			UDP (User Datagram Protocol)	Protokol pertukaran data non-orientasi (<i>connectionless</i>)
Network	IP, IPX, ARP, RARP, ICMP, RIP, OSFT, BGP	Internet	IP (Internet Protocol)	Protokol untuk menetapkan <i>routing</i>
			RIP (Routing Information Protocol)	Protokol untuk memilih <i>routing</i>

				ARP (Address Resolution Protocol)	Protokol untuk mendapatkan alamat MAC dari nomer IP
				ICMP (Internet Control Message Protocol)	Protokol biasa digunakan dalam ping
				RARP (Reverse ARP)	Protokol untuk mendapatkan informasi nomer IP dari alamat MAC
Datalink	LLC	SLIP, PPP, MTU	Network Interface	PPP (Point to Point Protocol)	Protokol untuk <i>point ke point</i>
	MAC			SLIP (Serial Line Internet Protocol)	Protokol dengan menggunakan sambungan serial
Fisik		10BaseT, 100BaseTX, HSSI, V.35, X.21		Ethernet, FDDI, ISDN, ATM	

Suatu jaringan komputer lokal dan jaringan komputer lokal lainnya dihubungkan sehingga membentuk suatu jaringan komputer global atau yang lebih dikenal dengan Internet global (atau Internet) [Tanenbaum, A. S., 1996]. Jaringan komputer global (Internet) dapat digambarkan secara sederhana seperti yang ditunjukkan dalam Gambar 1.2



Gambar 1. 2 Jaringan Komputer Global (Internet)

Setiap *node* di jaringan komputer harus mempunyai identitas. Di dalam protokol TCP/IP¹ - yang biasa digunakan untuk berkomunikasi antar *node* di Internet - [Clark, D. D, 1988], identitas tersebut berupa alamat IP (*Internet Protokol*) [Anonim, 1981a][Su, Z. S., 1983][Tanenbaum, A. S., 1996]. Identitas ini diperlukan agar setiap *node* dapat berkomunikasi dengan baik satu dengan lainnya. Suatu *node* yang mengirim data harus mengetahui kemana data ditujukan. Sebaliknya suatu *node* yang menerima data harus mengetahui dari mana asal data tersebut.

Sebagaimana disebutkan di atas, bahwa di Internet setiap *node* berkomunikasi menggunakan protokol TCP/IP. Protokol ini pada dasarnya meliputi beberapa lapisan di protokol TCP/IP seperti dalam Tabel 1.1 Protokol TCP/IP yang terdiri dari 4 lapisan ini sedikit berbeda dengan protokol OSI yang berjumlah 7 lapisan². [Washburn, K., dan Evans, J., 1996][Wilder, F., 1993].

❖ **Analogi jaringan TCP/IP dan Sistem Postal**

Paket TCP/IP mirip dengan surat atau paket pos. Keduanya memiliki alamat pengiriman dan alamat penerima. Mengirim sebuah file pada suatu jaringan layaknya seperti kita mengirim sebuah *mobil* (dengan bagian-bagian yang dipisahkan untuk alasan efisiensi) kepada seseorang di New York US dan kita berada di Malang

- Diperlukan banyak paket untuk mengirim bagian mobil secara keseluruhan
- Paket individual (paket pos) dapat berjalan pada rute yang berbeda, sekalipun berasal dari sumber yang sama dan menuju tujuan yang sama
- Ketika kita mengirimkan sebuah paket, saya tidak tahu rute mana yang dipakai. Paket tidak berisi informasi yang menyebutkan rute mana yang diambil, hanya informasi dari mana dia berasal dan alamat tujuan akhir.
- Pengirim perlu tahu alamat tujuan, tapi tidak harus tahu tentang jaringan/lokasi tujuan atau dimana jaringan itu berada.
- Paket pos dikirim ke tujuan tahap demi tahap, dan di setiap tahap petugas pos (*router*) memutuskan ke mana paket pos itu dikirim. Sebagai contoh, saya mengantarkan paket pos ke kantor pos. Petugas resepsionis menaruhnya di “tempat surat” kantor. Tukang pos mengambilnya ... berangkat ke kantor pusat ... ke bandara Juanda menitipkannya pada pesawat ... tiba di bandara NewYork ... ke kantor pos setempat ... ke alamat penerima.

¹ TCP/IP merupakan singkatan dari Transmission Control Protocol/Internet Protocol. Protokol komunikasi ini merupakan standard bagi setiap node untuk bertukar data di jaringan komputer global (Internet).

² Protokol TCP/IP telah digunakan di jaringan komputer Internet sebagai suatu standard, karena lebih sesuai untuk internetworking dan menghilangkan beberapa layer OSI yang dianggap tidak penting. Meskipun demikian, antara model OSI dan model TCP/IP mempunyai kesamaan fungsi.

- Petugas resepsionis barangkali melakukan hal yang lain untuk suatu kondisi khusus, jika bandara Juanda tertutup kabut, maka kantor pos akan mengirimkan menggunakan bandara lain. Hal ini memastikan sistem tetap tangguh, walaupun terdapat bagian sistem yang terganggu.

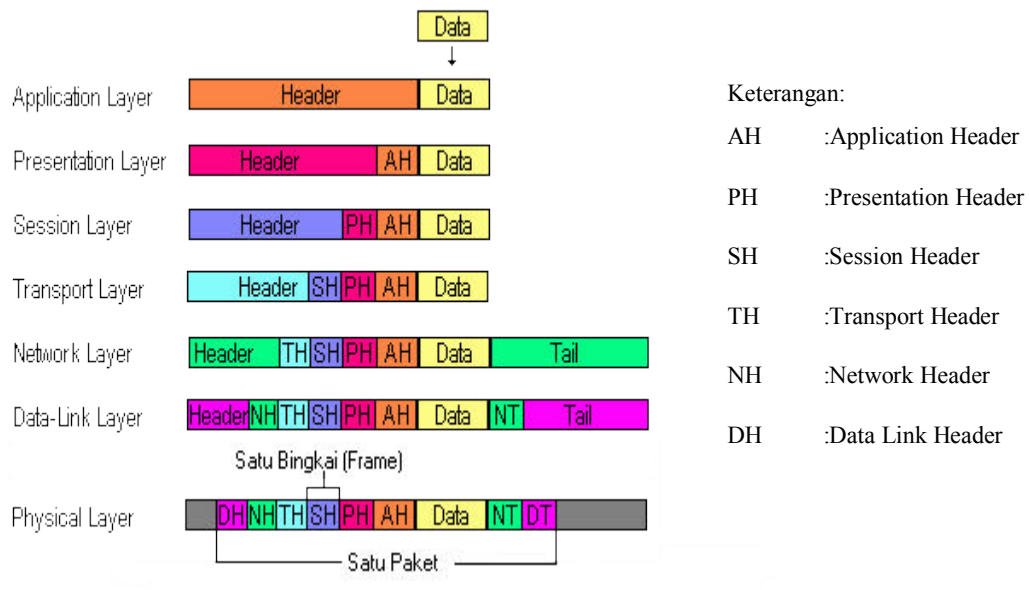
❖ **Analogi penggunaan router dalam sistem pos**

Router bertugas seperti petugas pos pada sistem pos. Ketika kita akan mengirimkan kue kepada tetangga kita, maka yang perlu kita lakukan adalah berjalan ke rumah tetangga tersebut tanpa bantuan petugas pos. Begitu pula host pada suatu network tidak memerlukan router bila paket dikirimkan dengan tujuan satu network (tetangga). Tetapi kita membutuhkan petugas pos ketika kita mengirimkan kepada teman kita di New York. Begitu pula router dibutuhkan dalam pengiriman antar network.

❖ **Konsep Enkapsulasi**

Enkapsulasi adalah proses penambahan header dan ending pada data, atau pembungkusan data. Header menandakan awal data, dan seringkali berisi alamat dan hal-hal lain, bergantung pada protokol dan layer. Ending bit digunakan untuk pengecekan eror.

Jika suatu protokol menerima data dari protokol lain di layer atasnya, ia akan menambahkan informasi (header dan ending) tambahan miliknya ke data tersebut. Informasi ini memiliki fungsi yang sesuai dengan fungsi protokol tersebut. Setelah itu, data diteruskan lagi ke protokol pada layer dibawahnya. Kadang - kadang, protokol layer memecah data (termasuk header ending layer diatasnya) menjadi beberapa unit data yang lebih kecil. Dan setiap unit kecil dibungkus dengan sebuah header baru protokol layer tersebut. Semakin rendah layer, data menjadi lebih kecil dan lebih seragam. Hal yang sebaliknya terjadi jika suatu protokol menerima data dari protokol lain yang berada pada layer dibawahnya. Jika data ini dianggap valid, protokol akan melepas informasi tambahan tersebut, yang berada pada layer di atasnya.



Gambar 1. 3 Enkapsulasi data dalam Model OSI

Topologi Jaringan Komputer

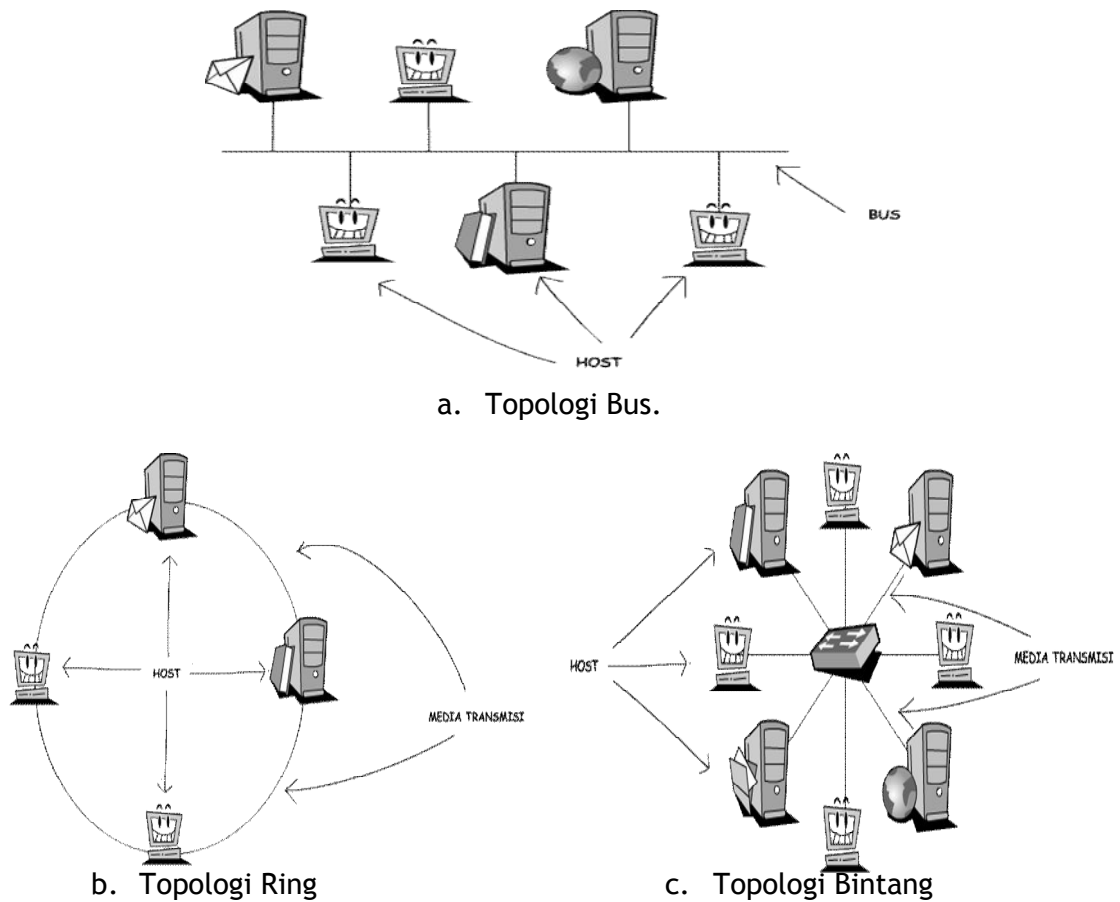
Topologi menggambarkan struktur jaringan atau bagaimana sebuah jaringan didesain. Terdapat dua definisi topologi:

- *Topologi fisik*, merupakan *lay out* aktual dari kabel-kabel (media) jaringan
 Topologi jaringan komputer³ dapat dibentuk dalam beberapa bentuk, yaitu topologi Bus, topologi Ring dan topologi Bintang [Tanenbaum, A. S., 1996].
- *Topologi logik*, mendefinisikan bagaimana media diakses oleh host-host

[Rafiudin R, 2003]

Pada intinya jaringan komputer adalah jaringan kabel, dimana bentuk dan fungsi dari jaringan tersebut menentukan pemilihan jenis kabel. Demikian juga sebaliknya, ketersediaan kabel dan harga menjadi pertimbangan utama untuk membangun sebuah jaringan (baik *home network*, *SOHO network* ataupun jaringan kelas raksasa seperti MAN - *metropolitan area network*).

³ Topologi jaringan dijelaskan sebagaimana suatu jaringan komputer itu disusun dengan node-nodenya.



Gambar 1. 4 Topologi Fisik Jaringan Komputer

Masing-masing topologi mempunyai cara yang berbeda untuk mengirimkan data dari suatu *node* ke *node* lainnya. Topologi Bus kerap menggunakan teknik CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*). Topologi Ring menggunakan teknik Token Ring, sedangkan topologi Bintang dapat menggunakan teknik ATM (*Asynchronous Transfer Mode*).

Topologi Logik dari sebuah jaringan menggambarkan bagaimana host-host saling berkomunikasi melalui sebuah media. Dua tipe umum dari Topologi logik adalah *Broadcast* dan *Token-passing*.

Ethernet

Ethernet adalah sistem jaringan yang dibuat dan dipatenkan oleh perusahaan Xerox. Ethernet merupakan implementasi metode CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) yang dikembangkan tahun 1960 pada proyek *wireless ALOHA* di Hawaii University di atas kabel coaxial. Standardisasi sistem ethernet dilakukan sejak tahun 1978 oleh IEEE. Kecepatan transmisi data di ethernet sampai saat ini adalah 10, 100 sampai 1000 Mbps.

Pada metoda CSMA/CD, sebuah host komputer yang akan mengirim data ke jaringan mula-mula memastikan bahwa jaringan sedang tidak dipakai untuk transfer dari dan oleh host komputer lainnya. Jika pada tahap pengecekan ditemukan transmisi data lain dan terjadi tabrakan (*collision*), maka host komputer tersebut diharuskan mengulang permohonan (*request*) pengiriman pada selang waktu berikutnya yang dilakukan secara acak (*random*). Dengan demikian maka jaringan efektif bisa digunakan secara bergantian.

Untuk menentukan pada posisi mana sebuah host komputer berada, maka tiap-tiap perangkat ethernet diberi alamat (*address*) sepanjang 48 bit yang unik. Informasi alamat disimpan dalam chip yang biasanya nampak pada saat komputer di start dalam urutan angka berbasis 16, seperti pada Gambar 2.

```
NE*000 ethercard probe at 0x300: 00 40 05 61 20 e6  
eth0: NE2000 found at 0x300, using IRQ 9.
```

Gambar 1. 5 Contoh ethernet address

Agar mudah dimengerti, 48 bit angka dikelompokkan masing-masing 8 bit untuk mendapatkan bilangan berbasis 16 seperti contoh di atas (00 40 05 61 20 e6), 3 angka didepan adalah kode perusahaan pembuat chip tersebut. Chip diatas dibuat oleh ANI Communications Inc. linformasi lebih lengkap lainnya dapat diperoleh di <http://standards.ieee.org/regauth/oui/index.html> [Prihanto H, 2003].

Tugas Pendahuluan

1. Tuliskan proses pengiriman data pada model komunikasi TCP/IP

2. Jelaskan pengertian *device-device* berikut ini! Jelaskan pula di layer mana *device* ini beroperasi!

a. Hub :

b. NIC :

c. Switch :

d. Bridge :

e. Router :

3. Sebut dan jelaskan perbedaan switch dan hub!

4. Jelaskan fungsi dan prinsip kerja tcpdump, beserta perintah dan opsi.

1.4. Prosedur Percobaan

1. Login ke komputer bersistem operasi OpenBSD.
2. Mengkonfigurasi TCP/IP
 - a) Mengecek konfigurasi awal

```
# ifconfig -a
```

```
# ifconfig [interface name] down
```

Jelaskan apa yang terjadi

Lepas kabel UTP yang menancap di komputer Anda

```
# ifconfig -a
```

Apakah ada perubahan pada output. Jelaskan bila ada.

Pasang kembali kabel UTP

- b) Mengkonfigurasi default gateway

Konfigurasi default gateway yg terdapat dalam file
/etc/mygate

- c) Mengedit konfigurasi ip address

```
# vi /etc/hostname.[nama interface]
```

Ganti konfigurasi ip address tersebut dengan

```
inet 10.100.100.2x 255.255.255.0 NONE
```

Dimana "x" adalah digit terakhir no meja praktikum

- d) Merestart konfigurasi network

```
# sh /etc/netstart
```

- e) Mengecek hasil konfigurasi yang baru

```
# ifconfig -a
```

Tulis dan jelaskan output perintah diatas?

f) Mengecek koneksitas ke host tetangga!

```
# ping [dua_ip_tetangga_Anda]
```

Tulis dan jelaskan output perintah di atas?

3. Menganalisis MAC Address

a) Mengecek MAC Address ethernet komputer lokal

```
# ifconfig -a
```

Tulis dan jelaskan MAC Address komputer yang Anda pakai

4. Mengecek MAC Address ethernet komputer yang terhubung ke komputer lokal

```
# arp -an
```

Tulis dan jelaskan output perintah diatas, dan apa yang Anda temukan dari output tersebut.

ARP - Bagaimana mesin saya menemukan alamat ethernet mesin Anda

Saya tahu IP address Anda, tetapi memerlukan alamat ethernet Anda supaya saya dapat mengirim paket pada Anda. TCP/IP memecahkan masalah ini dengan menggunakan ARP - *address resolution protocol*. Saya mem-*broadcast*, bertanya siapa yang mempunyai IP address a.b.c.d (ip address Anda). Anda menjawab dengan memberitahu saya alamat ethernet. Kita kemudian dapat berkomunikasi. Secara lengkap inilah yang terjadi.

- Saya mengirim sebuah broadcast ethernet, berisi paket permintaan ARP kepada payload/data field. Paket ARP berisi IP address yang MAC address-nya saya perlukan - katakanlah 10.9.8.7 (alamat IP address Anda). Tcpcmdump menunjukkan sebagai "arp who has 10.9.8.7 tell 10.9.8.8". Sambil mengirimkan paket pertanyaan, mesin saya juga mengirimkan MAC addressnya.
- Semua mesin pada network ini menerima paket tersebut, mengekstrak paket ARP, dan melihat IP address yang ada di dalamnya. Jika alamat tidak cocok dengan IP address mesin, maka paket ditolak.
- Mesin 10.9.8.7 menjawab ke mesin saya (10.9.8.8) dengan paket ARP yang diminta, berisi MAC address dari .7 (Mesin Anda tidak membroadcast jawaban karena hanya .8 yang meminta). Tcpcmdump memperlihatkan sebagai "arp-reply 10.9.8.7 is at a.b.c.d.e.f"
- .8 (mesin saya) sekarang tahu MAC address dari .7, dan dapat berkomunikasi dengan bebas.

Mekanisme di atas berlaku untuk komunikasi dalam satu network, karena ketika IP address tujuan berada diluar range network (yang ditentukan oleh mekanisme AND antara IP address dan netmask), maka paket akan dikirimkan ke router (*default gateway*). Begitu pula komunikasi antara router- router yang berhubungan, hingga sampai ke *gateway* host tujuan. Mekanisme ARP akan digunakan kembali pada gateway host tujuan.

5. Menggunakan ping untuk membangkitkan traffic tes antara dua mesin.

```
# arp -an
```

```
# arp -d [setiap ip address pada output arp -an]
```

```
# tcpdump -n arp or icmp
```

Pada terminal 2 [tekan Ctrl-Alt-F2]

```
# ping -c3 -n [ip address tetangga]
```

a) Tulis dan jelaskan output perintah diatas? Analisis apa yang terjadi?

ARP cache

TCP/IP memiliki sepasang record (IP address dan MAC address) pada cache ARP-nya. Ini hanya cache dan bukan penyimpanan permanent. Sekali sebuah entri mencapai umur tertentu, maka TCP/IP akan menghapusnya. Dengan demikian cache tidak terus menerus bertambah dan memecahkan masalah bagaimana mendeteksi apakah MAC address mengubah IP address tertentu (misal jika kita harus mengganti LAN card yang rusak). Di lain pihak ini berarti dialog ARP sering diulang, dan jawabannya selalu sama. Kita juga dapat memanipulasi ARP dengan perintah tertentu, untuk keterangan lebih lanjut ketik `man arp`.

6. Menganalisis route paket ke host tujuan

a. Ubah ip address komputer Anda menjadi 10.100.100.x, dimana x adalah nomor meja Anda.

b. Amati route paket ke:

- 10.100.100.63
- 172.17.63.129
- 172.17.63.241
- 172.17.100.130
- brawijaya.ac.id
- google.com

dengan perintah:

```
# traceroute [host_tujuan]
```


Tulis dan jelaskan output perintah diatas? Analisis apa yang terjadi?

Protokol TCP

Dalam protokol TCP/IP, IP berperan memindahkan paket dari mesin sumber ke mesin tujuan melalui router (bila diperlukan). Namun sayangnya **IP adalah protokol yang tidak handal**. Protokol ini sangat baik dalam mengirimkan data, tetapi paket tersebut dapat hilang. Misalnya jika ada kegagalan router atau koneksi terputus. Saat itu semua terjadi paket tersebut hilang tanpa ada pesan kesalahan. Untuk banyak aplikasi hal ini tidak dapat diterima, dan disinilah kegunaan TCP. TCP adalah protokol jaringan yang handal, yang dibutuhkan untuk bekerja sama bersama protokol IP. Protokol ini bekerja berkelanjutan untuk **menjamin pengiriman data Anda sesuai dengan urutan pengiriman sehingga si pengirim yakin bahwa si penerima akan menerima tepat seperti apa yang pengirim kirimkan**. Alasan lain mengapa kita memerlukan TCP adalah, IP meroutekan paket hanya pada tingkat mesin. Begitu paket tersebut tiba pada suatu mesin, **IP tidak memiliki mekanisme untuk membedakan aplikasi mana yang menggunakan paket tersebut** atau untuk membedakan antara banyak koneksi dalam aplikasi tunggal. TCP mengatasi hal tersebut dengan menggunakan **nomor port yang unik** pada masing-masing koneksi. IP adalah tanpa koneksi yaitu paket ditransmisikan secara individu dan benar-benar saling bebas. Untuk banyak aplikasi hal ini tidak cocok, karena seharusnya komunikasi data ditampilkan suatu sesi secara keseluruhan. Misalnya dalam popmail server, perintah *retrieve message* hanya dimungkinkan jika user telah memasukkan username dan password yang valid, tentunya proses ini harus berlangsung secara berurutan.

Analogi TCP/IP

Kita akan menggunakan analogi service post lagi untuk menjelaskan bagaimana TCP bekerja. Misalkan saya ingin mengirim kepada Anda suatu buku sebagai kartu pos berseri. Karena kartu pos dapat tiba tidak tepat waktu

- Anda memerlukan beberapa cara untuk mengetahui urutan pengiriman
- ... dan Anda harus mampu memberi tahu pada saya kapan Anda menerima kartu pos serta saat Anda kehilangan beberapa kartu saya dapat mengirim ulang.
- Anda juga harus mampu mendeteksi kartu pos yang terduplikasi.

Berikut ini cara-cara menangani persoalan tersebut:

- Sebelum saya mulai mengirim saya harus mengatakan kepada Anda bahwa saya akan mengirim sebuah buku, jadi Anda tahu apa yang Anda harus lakukan dengan paket pos tersebut. Saya juga memungkinkan kepada Anda mengirimkan beberapa buku dan artikel majalah yang berbeda dalam beberapa koneksi berbeda, atau Anda mungkin juga sedang mengirimkan paket kepada saya. TCP mengatasi hal ini dengan menggunakan alamat port, ip address tujuan dan alamat port, ip address asal.
- Saya meletakkan nomor urut pada kartu tersebut, sehingga Anda dapat mengurutkannya ke urutan yang benar.
- Begitu Anda selesai menerima seluruh paket, Anda mengirimkan kepada saya kartu (paket) pemberitahuan yang menyatakan pada saya kartu terakhir telah Anda terima. Dengan demikian saya dapat mengetahui jika dalam pengiriman ada kartu yang hilang.
- Kita tidak harus tahu isi paket, bahkan jika mengirimkan paket buku dalam bahasa Urdu, sistem tersebut tetap bekerja, dan saya yakin Anda menerima apa yang saya kirimkan (TCP hanya mengirimkan data ke aplikasi tanpa menginterpretasikan ke suatu arti tertentu, hanya layer aplikasi lah yang tahu gambar.jpeg adalah suatu file gambar dan bagaimana menanganinya).
- Hanya Anda dan saya yang memperhatikan nomor urut kartu, orang lain di antara kita, pegawai pos (router) hanya meneruskan paket ke tujuannya (layer TCP hanya digunakan pada mesin sumber dan tujuan).

Koneksi dan Port TCP

Aplikasi klien menggunakan nomor port untuk memberi tahu mesin tujuan servis TCP mana yang diinginkan. Server untuk aplikasi tertentu mendengarkan *well-known* port untuk mengetahui koneksi dari klien yang meminta servisnya. Agar suatu aplikasi dapat berkomunikasi dengan aplikasi lain, maka dua aplikasi tersebut harus membangun koneksi TCP di antara mereka. Koneksi TCP biasanya dibangun dengan menggunakan model klien/server. Server untuk aplikasi tersebut bekerja

sepanjang waktu menunggu dan mendengar permintaan koneksi yang datang dari klien. Saat mendeteksi adanya koneksi, server membangun koneksi TCP dengan klien yang meminta. Mereka sekarang dapat menggunakan koneksi ini untuk bertukar data hingga salah satu atau keduanya menghentikan koneksi tersebut. Penjelasan tersebut memunculkan beberapa pertanyaan tentang bagaimana koneksi bekerja:

- Misalnya Anda ingin *browse* beberapa halaman web di server saya. Bagaimana TCP dalam browser web Anda memberi tahu pada saya bahwa Anda ingin menggunakan server web dan bukan servis server yang lain (yang juga saya tawarkan).
- Saat permintaan koneksi TCP datang dari Anda, bagaimana saya tahu server aplikasi mana yang harus melayani?
- Jika Anda memiliki beberapa koneksi TCP ke server saya, semua paket tersebut melalui kabel yang sama. Bagaimana server saya tahu cara menanganinya untuk setiap koneksi (seperti saat Anda membuka web saya dengan beberapa tab pada browser)? Dan jika teman Anda melakukan hal yang sama, bagaimana server tersebut menanganinya?

Inilah kegunaan port TCP yang sesungguhnya:

- Port adalah alamat yang membedakan koneksi TCP yang berbeda-beda pada mesin yang sama, sedangkan IP address adalah nomor yang mengidentifikasi mesin mana yang menjadi tujuan/sumber suatu paket. Nomor port khusus dialokasikan dengan konversi ke servis tertentu. Anda dapat melihatnya di `/etc/services`.

Tabel 1.2 *Well-known Port*

Servis	Port
Telnet	23
Email	25
Web	80
ftp	21
Ssh	22

Server untuk servis tertentu mendengarkan pada *well-known* port yang sesuai, misalnya server web mendengar pada port 80 dan memperlakukan permintaan apapun yang datang pada port tersebut sebagai permintaan http dan memprosesnya sesuai dengan permintaan tersebut

- Klien menetapkan port tujuan mana yang ingin dihubungkan saat mengeluarkan permintaan koneksi ke server. Klien juga menetapkan port sumber secara random yang digunakan untuk melakukan koneksi. Setiap mesin tidak boleh menggunakan port sumber yang masih digunakan oleh koneksi sebelumnya (sepanjang koneksi tersebut masih aktif). Suatu kombinasi port dan IP digunakan sebagai berikut:

2. Nomor IP sumber (N1)
3. Nomor port sumber (P1)
4. Nomor IP tujuan (N2)
5. Nomor port tujuan (P2)

N1, N2 dan P2 dapat sama untuk beberapa koneksi, namun P1 harus tidak pernah sama pada suatu mesin.

7. Pastikan sshd aktif pada komputer Anda (server)
8. Menganalisis port yang terbuka pada mesin server\

```
# netstat -l -n|more
```

Tulis dan jelaskan output perintah diatas? Analisis apa yang terjadi?

```
# nmap -PO [ip_tujuan]
```

Tulis dan jelaskan output perintah diatas? Analisis apa yang terjadi? Apakah perbedaannya dengan perintah netstat.

9. Menganalisis IP address asal dan IP address tujuan, port asal, port tujuan dalam sebuah sesi koneksi. Praktikan bergantian menjadi client dan server.

a) Menganalisa paket dari komputer client

1. SSH lah ke komputer tetangga Anda

```
# ssh [ip_tetangga]
```

2. Amati IP asal, IP tujuan, port asal, port tujuan yang Anda gunakan pada sesi koneksi tersebut

```
# netstat -l -n |grep ESTABLISHED
```

Tulis dan jelaskan output perintah diatas? Analisis apa yang terjadi?

b) Menganalisa paket dari komputer server (saat praktikan lain menjadi client)

```
# netstat -l -n |grep ESTABLISHED
```

Tulis dan jelaskan output perintah diatas? Analisis apa yang terjadi?
