JARINGAN KOMPUTER

Data Link, Network & Issue

Moechammad SAROSA - 23299509
Sigit ANGGORO - 23299081

TEKNIK SISTEM KOMPUTER
ELEKTROTEKNIK
INSTITUT TEKNOLOGI BANDUNG
2000

1 Pendahuluan

Perkembangan teknologi komputer meningkat dengan cepat, hal ini terlihat pada era tahun 80-an jaringan komputer masih merupakan teka-teki yang ingin dijawab oleh kalangan akademisi, dan pada tahun 1988 jaringan komputer mulai digunakan di universitas-universitas, perusahaan-perusahaan, sekarang memasuki era milenium ini terutama world wide internet telah menjadi realitas sehari-hari jutaan manusia di muka bumi ini.

Selain itu, perangkat keras dan perangkat lunak jaringan telah benar-benar berubah, di awal perkembangannya hampir seluruh jaringan dibangun dari kabel koaxial, kini banyak telah diantaranya dibangun dari serat optik (*fiber optics*) atau komunikasi tanpa kabel.

Sebelum lebih banyak lagi dijelaskan mengenai jaringan komputer secara teknis, pada bab pendahuluan ini akan diuraikan terlebih dahulu definisi jaringan komputer, manfaat jaringan komputer, ddan macam jaringan komputer.

1.1 Definisi Jaringan Komputer

Dengan berkembangnya teknologi komputer dan komunikasi suatu model komputer tunggal yang melayani seluruh tugas-tugas komputasi suatu organisasi kini telah diganti dengan sekumpulan komputer yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya, sistem seperti ini disebut jaringan komputer (*computer network*).[(1)]

Dalam buku ini kita akan menggunakan istilah jaringan komputer untuk mengartikan suatu himpunan *interkoneksi* sejumlah komputer yang *autonomous.* Dua buah komputer dikatakan terinterkoneksi bila keduanya dapat saling bertukar informasui. Betuk koneksinya tidak harus melalui kawat tembaga saja melainkan dapat emnggunakan serat optik, gelomabng mikro, atau satelit komunikasi.

Untuk memahami istilah jaringan komputer sering kali kita dibingungkan dengan sistem terdistribusi (*distributed system*). Kunci perbedaannya adalah bahwa sebuah sistem

terdistribusi,keberadaan sejumlah komputer autonomous bersifat transparan bagi pemakainya. Seseorang dapat memberi perintah untuk mengeksekusi suatu program, dan kemudian program itupun akan berjalan dan tugas untuk memilih prosesor, menemukan dan mengirimkan file ke suatu prosesor dan menyimpan hasilnya di tempat yang tepat mertupakan tugas sistem operasi. Dengan kata lain, pengguna sistem terditribusi tidak akan menyadari terdapatnya banyak prosesor (multiprosesor), alokasi tugas ke prosesor-prosesor, alokasi f\ile ke disk, pemindahan file yang dfisimpan dan yang diperlukan, serta fungsi-fungsi lainnya dari sitem harus bersifat otomatis.

Pada suatu jaringan komputer, pengguna harus secara eksplisit log ke sebuah mesin, secara eksplisit menyampaikan tugasnya dari jauh, secara eksplisity memindahkan file-file dan menangani sendiri secara umum selusurh manajemen jaringan. Pada sistem terdistribusi, tidak ada yang perlu dilakukan secara eksplisit, sermunya sudah dilakukan secara otomatis oleh sistem tanpa sepengetahuan pemakai.

Dengan demikian sebuah sistem terdistribusi adalah suatu sistem perangkat lunak yang dibuat pada bagian sebuah jaringan komputer. Perangkat lunaklah yang menentukan tingkat keterpaduan dan transparansi jarimngan yang bersangkutan. Karena itu perbedaan jaringan dengan sistem terdistribusi lebih terletak pada perangkat lunaknya (khususnya sistem operasi), bukan pada perangkat kerasnya.

1.2 Manfaat Jaringan Komputer

Sebelum membahas kita masalah-masalah teknis lebih mendalam lagi, perlu kiranya diperhatikan hal-hal yang membuat orang tertarik pada jaringan komputer dan untuk apa jaringan ini digunakan. Manfaat jaringan komputer bagi manusia dapat dikelompokkan pada jaringan untuk perusahaan, jaringan untuk umum, dan masalah sosial jaringan.

1.1.1 Jaringan untuk perusahaan/organisasi

Dalam membangun jaringan komputer di perusahaan/ organisasi, ada beberapa keuntungan yang dapat diperoleh dalam

hal-hal resource sharing, reliabilitas tinggi, lebih ekonomis, skalabilitas, dan media komunikasi.

Resource sharing bertujuan agar seluruh program, peralatan, khususnya data dapat digunakan oleh setiap orang yang ada pada jaringan tanpa terpengaruh oleh lokasi resource dan pemakai. jadi source sharing adalah suatu usaha untuk menghilangkan kendala jarak.

Dengan menggunakan jaringan komputer akan memberikan **reliabilitas tinggi** yaitu adanya sumber-sumber alternatif pengganti jika terjadi masalah pada salah satu perangkat dalam jaringan, artinya karena perangkat yang digunakan lebih dari satu jika salah satu perangkat mengalami masalah, maka perangkat yang lain dapat menggantikannya.

Komputer yang kecil memiliki rasio harga/kinerja yang lebih baik dibanding dengan komputer besar. Komputer mainframe memiliki kecepatan kurang lebih sepuluh kali lipat kecepatan komputer pribadi, akan tetapi harga mainframe seribu kalinya lebih mahal. Dengan selisih rasio harga/kinerja yang cukup besar ini menyebabkan perancang sistem memilih membangun sistem yang terdiri dari komputer-komputer pribadi dibanding menggunakan mainframe.

Yang dimaksud dengan **skalabilitas** yaitu kemampuan untuk meningkatkan kinerja sistem secara berangsur-angsur sesuai dengan beban pekerjaan dengan hanya menambahkan sejumlah prosesor. Pada komputer mainframe yang tersentralisasi, jika sistem sudah jenuh, maka komputer harus diganti dengan komputer yang mempunyai kemampuan lebih besar. Hal ini membutuhkan biaya yang sangat besar dan dapat menyebabkan gangguan terhadap kontinyuitas kerja para pemakai.

Sebuah jaringan komputer mampu bertindak sebagai **media komunikasi** yang baik bagi para pegawai yang terpisah jauh. Dengan menggunakan jaringan, dua orang atau lebih yang tinggal berjauhan akan lebih mudah bekerja sama dalam menyusun laporan.

1.1.2 Jaringan untuk umum

Apa yang telah diulas di atas bahwa minat untuk membangun jaringan komputer semata-mata hanya didasarkan pada

alasan ekonomi dan teknologi saja. Bila komputer mainframe yang besar dan baik dapat diperoleh dengan harga murah, maka akan banyak perusahaan/organisasi yang menggunakannya.

Jaringan komputer akan memberikan layanan yang berbeda kepada perorangan di rumah-rumah dibandingkan dengan layanan yang diberikan pada perusahaan seperti apa yang telah diulas di atas. Terdapat tiga hal pokok yang mejadi daya tarik jaringan komputer pada perorangan yaitu:

- access ke informasi yang berada di tempat yang jauh
- komunikasi orang-ke-orang
- hiburan interaktif.

Ada bermacam-macam bentuk access ke infomasi jarak jauh yang dapat dilakukan, terutama setelah berkembangnya teknologi internet , berita-berita di koran sekarang dapat di down load ke komputer kita melalui internet, dan tidak hanya itu sekarang kita dapat melakukan pemesanan suatu produk melalui internet, bisnis yang dikenal dengan istilah *electronic commerce* (e-commerce), ini sekarang sedang berkemang dengan pesat .

Dengan menggunakan internet kita juga dapat melakukan komunikasi orang-ke orang , fasilitas *electronic mail* (e-mail) telah dipakai secara meluas oleh jutaan orang. Komunikasi menggunakan e-mail ini masih mengandung *delay* atau waktu tunda.

Videoconference atau pertemuan maya merupakan teknologi yang memungkinkan terjadinya komunikasi jarak jauh tanpa delay. Pertemuan maya ini dapat pula digunakan untuk keperluan sekolah jarak jauh, memperoleh hasil pemeriksaan medis seorang dokter yang berada di tempat yang jauh, dan sejumlah aplikasi lainnya.

Video on demand merupakan daya tarik ketiga dai jaringan komputer bagi orang per orang dimana kita dapat memilih film atau acara televisi dari negara mana saja dan kemudian ditampilkan di layar monitor kita.

1.1.3 Masalah sosial jaringan

Penggunaan jaringan oleh masyarakat luas akan menyebabkan masalah-masalah sosial, etika, dan politik. Internet

telah masuk ke segala penjuru kehidupan masyarakat, semua orang dapat memanfaatkannya tanpa memandang status sosial, usia, jenis kelamin. Penggunaan internet tidak akan menimbulkan masalah selama subyeknya terbatas pada topik-topik teknis, pendidikan atau hobi, hal-hal dalam batas norma-norma kehidupan, tetapi kesulitan mulai muncul bila suatu situs di internet mempunyai topik yang sangat menarik perhatian orang, seperti politik, agama, sex. Gambar-gambar yang dipasang di situs-situs tersebut mungkin akan merupakan sesuatu yang sangat mengganggu bagi sebagian orang. Selain itu, bentuk pesan-pesan tidaklah terbatas hanya pesan tekstual saja. Foto berwarna dengan resolusi tinggi dan bahkan video clip singkatpun sekarang dapat dengan mudah disebar-luaskan melalui jaringan komputer. Sebagian orang dapat bersikap acuh tak acuh, tapi bagi sebgaian lainnya pemasangan materi tertentu (misalnya pornografi) merupakan sesuatu yang tidak dapat diterima.

1.2 Macam Jaringan Komputer

Dalam mempelajari macam-macam jaringan komputer terdapat dua klasifikasi yang sangat penting yaitu teknologi transmisi dan jarak. Secara garis besar, terdapat dua jenis teknologi transmisi yaitu jaringan broadcast dan jaringan point-to-point

Jaringan broadcast memiliki saluran komunikasi tunggal yang dipakai bersama-sama oleh semua mesin yang ada pada jaringan.

Pesan-pesan berukuran kecil, disebut paket, yang dikirimkan oleh suatu mesin akan diterima oleh mesin-mesin lainnya. Field alamat pada sebuah paket berisi keterangan tentang kepada siapa paket tersebut ditujukan. Saat menerima paket, mesin akan mencek field alamat. Bila paket terserbut ditujukan untuk dirinya, maka mesin akan memproses paket itu , bila paket ditujukan untuk mesin lainnya, mesin terserbut akan mengabaikannya.

Jaringan point-to-point terdiri dari beberapa koneksi pasangan individu dari mesin-mesin. Untuk mengirim paket dari sumber ke suatu tujuan, sebuah paket pad ajringan jenis ini mungkin harus melalui satu atau lebih mesin-mesin perantara. Seringkali harus melalui baynak route yang mungkin berbeda jaraknya. Karena

itu algoritma rout memegang peranan penting pada jaringan point-to-point.

Pada umumnya jaringan yang lebih kecil dan terlokalisasi secara geografis cendurung memakai broadcasting, sedangkan jaringan yang lebih besar menggunakan point-to-point.

Kriteria alternatif untuk mengklasifikasikan jaringan adalah didasarkan pada jaraknya. Tabel berikut ini menampilkan klasifikasi sistem multiprosesor berdasarkan ukuran-ukuran fisiknya.

Jarak antar prosesor	Prosesor di tempat yang sama	Contoh
0,1 m	Papan rangkaian	Data flow machine
1 m	Sistem	Multicomputer
10 m	Ruangan	Local Area Network
100 m	Gedung	
1 km	Kampus	
10 km	Kota	Metropolitan Area Network
100 km	Negara	Wide area Network
1.000 km	Benua	
10.000 km	Planet	The Internet

Tabel 1.1 Klasifikasi prosesor interkoneksi berdasarkan jarak

Dari tabel di atas terlihat pada bagian paling atas adalah dataflow machine, komputer-komputer yang sangat paralel yang memiliki beberapa unit fungsi yang semuanya bekerja untuk program yang sama. Kemudian multicomputer, sistem yang berkomunikasi dengan cara mengirim pesan-pesannya melalui bus pendek dan sangat cepat. Setelah kelas multicomputer adalah jaringan sejati, komputer-komputer yang bekomunikasi dengan cara bertukar data/pesan melalui kabel yang lebih panjang. Jaringan seperti ini dapat dibagi menjadi local area network (LAN), metropolitan area network (MAN), dan wide area network (WAN). Akhirnya, koneksi antara dua jaringan atau lebih disebut internetwork. Internet merupakan salah satu contoh yang terkenal dari suatu internetwork.

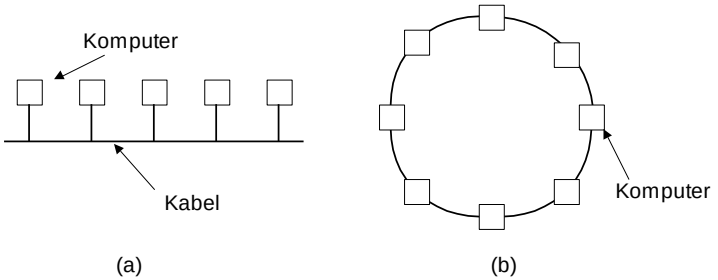
1.2.1 Local Area Network

Local Area Network (LAN) merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer.

LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor perusahaan atau pabrik-pabrik untuk memakai bersama resource (misalnya, printer, scanner) dan saling bertukar informasi. LAN dapat dibedakan dari jenis jaringan lainnya berdasarkan tiga karakteristik: ukuran, teknologi transmisi dan topologinya.

LAN mempunyai ukuran yang terbatas, yang berarti bahwa waktu transmisi pada keadaan terburuknya terbatas dan dapat diketahui sebelumnya. Dengan mengetahui keterbatasnnya, menyebabkan adanya kemungkinan untuk menggunakan jenis desain tertentu. Hal ini juga memudahkan manajemen jaringan.

LAN seringkali menggunakan teknologih transmisi kabel tunggal. LAN tradisional beroperasi pada kecepatan mulai 10 sampai 100 Mbps (mega bit/detik) dengan delay rendah (puluhan mikro second) dan mempunyai faktor kesalahan yang kecil. LAN-LAN modern dapat beroperasi pada kecepatan yang lebih tinggi, sampai ratusan megabit/detik.



Gambar 1.1 Dua jenis jaringan broadcast. (a) Bus. (b) Ring

Terdapat beberapa macam topologi yang dapat digunakan pada LAN broadcast. Gambar 1.1 menggambarkan dua diantara topologi-topologi yang ada. Pada jaringan bus (yaitu kabel liner), pada suatu saat sebuah mesin bertindak sebagai master dan diijinkan untuk mengirim paket. Mesin-mesin lainnya perlu menahan diri untuk tidak mengirimkan apapun. Maka untuk mencegah terjadinya

konflik, ketika dua mesin atau lebih ingin mengirikan secara bersamaan, maka mekanisme pengatur diperlukan. Me4kanisme pengatur dapat berbentuk tersentralisasi atau terdistribusi. IEEE 802.3 yang populer disebut Ethernet merupakan jaringan broadcast bus dengan pengendali terdesentralisasi yang beroperasi pada kecepatan 10 s.d. 100 Mbps. Komputer-komputer pada Ethernet dapat mengirim kapan saja mereka inginkan, bila dua buah paket atau lebih bertabrakan, maka masing-masing komputer cukup menunggu dengan waktu tunggu yang acak sebelum mengulangi lagi pengiriman.

Sistem broadcast yang lain adalah ring, pada topologi ini setiap bit dikirim ke daerah sekitarnya tanpa menunggu paket lengkap diterima. Biasanya setiap bit mengelilingi ring dalam waktu yang dibutuhkan untuk mengirimkan beberapa bit, bahkan seringkali sebelum paket lengkap dikirim seluruhnya. Seperti sistem broadcast lainnya, beberapa aturan harus dipenuhi untuk mengendalikan access simultan ke ring. IEEE 802.5 (token ring) merupakan LAN ring yang populer yang beroperasi pada kecepatan antara 4 s.d 16 Mbps.

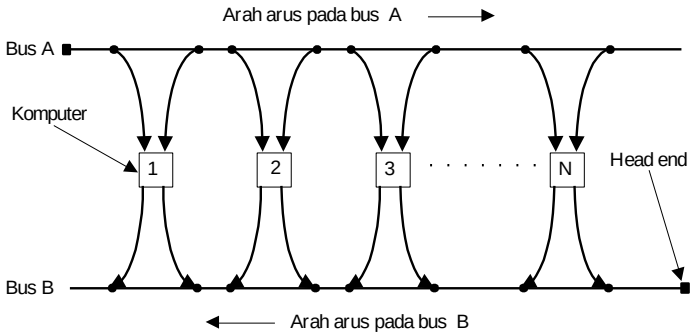
Berdasarkan alokasi channelnya, jaringan broadcast dapat dibagi menjadi dua, yaitu statik dan dinamik. Jenis al;okasi statik dapat dibagi berdasarkan waktu interval-interval diskrit dan algoritma round robin, yang mengijinkan setiap mesin untuk melakukan broadcast hanya bila slot waktunya sudah diterima. Alokasi statik sering menyia-nyiakan kapasitas channel bila sebuah mesin tidak punya lgi yang perlu dikerjakan pada saat slot alokasinya diterima. Karena itu sebagian besar sistem cenderung mengalokasi channel-nya secara dinamik (yaitu berdasarkan kebutuhan).

Metoda alokasi dinamik bagi suatu channel dapat tersentralisasi ataupun terdesentralisasi. Pada metoda alokasi channel tersentralisasi terdapat sebuah entity tunggal, misalnya unit bus pengatur, yang menentukan siapa giliran berikutnya. Pengiriman paket ini bisa dilakukan setelah menerima giliran dan membuat keputusan yang berkaitan dengan algoritma internal. Pada metoda aloksi channel terdesentralisasi, tidak terdapat entity sentral, setiap mesin harus dapat menentukan dirinya sendiri kapan bisa atau tidaknya mengirim.

1.2.2 Metropolitan Area Network

Metropolitan Area Network (MAN) pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya memakai teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang berdekatan dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN biasanya mamapu menunjang data dan suara, dan bahkan dapat berhubungan dengan jaringan televisi kabel. MAN hanya memiliki sebuah atau dua buiah kabel dan tidak mempunyai elemen switching, yang berfungsi untuk mengatur paket melalui beberapa output kabel. Adanya elemen switching membuat rancangan menjadi lebih sederhana.

Alasan utama memisahkan MAN sebagai kategori khusus adalah telah ditentukannya standart untuk MAN, dan standart ini sekarang sedang diimplementasikan. Standart tersebut disebut DQDB (Distributed Queue Dual Bus) atau 802.6 menurut standart IEEE. DQDB terdiri dari dua buah kabel unidirectional dimana semua komputer dihubungkan, seperti ditunjukkan pada gambar 1.2. Setiap bus mempunyai sebuah head–end, perangkat untuk memulai aktivitas transmisi. Lalulintas yang menuju komputer yang berada di sebelah kanan pengirim menggunakan bus bagian atas. Lalulintas ke arah kiri menggunakan bus yang berada di bawah.



Gambar 1.3 Arsitektur MAN DQDB

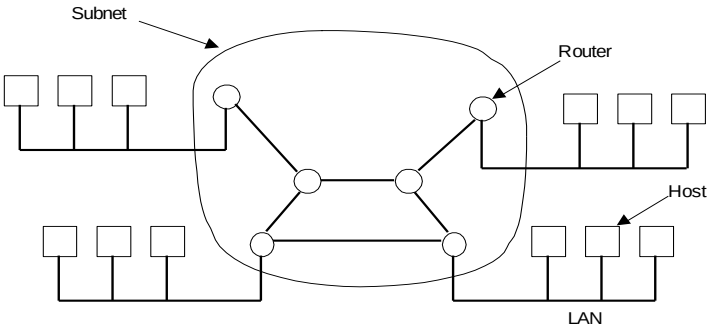
1.2.3 Wide Area Network

Wide Area Network (WAN) mencakup daerah geografis yang luas, sertingkali mencakup sebuah negara atau benua. WAN terdiri dari kumpulan mesin yang bertujuan untuk mejalankan program-program aplikasi.

Kita akan mengikuti penggunaan tradisional dan menyebut
mesin-mesin ini sebagai host. Istilah End System kadang-kadang juga digunakan dalam literatur. Host dihubungkan dengan sebuah subnet komunikasi, atau cukup disebut subnet. Tugas subnet adalah membawa pesan dari host ke host lainnya, seperti halnya sistem telepon yang membawa isi pembicaraan dari pembicara ke pendengar. Dengan memisahkan aspek komunikasi murni sebuah jaringan (subnet) dari aspek-aspek aplikasi (host), rancangan jaringan lengkap menjadi jauh lebih sederhana.

Pada sebagian besar WAN, subnet terdiri dari dua komponen, yaitu kabel transmisi dan elemen switching. Kabel transmisi (disebut juga sirkuit, channel, atau trunk) memindahkan bit-bit dari satu mesin ke mesin lainnya.

Element switching adalah komputer khusus yang dipakai untuk menghubungkan dua kabel transmisi atau lebih. Saat data sampai ke kabel penerima, element switching harus memilih kabel pengirim untuk meneruskan pesan-pesan tersebut. Sayangnya tidak ada terminologi standart dalam menamakan komputer seperti ini. Namanya sangat bervariasi disebut paket switching node, intermidiate system, data switching exchange dan sebagainya.

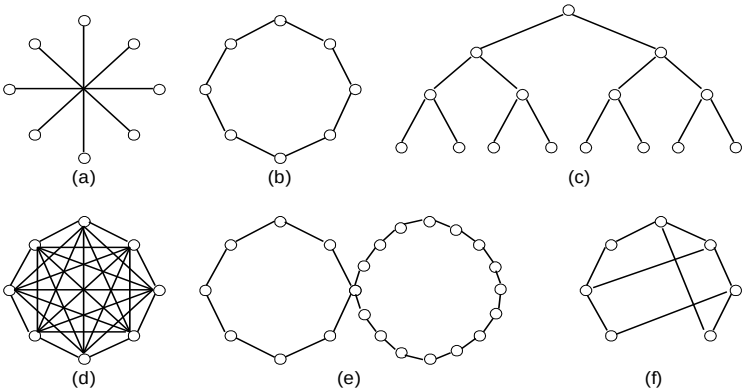


Gambar 1.4 Hubungan antara host-host dengan subnet

Sebagai istilah generik bagi komputer switching, kita akan menggunakan istilah router. Tapi perlu diketahui terlebih dahulu bahwa tidak ada konsensus dalam penggunaan terminologi ini. Dalam model ini, seperti ditunjukkan oleh gambar 1.4 setiap host dihubungkan ke LAN tempat dimana terdapat sebuah router, walaupun dalam beberapa keadaan tertentu sebuah host dapat dihubungkan langsung ke sebuah router. Kumpulan saluran komunikasi dan router (tapi bukan host) akan membentuk subnet.

Istilah subnet sangat penting, tadinya subnet berarti kumpulan kumpulan router-router dan saluran-sakuran komunikasi yang memindahkan paket dari host host tujuan. Akan tatapi, beberpa tahun kemudian subnet mendapatkan arti lainnya sehubungan dengan pengalamatan jaringan.

Pada sebagian besar WAN, jaringan terdiri dari sejumlah banyak kabel atau saluran telepon yang menghubungkan sepasang router. Bila dua router yang tidak mengandung kabel yang sama akan melakukan komunikasi, keduanya harus berkomunikasi secara tak langsung melalui router lainnya. ketika sebuah paket dikirimkan dari sebuah router ke router lainnya melalui router perantara atau lebih, maka paket akan diterima router dalam keadaan lengkap, disimpan sampai saluran output menjadi bebas, dan kemudian baru diteruskan.



Gambar 1.5 bebarapa topologi subnet untuk poin-to-point . (a)Bintang (b)Cincin (c)Pohon (d)Lengkap (e) Cincin berinteraksi (f)Sembarang.

Subnet yang mengandung prinsip seperti ini disebut subnet point-to-point, store-and-forward, atau packet-switched. Hampir semua WAN (kecuali yang menggunakan satelit) memiliki subnet store-and-forward.

Di dalam menggunakan subnet point-to-point, masalah rancangan yang penting adalah pemilihan jenis topologi interkoneksi router. Gambar 1.5 menjelaskan beberapa kemungkinan topologi. LAN biasanya berbentuk topologi simetris, sebaliknya WAN umumnya bertopologi tak menentu.

1.2.4 Jaringan Tanpa Kabel

Komputer mobile seperti komputer notebook dan personal digital assistant (PDA), merupakan cabang industri komputer yang paling cepat pertumbuhannya. Banyak pemilik jenis komputer tersebut yang sebenarnya telah memiliki mesin-mesin desktop yang terpasang pada LAN atau WAN tetapi karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat terbang, maka banyak yang tertarik untuk memiliki komputer dengan jaringan tanpa kabel ini.

Jaringan tanpa kabel mempunyai berbagai manfaat, yang telah umum dikenal adalah kantor portable. Orang yang sedang dalam perjalanan seringkali ingin menggunakan peralatan elektronik portable-nya untuk mengirim atau menerima telepon, fax, e-mail, membaca fail jarak jauh login ke mesin jarak jauh, dan sebagainya dan juga ingin melakukan hal-hal tersebut dimana saja, darat, laut, udara. Jaringan tanpa kabel sangat bermanfaat untuk mengatasi masalah-masalah di atas.

Wireless	Mobile	Aplikasi
Tidak	Tidak	Worksation tetap di kantor
Tidak	Ya	Komputer portable terhubung ke len telepon
Ya	Tidak	LAN dengan komunikasi wireless
Ya	Ya	Kantor portable, PDA untuk persediaan

Tabel 1.2 Kombinasi jaringan tanpa kabel dan komputasi mobile

Walaupun jaringan tanpa kabel dan sistem komputasi yang dapat berpindah-pindah sering kali berkaitan erat, sebenarnya tidaklah sama, seperti yang tampak pada tabel 1.2. Komputer portabel kadang-kadang menggunakan kabel juga, yaitu disaat seseorang yang sedang dalam perjalanan menyambungkan komputer portable-nya ke jack telepon di sebuah hotel, maka kita mempunyai mobilitas yang bukan jaringan tanpa kabel. Sebaliknya, ada juga komputer-komputer yang menggunakan jaringan tanpa kabel tetapi bukan portabel, hal ini dapat terjadi disaat komputer-komputer tersebut terhubung pada LAN yang menggunakan fasilitas komunikasi wireless (radio).

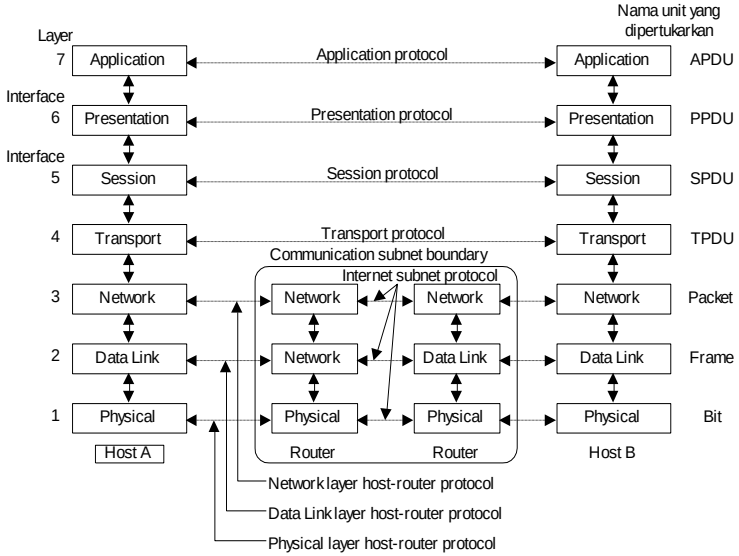
Meskipun jaringan tanpa kabel ini cukup mudah untuk di pasang, tetapi jaringan macam ini memiliki banyak kekurangan. Biasanya jaringan tanpa kabel mempunyai kemampuan 1-2 Mbps, yang mana jauh lebih rendah dibandingkan dengan jaringan berkabel. Laju kesalahan juga sering kali lebih besar, dan transmisi dari komputer yang berbeda dapat mengganggu satu sama lain.

1.4 Referensi

1. Tanenbaum, AS, *Computer Networks*, Prentise Hall, 1996
2. Stallings, W. *Data and Computer Communications*, Macmillan Publishing Company, 1985.
3. Stallings, W. *Local Network*, Macmillan Publishing Company, 1985.

2 Model Referensi OSI

Model referensi OSI (Open System Interconnection) menggambarkan bagaimana informasi dari suatu software aplikasi di sebuah komputer berpindah melewati sebuah media jaringan ke suatu software aplikasi di komputer lain. Model referensi OSI secara konseptual terbagi ke dalam 7 lapisan dimana masing-masing lapisan memiliki fungsi jaringan yang spesifik, seperti yang dijelaskan oleh gambar 2.1 (tanpa media fisik). Model ini diciptakan berdasarkan sebuah proposal yang dibuat oleh the International Standards Organization (ISO) sebagai langkah awal menuju standarisasi protokol internasional yang digunakan pada berbagai layer . Model ini disebut ISO OSI (Open System Interconnection) Reference Model karena model ini ditujukan bagi pengkoneksian open system. Open System dapat diartikan sebagai suatu sistem yang terbuka untuk berkomunikasi dengan sistem-sistem lainnya. Untuk ringkas-nya, kita akan menyebut model tersebut sebagai model OSI saja.



Gambar 2.1. Model Referensi OSI

Model OSI memiliki tujuh layer. Prinsip-prinsip yang digunakan bagi ketujuh layer tersebut adalah :

1. Sebuah layer harus dibuat bila diperlukan tingkat abstraksi yang berbeda.
2. Setiap layer harus memiliki fungsi-fungsi tertentu.
3. Fungsi setiap layer harus dipilih dengan teliti sesuai dengan ketentuan standar protocol internasional.
4. Batas-batas layer diusahakan agar meminimalkan aliran informasi yang melewati interface.
5. Jumlah layer harus cukup banyak, sehingga fungsi-fungsi yang berbeda tidak perlu disatukan dalam satu layer diluar keperluannya. Akan tetapi jumlah layer juga harus diusahakan sesedikit mungkin sehingga arsitektur jaringan tidak menjadi sulit dipakai.

Di bawah ini kita membahas setiap layer pada model OSI secara berurutan, dimulai dari layer terbawah. Perlu dicatat bahwa model OSI itu sendiri bukanlah merupakan arsitektur jaringan, karena model ini tidak menjelaskan secara pasti layanan dan protokolnya untuk digunakan pada setiap layernya. Model OSI hanya menjelaskan tentang apa yang harus dikerjakan oleh sebuah layer. Akan tetapi ISO juga telah membuat standard untuk semua layer, walaupun standard-standard ini bukan merupakan model referensi itu sendiri. Setiap layer telah dinyatakan sebagai standard internasional yang terpisah.

2.1 Karakteristik Lapisan OSI

Ke tujuh lapisan dari model referensi OSI dapat dibagi ke dalam dua kategori, yaitu lapisan atas dan lapisan bawah.

Lapisan atas dari model OSI berurusan dengan persoalan aplikasi dan pada umumnya diimplementasi hanya pada software. Lapisan tertinggi (lapisan applikasi) adalah lapisan penutup sebelum ke pengguna (user), keduanya, pengguna dan lapisan aplikasi saling berinteraksi proses dengan software aplikasi yang berisi sebuah komponen komunikasi. Istilah lapisan atas kadang-kadang digunakan untuk menunjuk ke beberapa lapisan atas dari lapisan lapisan yang lain di model OSI.

Lapisan bawah dari model OSI mengendalikan persoalan transport data. Lapisan fisik dan lapisan data link diimplementasikan

ke dalam hardware dan software. Lapisan-lapisan bawah yang lain pada umumnya hanya diimplementasikan dalam software. Lapisan terbawah, yaitu lapisan fisik adalah lapisan penutup bagi media jaringan fisik (misalnya jaringan kabel), dan sebagai penanggung jawab bagi penempatan informasi pada media jaringan. Tabel berikut ini menampilkan pemisahan kedua lapisan tersebut pada lapisan-lapisan model OSI.

Application	Application	Lapisan Atas
Presentation		
Session		
Transport	Data Transport	Lapisan Bawah
Network		
Data Link		
Physical		

Tabel 2.1 Pemisahan Lapisan atas dan Lapisan bawah pada model OSI

2.2 Protokol

Model OSI menyediakan secara konseptual kerangka kerja untuk komunikasi antar komputer, tetapi model ini bukan merupakan metoda komunikasi. Sebenarnya komunikasi dapat terjadi karena menggunakan protokol komunikasi. Di dalam konteks jaringan data, sebuah protokol adalah suatu aturan formal dan kesepakatan yang menentukan bagaimana komputer bertukar informasi melewati sebuah media jaringan. Sebuah protokol mengimplementasikan salah satu atau lebih dari lapisan-lapisan OSI. Sebuah variasi yang lebar dari adanya protokol komunikasi, tetapi semua memelihara pada salah satu aliran group: protokol LAN, protokol WAN, protokol jaringan, dan protokol routing. Protokol LAN beroperasi pada lapisan fisik dan data link dari model OSI dan mendefinisikan komunikasi di atas macam-macam media LAN. Protokol WAN beroperasi pada ketiga lapisan terbawah dari model OSI dan mendefinisikan komunikasi di atas macam-macam WAN. Protokol routing adalah protokol lapisan jaringan yang bertanggung jawab untuk menentukan jalan dan pengaturan lalu lintas. Akhirnya

protokol jaringan adalah berbagai protokol dari lapisan teratas yang ada dalam sederetan protokol.

2.3 Lapisan-lapisan Model OSI

2.3.1 Physical Layer

Physical Layer berfungsi dalam pengiriman raw bit ke channel komunikasi. Masalah desain yang harus diperhatikan disini adalah memastikan bahwa bila satu sisi mengirim data 1 bit, data tersebut harus diterima oleh sisi lainnya sebagai 1 bit pula, dan bukan 0 bit. Pertanyaan yang timbul dalam hal ini adalah : berapa volt yang perlu digunakan untuk menyatakan nilai 1? dan berapa volt pula yang diperlukan untuk angka 0?. Diperlukan berapa mikrosekon suatu bit akan habis? Apakah transmisi dapat diproses secara simultan pada kedua arahnya? Berapa jumlah pin yang dimiliki jaringan dan apa kegunaan masing-masing pin? Secara umum masalah-masalah desain yang ditemukan di sini berhubungan secara mekanik, elektrik dan interface prosedural, dan media fisik yang berada di bawah physical layer.

2.3.2 Data Link Layer

Tugas utama data link layer adalah sebagai fasilitas transmisi raw data dan mentransformasi data tersebut ke saluran yang bebas dari kesalahan transmisi. Sebelum diteruskan kenetwork layer, data link layer melaksanakan tugas ini dengan memungkinkan pengirim memecag-mecah data input menjadi sejumlah data frame (biasanya berjumlah ratusan atau ribuan byte). Kemudian data link layer mentransmisikan frame tersebut secara berurutan, dan memproses acknowledgement frame yang dikirim kembali oleh penerima. Karena physical layer menerima dan mengirim aliran bit tanpa mengindahkan arti atau arsitektur frame, maka tergantung pada data link layer-lah untuk membuat dan mengenali batas-batas frame itu. Hal ini bisa dilakukan dengan cara membubuhkan bit khusus ke awal dan akhir frame. Bila secara insidental pola-pola bit ini bisa ditemui pada data, maka diperlukan perhatian khusus untuk menyakinkan bahwa pola tersebut tidak secara salah dianggap sebagai batas-batas frame.

Terjadinya noise pada saluran dapat merusak frame. Dalam hal ini, perangkat lunak data link layer pada mesin sumber dapat mengirim kembali frame yang rusak tersebut. Akan tetapi transmisi frame sama secara berulang-ulang bisa menimbulkan duplikasi frame. Frame duplikat perlu dikirim apabila acknowledgement frame dari penerima yang dikembalikan ke pengirim telah hilang. Tergantung pada layer inilah untuk mengatasi masalah-masalah yang disebabkan rusaknya, hilangnya dan duplikasi frame. Data link layer menyediakan beberapa kelas layanan bagi network layer. Kelas layanan ini dapat dibedakan dalam hal kualitas dan harganya.

Masalah-masalah lainnya yang timbul pada data link layer (dan juga sebagian besar layer-layer di atasnya) adalah mengusahakan kelancaran proses pengiriman data dari pengirim yang cepat ke penerima yang lambat. Mekanisme pengaturan lalu-lintas data harus memungkinkan pengirim mengetahui jumlah ruang buffer yang dimiliki penerima pada suatu saat tertentu. Seringkali pengaturan aliran dan penanganan error ini dilakukan secara terintegrasi.

Saluran yang dapat mengirim data pada kedua arahnya juga bisa menimbulkan masalah. Sehingga dengan demikian perlu dijadikan bahan pertimbangan bagi software data link layer. Masalah yang dapat timbul di sini adalah bahwa frame-frame acknoeledgement yang mengalir dari A ke B bersaing saling mendahului dengan aliran dari B ke A. Penyelesaian yang terbaik (piggy backing) telah bisa digunakan; nanti kita akan membahasnya secara mendalam.

Jaringan broadcast memiliki masalah tambahan pada data link layer. Masalah tersebut adalah dalam hal mengontrol akses ke saluran yang dipakai bersama. Untuk mengatasinya dapat digunakan sublayer khusus data link layer, yang disebut medium access sublayer.

Masalah mengenai data link control akan diuraikan lebih detail lagi pada bab tiga.

2.3.3 Network Layer

Network layer berfungsi untuk pengendalian operasi subnet. Masalah desain yang penting adalah bagaimana caranya

menentukan route pengiriman paket dari sumber ke tujuannya. Route dapat didasarkan pada table statik yang "dihubungkan ke" network. Route juga dapat ditentukan pada saat awal percakapan misalnya session terminal. Terakhir, route dapat juga sangat dinamik, dapat berbeda bagi setiap paketnya. Oleh karena itu, route pengiriman sebuah paket tergantung beban jaringan saat itu.

Bila pada saat yang sama dalam sebuah subnet terdapat terlalu banyak paket, maka ada kemungkinan paket-paket tersebut tiba pada saat yang bersamaan. Hal ini dapat menyebabkan terjadinya bottleneck. Pengendalian kemacetan seperti itu juga merupakan tugas network layer.

Karena operator subnet mengharap bayaran yang baik atas tugas pekerjaannya. seringkali terdapat beberapa fungsi accounting yang dibuat pada network layer. Untuk membuat informasi tagihan, setidaknya software mesti menghitung jumlah paket atau karakter atau bit yang dikirimkan oleh setiap pelanggannya. Accounting menjadi lebih rumit, bilamana sebuah paket melintasi batas negara yang memiliki tarip yang berbeda.

Perpindahan paket dari satu jaringan ke jaringan lainnya juga dapat menimbulkan masalah yang tidak sedikit. Cara pengalamatan yang digunakan oleh sebuah jaringan dapat berbeda dengan cara yang dipakai oleh jaringan lainnya. Suatu jaringan mungkin tidak dapat menerima paket sama sekali karena ukuran paket yang terlalu besar. Protokolnyapun bisa berbeda pula, demikian juga dengan yang lainnya. Network layer telah mendapat tugas untuk mengatasi semua masalah seperti ini, sehingga memungkinkan jaringan-jaringan yang berbeda untuk saling terinterkoneksi.

2.3.4 Transport Layer

Fungsi dasar transport layer adalah menerima data dari session layer, memecah data menjadi bagian-bagian yang lebih kecil bila perlu, meneruskan data ke network layer, dan menjamin bahwa semua potongan data tersebut bisa tiba di sisi lainnya dengan benar. Selain itu, semua hal tersebut harus dilaksanakan secara efisien, dan bertujuan dapat melindungi layer-layer bagian atas dari perubahan teknologi hardware yang tidak dapat dihindari.

Dalam keadaan normal, transport layer membuat koneksi jaringan yang berbeda bagi setiap koneksi transport yang diperlukan oleh session layer. Bila koneksi transport memerlukan throughput yang tinggi, maka transport layer dapat membuat koneksi jaringan yang banyak. Transport layer membagi-bagi pengiriman data ke sejumlah jaringan untuk meningkatkan throughput. Di lain pihak, bila pembuatan atau pemeliharaan koneksi jaringan cukup mahal, transport layer dapat menggabungkan beberapa koneksi transport ke koneksi jaringan yang sama. Hal tersebut dilakukan untuk membuat penggabungan ini tidak terlihat oleh session layer.

Transport layer juga menentukan jenis layanan untuk session layer, dan pada gilirannya jenis layanan bagi para pengguna jaringan. Jenis transport layer yang paling populer adalah saluran error-free point to point yang meneruskan pesan atau byte sesuai dengan urutan pengirimannya. Akan tetapi, terdapat pula jenis layanan transport lainnya. Layanan tersebut adalah transport pesan terisolasi yang tidak menjamin urutan pengiriman, dan membroadcast pesan-pesan ke sejumlah tujuan. Jenis layanan ditentukan pada saat koneksi dimulai.

Transport layer merupakan layer end to end sebenarnya, dari sumber ke tujuan. Dengan kata lain, sebuah program pada mesin sumber membawa percakapan dengan program yang sama dengan pada mesin yang dituju. Pada layer-layer bawah, protokol terdapat di antara kedua mesin dan mesin-mesin lain yang berada didekatnya. Protokol tidak terdapat pada mesin sumber terluar atau mesin tujuan terluar, yang mungkin dipisahkan oleh sejumlah router. Perbedaan antara layer 1 sampai 3 yang terjalin, dan layer 4 sampai 7 yang end to end. Hal ini dapat dijelaskan seperti pada gambar 2-1.

Sebagai tambahan bagi penggabungan beberapa aliran pesan ke satu channel, transport layer harus hati-hati dalam menetapkan dan memutuskan koneksi pada jaringan. Proses ini memerlukan mekanisma penamaan, sehingga suatu proses pada sebuah mesin mempunyai cara untuk menerangkan dengan siapa mesin itu ingin bercakap-cakap. Juga harus ada mekanisme untuk mengatur arus informasi, sehingga arus informasi dari host yang cepat tidak membanjiri host yang lambat. Mekanisme seperti itu disebut pengendalian aliran dan memainkan peranan penting pada transport layer (juga pada layer-layer lainnya). Pengendalian aliran

antara host dengan host berbeda dengan pengendalian aliran router dengan router. Kita akan mengetahui nanti bahwa prinsip-prinsip yang sama digunakan untuk kedua jenis pengendalian tersebut.

2.3.5 Session Layer

Session layer mengijinkan para pengguna untuk menetapkan session dengan pengguna lainnya. Sebuah session selain memungkinkan transport data biasa, seperti yang dilakukan oleh transport layer, juga menyediakan layanan yang istimewa untuk aplikasi-aplikasi tertentu. Sebuah session digunakan untuk memungkinkan seseorang pengguna log ke remote timesharing system atau untuk memindahkan file dari satu mesin kemesin lainnya.

Sebuah layanan session layer adalah untuk melaksanakan pengendalian dialog. Session dapat memungkinkan lalu lintas bergerak dalam bentuk dua arah pada suatu saat, atau hanya satu arah saja. Jika pada satu saat lalu lintas hanya satu arah saja (analog dengan rel kereta api tunggal), session layer membantu untuk menentukan giliran yang berhak menggunakan saluran pada suatu saat.

Layanan session di atas disebut manajemen token. Untuk sebagian protokol, adalah penting untuk memastikan bahwa kedua pihak yang bersangkutan tidak melakukan operasi pada saat yang sama. Untuk mengatur aktivitas ini, session layer menyediakan token-token yang dapat digilirkan. Hanya pihak yang memegang token yang diijinkan melakukan operasi kritis.

Layanan session lainnya adalah sinkronisasi. Ambil contoh yang dapat terjadi ketika mencoba transfer file yang berdurasi 2 jam dari mesin yang satu ke mesin lainnya dengan kemungkinan mempunyai selang waktu 1 jam antara dua crash yang dapat terjadi. Setelah masing-masing transfer dibatalkan, seluruh transfer mungkin perlu diulangi lagi dari awal, dan mungkin saja mengalami kegagalan lain. Untuk mengurangi kemungkinan terjadinya masalah ini, session layer dapat menyisipkan tanda tertentu ke aliran data. Karena itu bila terjadi crash, hanya data yang berada sesudah tanda tersebut yang akan ditransfer ulang.

2.3.6 Pressentation Layer

Pressentation layer melakukan fungsi-fungsi tertentu yang diminta untuk menjamin penemuan sebuah penyelesaian umum bagi masalah tertentu. Pressentation Layer tidak mengijinkan pengguna untuk menyelesaikan sendiri suatu masalah. Tidak seperti layer-layer di bawahnya yang hanya melakukan pemindahan bit dari satu tempat ke tempat lainnya, presentation layer memperhatikan syntax dan semantik informasi yang dikirimkan.

Satu contoh layanan pressentation adalah encoding data. Kebanyakan pengguna tidak memindahkan string bit biner yang random. Para pengguna saling bertukar data sperti nama orang, tanggal, jumlah uang, dan tagihan. Item-item tersebut dinyatakan dalam bentuk string karakter, bilangan interger, bilangan floating point, struktur data yang dibentuk dari beberapa item yang lebih sederhana. Terdapat perbedaan antara satu komputer dengan komputer lainnya dalam memberi kode untuk menyatakan string karakter (misalnya, ASCII dan Unicode), integer (misalnya komplemen satu dan komplemen dua), dan sebagainya. Untuk memungkinkan dua buah komputer yang memiliki presentation yang berbeda untuk dapat berkomunikasi, struktur data yang akan dipertukarkan dapat dinyatakan dengan cara abstrak, sesuai dengan encoding standard yang akan digunakan "pada saluran". Presentation layer mengatur data-struktur abstrak ini dan mengkonversi dari representation yang digunakan pada sebuah komputer menjadi representation standard jaringan, dan sebaliknya.

2.3.7 Application Layer

Application layer terdiri dari bermacam-macam protokol. Misalnya terdapat ratusan jenis terminal yang tidak kompatibel di seluruh dunia. Ambil keadaan dimana editor layar penuh yang diharapkan bekerja pada jaringan dengan bermacam-macam terminal, yang masing-masing memiliki layout layar yang berlainan, mempunyai cara urutan penekanan tombol yang berbeda untuk penyisipan dan penghapusan teks, memindahkan sensor dan sebagainya.

Suatu cara untuk mengatasi masalah seperti di ata, adalah dengan menentukan terminal virtual jaringan abstrak, serhingga editor dan program-program lainnya dapat ditulis agar saling bersesuaian. Untuk menangani setiap jenis terminal, satu bagian software harus ditulis untuk memetakan fungsi terminal virtual jaringan ke terminal sebenarnya. Misalnya, saat editor menggerakkan cursor terminal virtual ke sudut layar kiri, software tersebut harus mengeluarkan urutan perintah yang sesuai untuk mencapai cursor tersebut. Seluruh software terminal virtual berada pada application layer.

Fungsi application layer lainnya adalah pemindahan file. Sistem file yang satu dengan yang lainnya memiliki konvensi penamaan yang berbeda, cara menyatakan baris-baris teks yang berbeda, dan sebagainya. Perpindahan file dari sebuah sistem ke sistem lainnya yang berbeda memerlukan penanganan untuk mengatasi adanya ketidak-kompatibelan ini. Tugas tersebut juga merupakan pekerjaan appication layer, seperti pada surat elektronik, remote job entry, directory lookup, dan berbagai fasilitas bertujuan umum dan fasilitas bertujuan khusus lainnya.

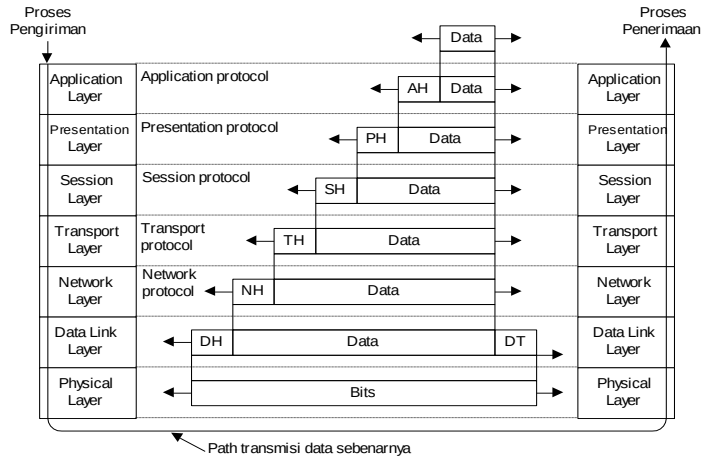
2.4 Transmisi Data Pada Model OSI

Gambar 1-17 menjelaskan sebuah contoh tentang bagaimana data dapat ditransmisikan dengan menggunakan model OSI. Proses pengiriman memiliki data yang akan dikirimkan ke proses penerima. Proses pengirim menyerahkan data ke application layer, yang kemudian menambahkan aplication header, AH (yang mungkin juga kosong), ke ujung depannya dan menyerahkan hasilnya ke presentation layer.

Pressentation layer dapat membentuk data ini dalam berbagai cara dan mungkin saja menambahkan sebuah header di ujung depannya, yang diberikan oleh session layer. Penting untuk diingat bahwa presentation layer tidak menyadari tentang bagian data yang mana yang diberi tanda AH oleh application layer yang merupakan data pengguna yang sebenarnya.

Proses pemberian header ini berulang terus sampai data tersebut mencapai physical layer, dimana data akan ditransmisikan

ke mesin lainnya. Pada mesin tersebut, semua header tadi dicopoti satu per satu sampai mencapai proses penerimaan.



Gambar 2.2 Contoh tentang bagaimana model OSI digunakan

Yang menjadi kunci di sini adalah bahwa walaupun transmisi data aktual berbentuk vertikal seperti pada gambar 1-17, setiap layer diprogram seolah-olah sebagai transmisi yang bersangkutan berlangsung secara horizontal. Misalnya, saat transport layer pengiriman mendapatkan pesan dari session layer, maka transport layer akan membubuhkan header transport layer dan mengirimkannya ke transport layer penerima.

2.5 Referensi

1. Tanenbaum, AS, *Computer Networks*, Prentise Hall, 1996
2. Stallings, W. *Data and Computer Communications*, Macmillan Publishing Company, 1985.
3. Stallings, W. *Local Network*, Macmillan Publishing Company, 1985.
4. Raj Jain, Professor of CIS The Ohio State University Columbus, OH 43210 Jain@ACM.Org http://www.cis.ohio-state.edu/~jain/cis677-98/
5. Cisco Press http://www.cicso.com/cpress/cc/td/cpress/fund/ith2nd/it2401.html

3 Data Link Control

Pembahasan kita kali ini mengenai pengiriman sinyal melewati sebuah saluran transmisi, agar komunikasi dapat efektif banyak hal tentang pengendalian dan managemen pertukaran yang harus diperhatikan. Data link control ini bekerja di lapisan ke dua pada model referensi OSI.

Beberapa hal yang diperlukan untuk mengefektifkan komunikasi data antara dua stasiun transmiter dan receiver adalah:

- Sinkronisasi frame, data yang dikirimkan dalam bentuk blok disebut frame. Awal dan akhir suatu frame harus teridentifikasi dengan jelas.
- Menggunakan salah satu dari konfigurasi saluran, akan dibahas pada bab selanjutnya.
- Kendali Aliran, stasiun pengirim harus tidak mengirimkan frame sebelum memastikan bahwa data yang dikirimkan sebelumnya telah sampai.
- Kendali kesalahan, bit-bit kesalahan yang ditunjukkan oleh sistem transmisi harus benar.
- Pengalamat, pada sebuah saluran multipoint, indentitas dari dua buah stasiun dalam sebuah transmisi harus dikenali.
- Kendali dan data dalam beberapa saluran, biasanya tidak diperlukan sinyal kontrol dalam sistem komunikasi yang terpisah, maka penerima harus dapat membedakan informasi kendali dari data yang dirimkan.
- Managemen hubungan, inisiasi, perbaikan, akhir dari suatu data exchange memerlukan beberapa korodinasi dan kerja sama antar stasiun.

3.1 Konfigurasi Saluran

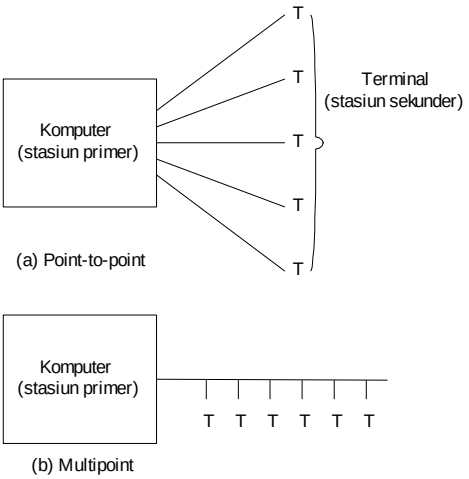
Tiga karakteristik yang membedakan macam-macam konfigurasi saluran adalah topologi, dupleksitas, dan disiplin saluran.

3.1.1 Topologi dan dupleksitas.

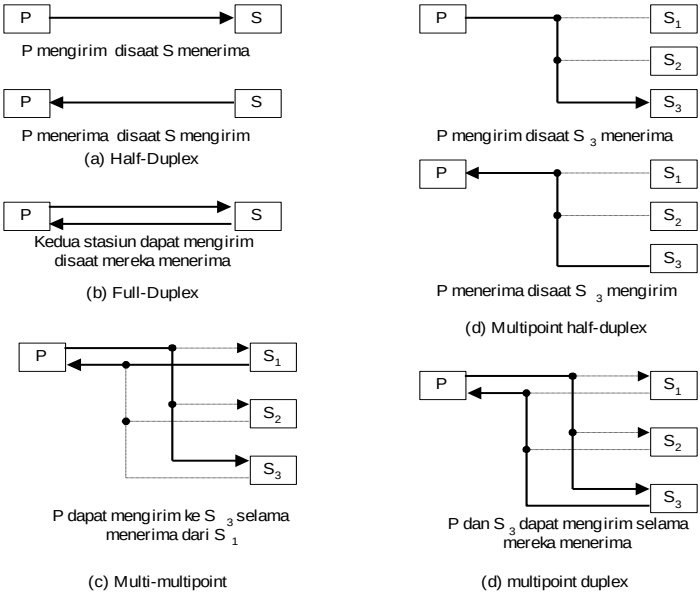
Topologi dari sebuah hubungan data berkenaan dengan susunan fisik dari sebuah stasiun pada sebuah hubungan.jika hanya terdapat dua buah stasiun maka hubungan yang dapat dibangun diantara keduanya adalah point-to-poitn. Jika terdapat lebih dari dua stasiun, maka harus digunakan topoloty multipoint. Dahulu, sebuah hubungan multipoint digunakan pada suatu kasus hubungan antara sebuah komputer (stasiun primer) dan satu set terminal (stasiun sekunder), tetapi sekarang untuk versi yang lebih kompleks topologi multipoint digunakan pada jaringan lokal.

Saluran multipoint tradisional memungkinkan dibuat ketika sebuah terminal hanya mengirim pada satu saat. Gambar 3.1 menunjukkan keuntungan dari konfigurasi multipoint. Jika tiap-tiap komputer memiliki hubungan point-to-point ke suatu komputer jadi komputer harus harus mempunyai sebuah I/O port untuk masing-masing terminal. Jadi terdapat sebuah saluran transmisi yang terpisah dari komputer ke masing-masing terminal. Di dalam sebuah konfigurasi multipoint, komputer memerlukan hanya sebuah I/O port, hanya sebuah saluran transmisi yang diperlukan.

Dupleksitas dari sebuah hubungan berkenaan dengan arah dan waktu aliran sinyal. Dalam transmisi simpleks, aliran sinyal selalu dalam satu arah. Sebagai contoh, sebuah perangkat input hanya dapat mentransmisikan, dan tidak pernah menerima. Sebuah perangkat output misalnya sebuah printer atau aktuator dapat dikonfigurasi hanya sebagai penerima. Simpleks tidak lazim digunakan karena dia tidak mungkin mmngirim ulang kesalahan atau sinyal kontrol ke sumber data . Simpleks identik dengan satu jalan ada satu lintasan.



Gambar 3.1 Konfigurasi terminal.



Gambar 3.2 Hubungan konfigurasi saluran

Sebuah hubungan half-dupleks dapat mengirim dan menerima tetapi tidak simultan. Mode ini seperti dua lintasan alternatif, dua stasiun dalam sebuah hubungan half-dupleks harus bergantian dalam mentransmisikan sesuatu. Hal ini dentik dengan satu jalan ada dua lintasan. Dalam sebuah hubungan full-dupleks, dua buah stasiun dapat mengirim dan menerima secara simultan data dari yang satu ke yang lain. Sehingga pada mode ini dikenal sebagai dua lintasan simultan, dan mungkin sebanding dengan dua jalan ada dua lintasan.

Sejumlah kombinasi dari topologi dan dupleksitas yang mungkin terjadi dapat dilihat pada gambar 3.2 yang melukiskan sebagian keadaan konfigurasi. Gambar selalu menunjukkan sebuah stasiun primer (P) tunggal dan lebih dari satu stasiun sekunder (S). Untuk hubungan point-to-point , dua kemungkinan dapat dijelaskan. Untuk hubungan multipoint, tiga konfigurasi mungkin terjadi:

- Primary full-duplex, secondaries half-duplex (multi-multipoint).
- Both primary and secondaries half-duplex (multipoint half-duplex).
- Both primary and secondaries full-duplex (multipoint duplex).

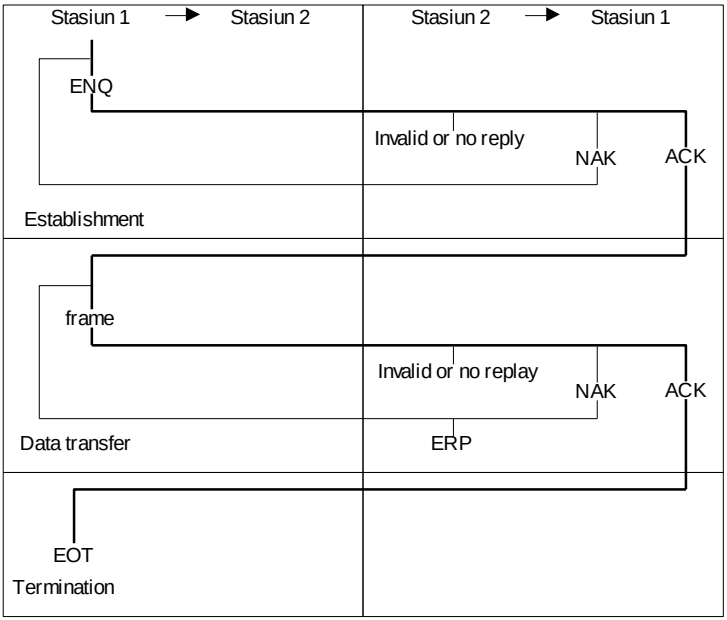
3.1.2 Disiplin saluran

Beberapa disiplin diperlukan dalam menggunakan sebuah hubungan tarnsmisi. Pada sebuah hubungan half-duplex, hanya sebuah stasiun pada suatu waktu yang harus mengirim. Pada kasus yang lain, hubungan half atau full-duplex, sebuah setasiun hanya dapat mengirim jika dia tahu bahwa di sisi penerima telah siap untuk menerima.

Hubungan point-to-point.

Disiplin saluran adalah sederhana dengan sebuah hubungan point-to-point. Marilah pertimbangkan pertama-tama sebuah hubungan half-duplex dalam masing-masing stasiun telah siap menerima perubahan. Sebuah contoh perubahan dilukiskan pada gambar 3.3 Jika masing-masing stasiun menginginkan untuk mengirimkan data ke yang lain, yang pertama dilakukan adalah mengetahui apakah stasiun tujuan telah siap untuk menerima. Stasiun kedua menjawab dengan sebuah positive acknowledge (ack)

untuk mengindikasikan bahwa dia telah siap. Stasiun pertama kemudian mengirim beberapa data yang telah dibentuk dalam frame. Pada komunikasi asinkron data akan dikirim seperti sebuah deretan karakter asinkron. Dalam beberapa kasus, setelah beberapa quantum data dikirimkan , stasiun pertama berhenti untuk menunggu jawaban. Stasiun kedua menjawab keberhasilan menerima data dengan ack. Stasiun pertama kemudian mengirim akhir dari transmisi (eot) yang mengakhiri komunikasi dan kembali ke keadaan awal.



Gambar 3.3 Hubungan kendali point-to-point

Beberapa ciri tambahan ditambahkan pada gambar 3.3 untuk melengkapi proses transmisi dengan kontrol kesalahan. Sebuah negative acknowledgement (nak) digunakan untuk menandakan bahwa sebuah stasiun belum siap menerima atau data diterima dalam keadaan error. Sebuah stasiun mungkin mengabaikan jawan atau menjawab dengan pesan yang cacat. Hasil dari kondisi ini ditunjukkan oleh garis kecil di dalam gambar, garis tebal

menandakan keadaan komunikasi yang normal. Jika sebuah keadaan tak diinginkan terjadi, seperti sebuah nak atau invalid reply, sebuah stasiun mungkin mengulang untuk memberikan aksi terakhir atau mungkin mengadakan beberapa prosedure penemuan kembali kesalahan (erp).

Terdapat tiga phase penting dalam prosedur pengontrolan komunikasi ini:

- Establishement, keputusan yang menentukan stasiun yang mana harus mengirim dan stasiun yang mana harus siap-siap untuk menerima.
- Data Transfer, data ditransfer dalam satu atau lebih blok pengiriman.
- Termination pemberhentian hubungan secara logika. (hubungan transmitter-receiver).

Hubungan Multipoint

Pilihan dari disiplin saluran untuk hubungan multipoint tergantung pada penentuan ada-tidaknya stasiun primer. Ketika terdapat sebuah stasiun primer, data hanya akan ditukar antara stasiun primer dan stasiun sekunder, bukan antara sesama stasiun sekunder. Sebagian besar disiplin bersama menggunakan situasi ini, yaitu semua perbedaan dari sebuah skema dikenal sebagai poll dan select.

- Poll, stasiun primer meminta data dari stasiun sekunder.
- Sellect, stasiun primer memiliki data untuk dikirim dan diberitahukan ke stasiun sekunder bahwa data sedang datang.

Gambar 3.4 menunjukkan konsep ini, dimana stasiun primer poll ke stasiun sekunder dengan mengirim sebuah pesan singkat. Pada kasus ini, stasiun sekunder tidak mengirim dan menjawab dengan beberapa pesan nak. Waktu keseluruhan untuk urutan ini ditunjukkan dengan

$$T_N = t_{prop} + t_{poll} + t_{proc} + t_{nak} + t_{prop}$$

dimana :

T_N : total waktu untuk poll tanpa mengirim

t_{prop} : waktu propagasi = t_1-t_0 = t_5-t_4

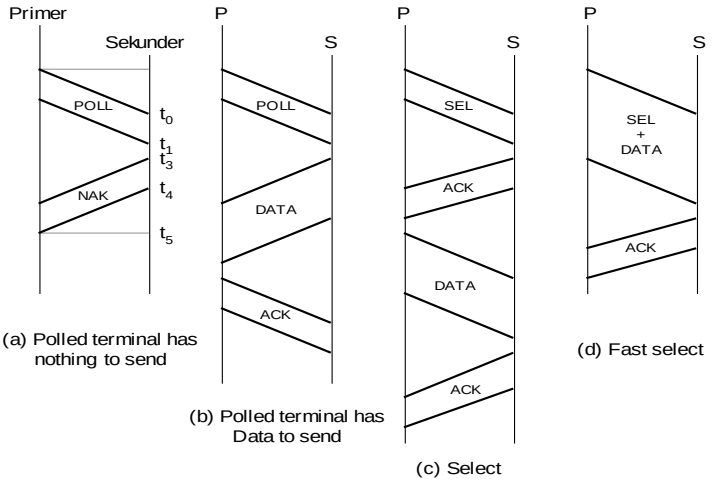
t_{poll} : waktu untuk mengririm poll = t_2-t_1

t_{proc} : waktu untuk pross poll sebelum menerima jawaban

= t_3-t_2

t_{nak} : waktu untuk mengririm sebuah negative acknowledgment

= t_4-t_3



Gambar 3.4 Poll and select sequences

Gambar 3.4 juga menjelaskan kasus dari sebuah keberhasilan poll, waktu yang dibutuhkan adalah:

$$T_P = 3t_{prop} + t_{poll} + t_{ack} + t_{data} + 2t_{proc}$$

$$T_P = T_N + t_{prop} + t_{data} + t_{proc}$$

disini kita asumsikan waktu proses untuk menjawab beberapa pesan adalah konstan.

Sebagian besar bentuk polling bersama disebut roll-call polling, yang mana stasiun primer menyeleksi masing-masing poll dari satsiun sekunder dalam sebuah urutan pra penentuan. Dalam kasus sederhana, stasiun primer poll ke tiap-tiap stasiun sekunder dalam urutan round robbin S_1, S_2, S_3, . . . S_n, sampai semua stasiun sekunder dan mengulang urutan. Waktu yang diperlukan dapat diekspersikan sebagai:

$$T_c = nT_N + kT_D$$

dimana

T_c : waktu untuk satu siklus polling lengkap

T_N : waktu rata-rata untuk poll sebuah stasiun sekunder dari data transfer

T_D: waktu transfer data

n : jumlah stasiun sekunder

k : jumlah stasiun sekundert dengan data untuk dikirim selama siklus.

Fungsi penyeleksian ditunjukkan pada gambar 3.4c Terlihat bahwa empat transmisi terpisah menerima transfer data dari stasiun primer ke stasiun sekunder. Sebuah teknik alternatif disebut fast sellect. pada kasus ini penyeleksian pesan termasuk data ditransfer (gambar 3.4d). Pertama kali mengganti dari stasiun sekunder sebuah acknowledgement yang mengindikasikan bahwa stasiun telah dipersiapkan untuk menerima dan telah menerima data dengan sukses. Pemilihan cepat adalah teristimewa cocok untuk aplikasi dimana pesan pendek sering dikirimkan dan waktu transfer untuk pesan tidak cukup lama dibanding waktu reply.

Penggunaan dari roll-call polling untuk konfigurasi lain adalah mudah dijelaskan. Pada kasus multi-multipoint (gambar 3.2c), stasiun primer dapat mengirim sebuah poll ke salah satu stasiun sekunder pada waktu yang samadia menerima sebuah pesan kontrol atau data dari yang lain. Untuk multipoint duplex stasiun primer dapat digunakan dalam komunikasi full duplex dengan beberapa stasiun sekunder.

Sebuah karakteristik dari semua saluran disiplin multipoint adalah membutuhkan pengalamatan. Dalam kasus roll call polling pengirirman dari sebuah stasiun sekunder harus diidentifikasi. Pada sebuah situasi, kedua pengirim dan penerima harus diidentifikasi. Terdapat tiga keadaan, yaitu:

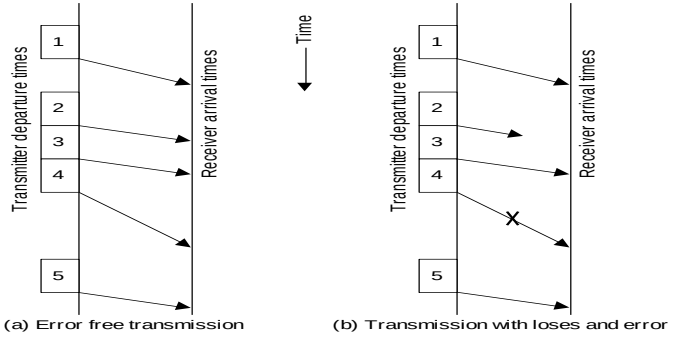
- point-to-point : tidak memerlukan pengalamatan
- primary-secundary multipoint : sebuah alamat diperlukan untuk mengidentifikasi stasiun sekunder.
- peer multipoint : diperlukan dua alamat, untuk mengiden-tifikasi pengirim dan penerima.

3.2 Kontrol Aliran

Flow control adalah suatu teknik untuk menjamin bahwa sebuah stasiun pengirim tidak membanjiri stasiun penerima dengan data. Stasiun penerima secara khas akan menyediakan suatu buffer data dengan panjang tertentu. Ketika data diterima, dia harus mengerjakan beberapa poses sebelum dia dapat membersihkan buffer dan mempersiapkan penerimaan data berikutnya.

Bentuk sederhana dari kontrol aliran dikenal sebagai stop and wait, dia bekerja sebagai berikut. Penerima mengindikasikan bahwa dia siap untuk menerima data dengan mengirim sebual poll atau menjawab dengan select. Pengirim kemudian mengirimkan data.

Flow control ini diatur/dikelola oleh Data Link Control (DLC) atau biasa disebut sebagai Line Protocol sehingga pengiriman maupun penerimaan ribuan message dapat terjadi dalam kurun waktu sesingkat mungkin. DLC harus memindahkan data dalam lalu lintas yang efisien. Jalur komunikasi harus digunakan sedatar mungkin, sehingga tidak ada stasiun yang berada dalam kadaan idle sementara stasiun yang lain saturasi dengan lalu lintas yang berkelebihan. Jadi flow control merupakan bagian yang sangat kritis dari suatu jaringan. Berikut ini ditampilkan time diagram Flow control saat komunikasi terjadi pada kondisi tanpa error dan ada error.



Gambar 3.5 Diagram waktu flow control saat transmisi tanpa kesalahan (a) dan saat terjadi kehilangan paket dan terjadi kesalahan (b)

Mekanisme Flow control yang sudah umum digunakan adalah Stop and Wait dan Sliding window, berikut ini akan dijelaskan kedua mekanisme tersebut.

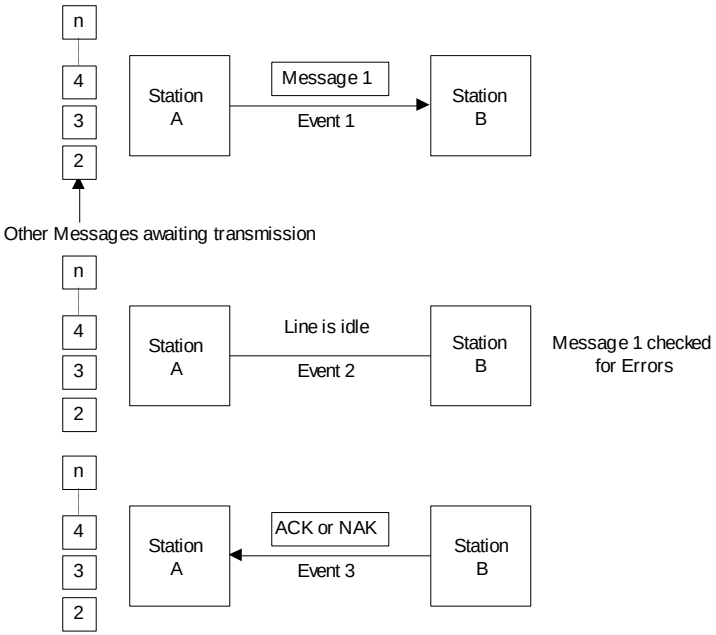
3.2.1 Stop and wait

Protokol ini memiliki karakteristik dimana sebuah pengirim mengirimkan sebuah frame dan kemudian menunggu *acknowledgment* sebelum memprosesnya lebih lanjut. Mekanisme *stop and wait* dapat dijelaskan dengan menggunakan gambar 3.6, dimana DLC mengizinkan sebuah message untuk ditransmisikan (event 1), pengujian terhadap terjadinya error dilakukan dengan teknik seperti VCR (*Vertical Redundancy Check*) atau LRC (*Longitudinal Redundancy Check*) terjadi pada even 2 dan pada saat yang tepat sebuah ACK atau NAK dikirimkan kembali untuk ke stasiun pengirim (event 3). Tidak ada messages lain yang dapat ditransmisikan selama stasiun penerima mengirimkan kembali sebuah jawaban. Jadi istilah *stop and wait* diperoleh dari proses pengiriman message oleh stasiun pengirim, menghentikan transmisi berikutnya, dan menunggu jawaban.

Pendekatan *stop and wait* adalah sesuai untuk susunan transmisi *half duplex*, karena dia menyediakan untuk transmisi data dalam dua arah, tetapi hanya dalam satu arah setiap saat. Kekurangan yang terbesar adalah disaat jalur tidak jalan sebagai akibat dari stasiun yang dalam keadaan menunggu, sehingga kebanyakan DLC *stop and wait* sekarang menyediakan lebih dari satu terminal yang on line. Terminal-terminal tetap beroperasi dalam susunan yang sederhana. Stasiun pertama atau host sebagai penaggung jawab untuk peletakkan message diantara terminal-terminal (biasanya melalui sebuah terminal pengontrol yang berada di depannya) dan akses pengontrolan untuk hubungan komunikasi.

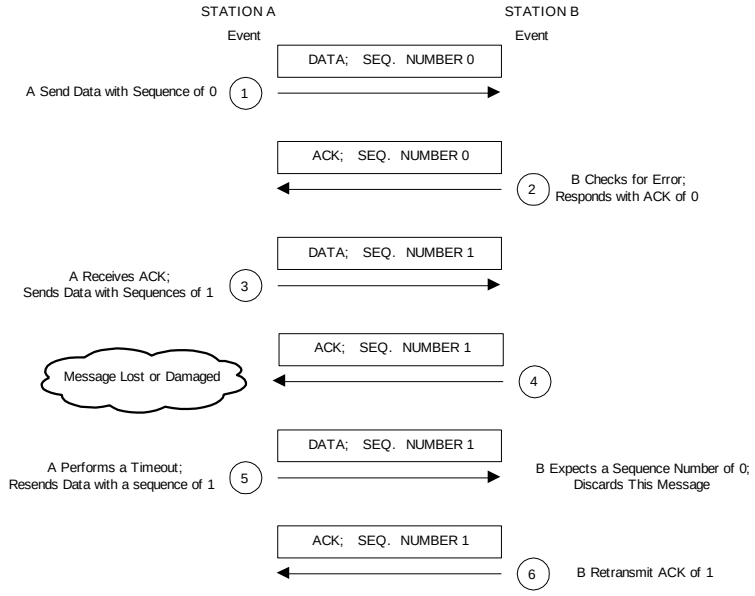
Urutan sederhana ditunjukkan pada gambar 3.6 dan menjadi masalah yang serius ketika ACK atau NAK hilang dalam jaringan atau dalam jalur. Jika ACK pada event 3 hilang, setelah

habis batas waktunya stasiun master mengirim ulang message yang sama untuk kedua kalinya. Transmisi yang berkelebihan mungkin terjadi dan menciptakan sebuah duplikasi record pada tempat kedua dari file data pengguna. Akibatnya, DLC harus mengadakan suatu cara untuk mengidentifikasi dan mengurutkan message yang dikirimkan dengan berdasarkan pada ACK atau NAK sehingga harus dimiliki suatu metoda untuk mengecek duplikat message.



Gambar 3.6 Stop and wait data link control

Pada gambar 3.7 ditunjukkan bagaimana urutan pendeteksian duplikasi message bekerja, pada event 1 stasiun pengirim mengirikan sebuah message dengan urutan 0 pada headernya. Stasiun penerima menjawab dengan sebuah ACK dan sebuah nomor urutan 0 (event 2). Pengirim menerima ACK, memeriksa nomor urutan 0 di headernya, mengubah nomor urutan menjadi 1 dan mengirimkan message berikutnya (event 3).



Gambar 3.7 Stop-and-wait alternating sequence

Stasiun penerima mendapatkan message dengan ACK 1 di event 4. Akan tetapi message ini diterima dalam keadaan rusak atau hilang pada jalan. Stasiun pengirim mengenali bahwa message di event 3 tidak dikenali. Setelah batas waktu terlampau (*timeout*) stasiun pengirim mengirim ulang message ini (event 5). Stasiun penerima mencari sebuah message dengan nomor urutan 0. Dia membuang message, sejak itu dia adalah sebuah duplikat dari message yang dikirim pada event 3. Untuk melengkapi pertang-gung-jawaban, stasiun penerima mengirim ulang ACK 1 (event 6).

Efek delay propagasi dan kecepatan transmisi

Kita akan menentukan efisiensi maksimum dari sebuah jalur *point-to-point* menggunakan skema *stop and wait*. Total waktu yang diperlukan untuk mengirim data adalah :

$T_d = T_I + nT_F$

dimana T_I = waktu untuk menginisiasi urutan = $t_{prop} + t_{poll} + t_{proc}$

T_F = waktu untuk mengirim satu frame

$T_F = t_{prop} + t_{frame} + t_{proc} + t_{prop} + t_{ack} + t_{proc}$

t_{prop} = waktu propagasi

t_{frame} = waktu pengiriman

t_{ack} = waktu balasan

Untuk menyederhanakan persamaan di atas, kita dapat mengabaikan term. Misalnya, untuk sepanjang urutan frame, T_I relatif kecil sehingga dapat diabaikan. Kita asumsikan bahwa waktu proses antara pengiriman dan penerimaan diabaikan dan waktu balasan frame adalah sangat kecil, sehingga kita dapat mengekspresikan T_D sebagai berikut:

$$T_D = n(2t_{prop} + t_{frame})$$

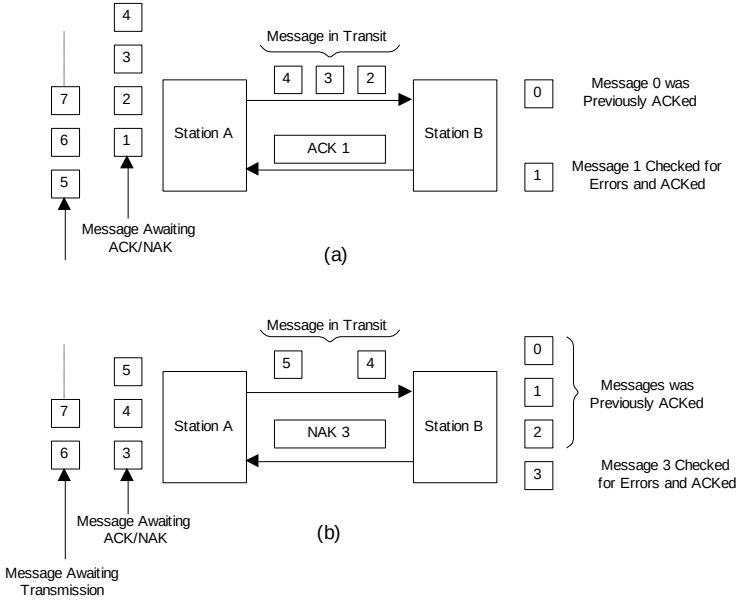
Dari keseluruhan waktu yang diperlukan hanya n x t frame yang dihabiskan selama pengiriman data sehingga utilization (U) atau efisiensi jalur diperoleh :

3.2.2 Sliding window control

Sifat inefisiensi dari stop and wait DLC telah menghasilkan teknik pengembangan dalam meperlengkapi overlapping antara message data dan message control yang sesuai. Data dan sinyal kontrol mengalir dari pengirim ke penerima secara kontinyu, dan beberapa message yang menonjol (pada jalur atau dalam buffer penerima) pada suatu waktu.

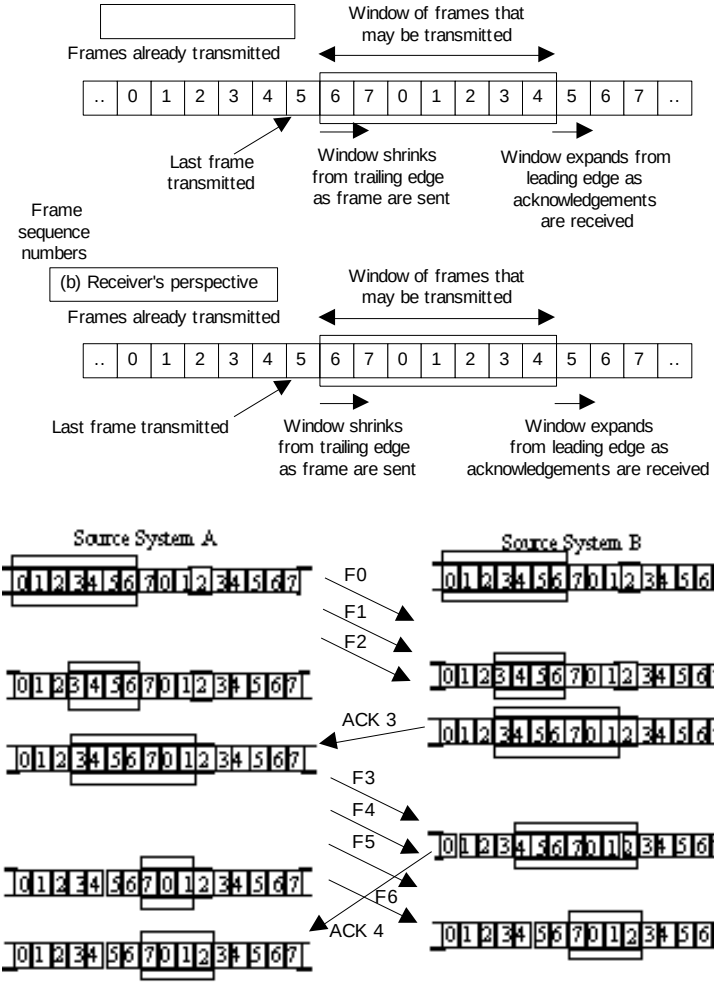
DLC ini sering disebut sliding windows karena metode yang digunakan sinkron dengan pengiriman nomer urutan pada header dengan pengenalan yang sesuai. Stasiun transmisi mengurus sebuah jendela pengiriman yang melukiskan jumlah dari message(dan nomor urutannya) yang diijinkan untuk dikirim. Stasiun penerima mengurus sebuah jendela penerimaan yang melakukan fungsi yang saling mengimbangi. Dua tempat menggunakan keadaan

jendela bagaimana banyak message dapat/ menonjol dalam suatu jalur atau pada penerima sebelum pengirim menghentikan pengiriman dan menunggu jawaban.



Gambar 3.8. Sliding window data link control

Sebagai contoh pada gambar 3.8 suatu penerima dari ACK dari message 1 mengalir ke Station A untuk menggeser jendela sesuai dengan urutan nomor. Jika total message 10 harus dalam jendela, Station A dapat menahan pengiriman message 5,6,7,8,9,0, dan 1. (menahan message-message 2,3 dan 4 dalam kondisi transit). Dia tidak harus mengirim sebuah message menggunakan urutan 2 sampai dia menerima sebuah ACK untuk 2. Jendela melilitkan secara melingkar untuk mengumpulkan nomor-nomor set yang sama. Untuk lebih jelasnya dapat dilihat gambar berikut menampilkan lebih detail mekanisme sliding window dan contoh transmisi messagenya.


Window of frames that may be transmitted
Frames already transmitted
.. 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 ..
Last frame transmitted
Window shrinks from trailing edge as frame are sent
Window expands from leading edge as acknowledgements are received
Frame sequence numbers
(b) Receiver's perspective
Window of frames that may be transmitted
Frames already transmitted
.. 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 ..
Last frame transmitted
Window shrinks from trailing edge as frame are sent
Window expands from leading edge as acknowledgements are received
Source System A
Source System B
F0
F1
F2
ACK 3
F3
F4
F5
F6
ACK 4

Gambar 3.9 Mekanisme sliding windows beserta contoh transimisi message

3.3 Deteksi Dan Koreksi Error

Sebagai akibat proses-proses fisika yang menyebabkannya terjadi, error pada beberapa media (misalnya, radio) cenderung timbul secara meletup (burst) bukannya satu demi satu. Error yang meletup seperti itu memiliki baik keuntungan maupun kerugian pada error bit tunggal yang terisolasi. Sisi keuntungannya, data komputer selalu dikirim dalam bentuk blok-blok bit. Anggap ukuran blok sama dengan 1000 bit, dan laju error adalah 0,001 per bit. Bila error-errornya independen, maka sebagian besar blok akan mengandung error. Bila error terjadi dengan letupan 100, maka hanya satu atau dua blok dalam 100 blok yang akan terpengaruh, secara rata-ratanya. Kerugian error letupan adalah bahwa error seperti itu lebih sulit untuk dideteksi dan dikoreksi dibanding dengan error yang terisolasi.

3.3.1 Kode-kode Pengkoreksian Error

Para perancang jaringan telah membuat dua strategi dasar yang berkenaan dengan error. Cara pertama adalah dengan melibatkan informasi redundan secukupnya bersama-sama dengan setiap blok data yang dikirimkan untuk memungkinkan penerima menarik kesimpulan tentang apa karakter yang ditransmisikan yang seharusnya ada. Cara lainnya adalah dengan hanya melibatkan redundansi secukupnya untuk menarik kesimpulan bahwa suatu error telah terjadi, dan membiarkannya untuk meminta pengiriman ulang. Strategi pertama menggunakan kode-kode pengkoreksian error (error-correcting codes), sedangkan strategi kedua menggunakan kode-kode pendeteksian error (error-detecting codes).

Untuk bisa mengerti tentang penanganan error, kita perlu melihat dari dekat tentang apa yang disebut error itu. Biasanya, sebuah frame terdiri dari m bit data (yaitu pesan) dan r redundan, atau check bits. Ambil panjang total sebesar n (yaitu, n=m+r).

Sebuah satuan n-bit yang berisi data dan checkbit sering kali dikaitkan sebagai codeword n-bit.

Ditentukan dua buah codeword: 10001001 dan 10110001. Disini kita dapat menentukan berapa banyak bit yang berkaitan berbeda. Dalam hal ini, terdapat 3 bit yang berlainan. Untuk menentukannya cukup melakukan operasi EXCLUSIVE OR pada kedua codeword, dan menghitung jumlah bit 1 pada hasil operasi. Jumlah posisi bit dimana dua codeword berbeda disebut jarak Hamming (Hamming, 1950). Hal yang perlu diperhatikan adalah bahwa bila dua codeword terpisah dengan jarak Hamming d, maka akan diperlukan error bit tunggal d untuk mengkonversi dari yang satu menjadi yang lainnya.

Pada sebagian besar aplikasi transmisi data, seluruh 2^m pesan data merupakan data yang legal. Tetapi sehubungan dengan cara penghitungan check bit, tidak semua 2^n digunakan. Bila ditentukan algoritma untuk menghitung check bit, maka akan dimungkinkan untuk membuat daftar lengkap codeword yang legal. Dari daftar ini dapat dicari dua codeword yang jarak Hamming-nya minimum. Jarak ini merupakan jarak Hamming bagi kode yang lengkap.

Sifat-sifat pendeteksian error dan perbaikan error suatu kode tergantung pada jarak Hamming-nya. Untuk mendeteksi d error, anda membutuhkan kode dengan jarak d+1 karena dengan kode seperti itu tidak mungkin bahwa error bit tunggal d dapat mengubah sebuah codeword yang valid menjadi codeword valid lainnya. Ketika penerima melihat codeword yang tidak valid, maka penerima dapat berkata bahwa telah terjadi error pada transmisi. Demikian juga, untuk memperbaiki error d, anda memerlukan kode yang berjarak 2d+1 karena hal itu menyatakan codeword legal dapat terpisah bahkan dengan perubahan d, codeword orisinil akan lebih dekat dibanding codeword lainnya, maka perbaikan error dapat ditentukan secara unik.

Sebagai sebuah contoh sederhana bagi kode pendeteksian error, ambil sebuah kode dimana parity bit tunggal ditambahkan ke data. Parity bit dipilih supaya jumlah bit-bit 1 dalam codeword menjadi genap (atau ganjil). Misalnya, bila 10110101 dikirimkan dalam parity genap dengan menambahkan sebuah bit pada bagian ujungnya, maka data itu menjadi 101101011, sedangkan dengan

parity genap 10110001 menjadi 101100010. Sebuah kode dengan parity bit tunggal mempunyai jarak 2, karena sembarang error bit tunggal menghasilkan sebuah codeword dengan parity yang salah. Cara ini dapat digunakan untuk mendeteksi erro-error tunggal.

Sebagai contoh sederhana dari kode perbaikan error, ambil sebuah kode yang hanya memiliki empat buah codeword valid :

0000000000,0000011111,1111100000 dan 1111111111

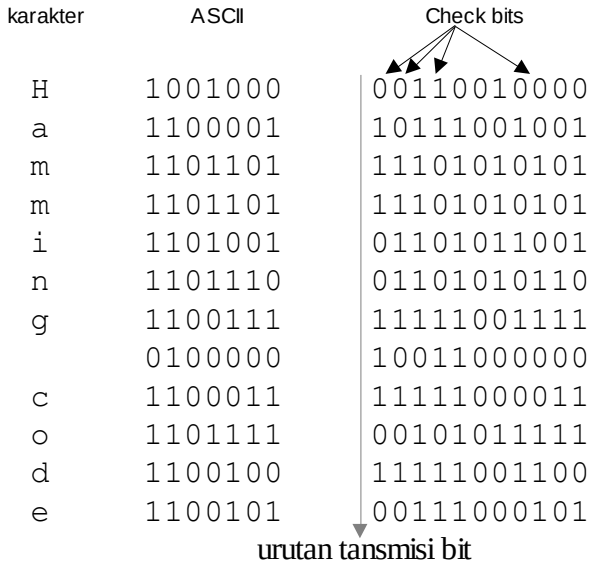
Kode ini mempunyai jarak 5, yang berarti bahwa code tersebut dapat memperbaiki error ganda. Bila codeword 0000011111 tiba, maka penerima akan tahun bahwa data orisinil seharusnya adalah 0000011111. Akan tetapi bila error tripel mengubah 0000000000 menjadi 0000000111, maka error tidak akan dapat diperbaiki.

Bayangkan bahwa kita akan merancang kode dengan m bit pesan dan r bit check yang akan memungkinkan semua error tunggal bisa diperbaiki. Masing-masing dari 2^m pesan yang legal membutuhkan pola bit n+1. Karena jumlah total pola bit adalah 2^n, kita harus memiliki $(n+1)2^m \leq 2^n$.

Dengan memakai n = m + r, persyaratan ini menjadi $(m + r + 1) \leq 2^r$. Bila m ditentukan, maka ini akan meletakkan batas bawah pada jumlah bit check yang diperlukan untuk mengkoreksi error tunggal.

Dalam kenyataannya, batas bawah teoritis ini dapat diperoleh dengan menggunakan metoda Hamming (1950). Bit-bit codeword dinomori secara berurutan, diawali dengan bit 1 pada sisi paling kiri. Bit bit yang merupakan pangkat 2 (1,2,4,8,16 dan seterusnya) adalah bit check. Sisanya (3,5,6,7,9 dan seterusnya) disisipi dengan m bit data. Setiap bit check memaksa parity sebagian kumpulan bit, termasuk dirinya sendiri, menjadi genap (atau ganjil). Sebuah bit dapat dimasukkan dalam beberapa komputasi parity. Untuk mengetahui bit check dimana bit data pada posisi k berkontribusi, tulis ulang k sebagai jumlahan pangkat 2. Misalnya, 11=1+2+8 dan 29=1+4+8+16. Sebuah bit dicek oleh bit check yang terjadi pada ekspansinya (misalnya, bit 11 dicek oleh bit 1,2 dan 8).

Ketika sebuah codeword tiba, penerima menginisialisasi counter ke nol. Kemudian codeword memeriksa setiap bit check, k (k=1,2,4,8,....) untuk melihat apakah bit check tersebut mempunyai parity yang benar. Bila tidak, codeword akan menambahkan k ke counter. Bila counter sama dengan nol setelah semua bit check diuji (yaitu, bila semua bit checknya benar), codeword akan diterima sebagai valid. Bila counter tidak sama dengan nol, maka pesan mengandung sejumlah bit yang tidak benar. Misalnya bila bit check 1,2, dan 8 mengalami kesalahan (error), maka bit inversinya adalah 11, karena itu hanya satu-satunya yang diperiksa oleh bit 1,2, dan 8. Gambar 3.10 menggambarkan beberapa karakter ASCII 7-bit yang diencode sebagai codeword 11 bit dengan menggunakan kode Hamming. Perlu diingat bahwa data terdapat pada posisi bit 3,5,6,7,9,10,11.



Gambar 3.10 Penggunaan kode Hamming untuk mengkoreksi burst error

Kode Hamming hanya bisa memperbaiki error tunggal. Akan tetapi, ada trick yang dapat digunakan untuk memungkinkan

kode Hamming dapat memperbaiki error yang meletup. Sejumlah k buah codeword yang berurutan disusun sebagai sebuah matriks, satu codeword per baris. Biasanya, data akan ditransmisikan satu baris codeword sekali, dari kiri ke kanan. Untuk mengkoreksi error yang meletup, data harus ditransmisikan satu kolom sekali, diawali dengan kolom yang paling kiri. Ketika seluruh k bit telah dikirimkan, kolom kedua mulai dikirimkan, dan seterusnya. Pada saat frame tiba pada penerima, matriks direkonstruksi, satu kolom per satuan waktu. Bila suatu error yang meletup terjadi, paling banyak 1 bit pada setiap k codeword akan terpengaruh. Akan tetapi kode Hamming dapat memperbaiki satu error per codeword, sehingga seluruh blok dapat diperbaiki. Metode ini memakai kr bit check untuk membuat km bit data dapat immune terhadap error tunggal yang meletup dengan panjang k atau kurang.

3.2.2 Kode-kode Pendeteksian Kesalahan

Kode pendeteksian error kadang kala digunakan dalam transmisi data. Misalnya, bila saturan simplex, maka transmisi ulang tidak bisa diminta. Akan tetapi sering kali deteksi error yang diikuti oleh transmisi ulang lebih disenangi. Hal ini disebabkan karena pemakaian transmisi ulang lebih efisien. Sebagai sebuah contoh yang sederhana, ambil sebuah saluran yang errornya terisolasi dan mempunyai laju error 10 –6 per bit.

Anggap ukuran blok sama dengan 1000 bit. Untuk melaksanakan koreksi error blok 1000 bit, diperlukan 10 bit check; satu megabit data akan membutuhkan 10.000 bit check. Untuk mendeteksi sebuah blok dengan error tunggal 1-bit saja, sebuah bit parity per blok akan mencukupi. Sekali setiap 1000 blok dan blok tambahan (1001) akan harus ditransmisikan. Overhead total bagi deteksi error + metoda transmisi ulang adalah hanya 2001 bit per megabit data, dibanding 10.000 bit bagi kode Hamming.

Bila sebuah bit parity tunggal ditambahkan ke sebuah blok dan blok dirusak oleh error letupan yang lama, maka probabilitas error dapat untuk bisa dideteksi adalah hanya 0,5 hal yang sangat sulit untuk bisa diterma. Bit-bit ganjil dapat ditingkatkan cukup banyak dengan mempertimbangkan setiap blok yang akan dikirim sebagai matriks persegi panjang dengan lebar n bit dan tinggi k bit. Bit parity dihitung secara terpisah bagi setiap kolomnya

dan ditambahkan ke matriks sebagai baris terakhir. Kemudian matriks ditransmisikan kembali baris per baris. Ketika blok tiba, penerima akan memeriksa semua bit parity, Bila ada bit parity yang salah, penerima meminta agar blok ditransmisi ulang.

Metoda ini dapat mendeteksi sebuah letupan dengan panjang n, karena hanya 1 bit per kolom yang akan diubah. Sebuah letupan dengan panjang n+1 akan lolos tanpa terdeteksi. Akan tetapi bila bit pertama diinversikan, maka bit terakhir juga akan diinversikan, dan semua bit lainnya adalah benar. (Sebuah error letupan tidak berarti bahwa semua bit salah; tetapi mengindikasikan bahwa paling tidak bit pertama dan terakhirnya salah). Bila blok mengalami kerusakan berat akibat terjadinya error letupan yang panjang atau error letupan pendek yang banyak, maka probabilitas bahwa sembarang n kolom akan mempunyai parity yang benar adalah 0,5. Sehingga probabilitas dari blok yang buruk akan bisa diterima adalah 2^{-n}.

Walaupun metoda di atas kadang-kadang adekuat, pada prakteknya terdapat metode lain yang luas digunakan: Kode polynomial (dikenal juga sebagai cyclic redundancy code atau kode CRC). Kode polynomial didasarkan pada perlakuan string-string bit sebagai representatsi polynomial dengan memakai hanya koefisien 0 dan 1 saja. Sebuah frame k bit berkaitan dengan daftar koefisien bagi polynomial yang mempunyai k suku, dengan range dari x^{k-1} sampai x^0. Polynomial seperti itu disebut polynomial yang bertingkat k-1. Bit dengan orde tertinggi (paling kiri) merupakan koefisien dari x^{k-1}; bit berikutnya merupakan koefisien dari x^{k-2}, dan seterusnya. Misalnya 110001 memiliki 6 bit, maka merepresentasikan polynomial bersuku 6 dengan koefisien 1,1,0,0,0 dan 1:$x^5+x^4+x^0$.

Aritmetika polynomial dikerjakan dengan modulus 2, mengikuti aturan teori aljabar. Tidak ada pengambilan untuk pertambahan dan peminjaman untuk pengurangan. Pertambahan dan pengurangan identik dengan EXCLUSIVE OR, misalnya :

```
  10011011     00110011        11110000
+ 11001010   + 11001101      + 10100110
----------   ----------      ----------
  01010001     11111110        01010110
```

Gambar 3.11 Pertambahan dengan EXOR

Pembagian juga diselesaikan dengan cara yang sama seperti pada pembagian bilangan biner, kecuali pengurangan dikerjakan berdasarkan modulus 2. Pembagi dikatakan "masuk ke" yang dibagi bila bilangan yang dibagi mempunyai bit sebanyak bilangan pembagi.

Saat metode kode polynomial dipakai, pengirim dan penerima harus setuju terlebih dahulu tentang polynomial generator, G(x). Baik bit orde tinggi maupun bit orde rendah dari generator harus mempunyai harga 1. Untuk menghitung checksum bagi beberapa frame dengan m bit, yang berkaitan dengan polynomial M(x), maka frame harus lebih panjang dari polynomial generator. Hal ini untuk menambahkan checksum keakhir frame sedemikian rupa sehingga polynomial yang direpresentasikan oleh frame berchecksum dapat habis dibagi oleh G(x). Ketika penerima memperoleh frame berchecksum, penerima mencoba membaginya dengan G(x). Bila ternyata terdapat sisa pembagian, maka dianggap telah terjadi error transmisi.

Algoritma untuk perhitungan checksum adalah sebagai berikut :

1. Ambil r sebagai pangkat G(x), Tambahkan bit nol r ke bagian orde rendah dari frame, sehingga sekarang berisi m+r bit dan berkaitan dengan polynomial xrM(x).
2. Dengan menggunakan modulus 2, bagi string bit yang berkaitan dengan G(x) menjadi string bit yang berhubungan dengan xrM(x).
3. Kurangkan sisa (yang selalu bernilai r bit atau kurang) dari string bit yang berkaitan dengan xrM(x) dengan menggunakan pengurangan bermodulus 2. Hasilnya merupakan frame berchecksum yang akan ditransmisikan. Disebut polynomial T(x).

Gambar 3-12 menjelaskan proses perhitungan untuk frame 1101011011 dan $G(x) = x^4 + x + 1$.

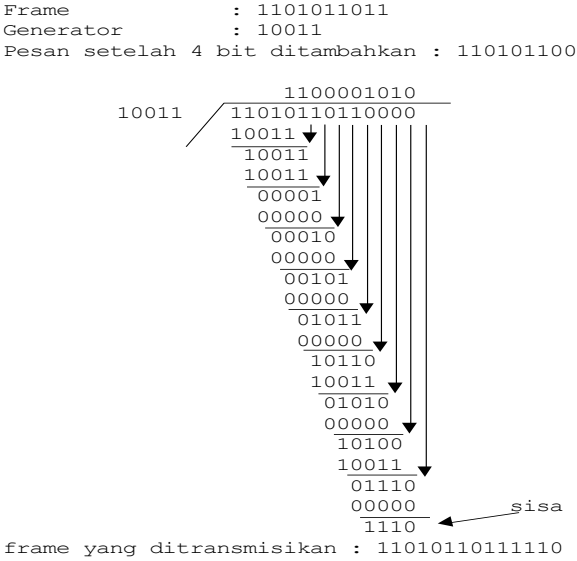
Jelas bahwa T(x) habis dibagi (modulus 2) oleh G(x). Dalam sembarang masalah pembagian, bila anda mengurangi angka yang dibagi dengan sisanya, maka yang akan tersisa adalah angka yang dapat habis dibagi oleh pembagi. Misalnya dalam basis 10, bila anda

membagi 210.278 dengan 10.941, maka sisanya 2399. Dengan mengurangkan 2399 ke 210.278, maka yang bilangan yang tersisa (207.879) habis dibagi oleh 10.941.

Sekarang kita menganalisis kekuatan metoda ini. Error jenis apa yang akan bisa dideteksi ? Anggap terjadi error pada suatu transmisi, sehingga bukannya string bit untuk T(x) yang tiba, akan tetapi T(x) + E(X). Setiap bit 1 pada E(x) berkaitan dengan bit yang telah diinversikan. Bila terdapat k buah bit 1 pada E(x), maka k buah error bit tunggal telah terjadi. Error tunggal letupan dikarakterisasi oleh sebuah awalan 1, campuran 0 dan 1, dan sebuah akhiran 1, dengan semua bit lainnya adalah 0.

Begitu frame berchecksum diterima, penerima membaginya dengan G(x); yaitu, menghitung [T(x)+E(x)]/G(x). T(x)/G(x) sama dengan 0, maka hasil perhitungannya adalah E(x)/G(x). Error seperti ini dapat terjadi pada polynomial yang mengandung G(x) sebagai faktor yang akan mengalami penyimpangan, seluruh error lainnya akan dapat dideteksi.

Bila terdapat error bit tunggal, $E(x)=x^i$, dimana i menentukan bit mana yang mengalami error. Bila G(x) terdiri dari dua suku atau lebih, maka x tidak pernah dapat habis membagi E(x), sehingga seluruh error dapat dideteksi.



Gambar 3-12.Perhitungan checksum kode polynomial

Bila terdapat dua buah error bit-tunggal yang terisolasi, $E(x)=x^i+x^j$, dimana i > j. Dapat juga dituliskan sebagai $E(x)=x^j(x^{i-j} + 1)$. Bila kita mengasumsikan bahwa G(x) tidak dapat dibagi oleh x, kondisi yang diperlukan untuk dapat mendeteksi semua error adalah bahwa G(x) tidak dapat habis membagi x^k+1 untuk sembarang harga k sampai nilai maksimum i-j (yaitu sampai panjang frame maksimum). Terdapat polynomial sederhana atau berorde rendah yang memberikan perlindungan bagi frame-frame yang panjang. Misalnya, $x^{15}+x^{14}+1$ tidak akan habis membagi x^k+1 untuk sembarang harga k yang kurang dari 32.768.

Bila terdapat jumlah bit yang ganjil dalam error, E(x) terdiri dari jumlah suku yang ganjil (misalnya,x^5+x^2+1, dan bukannya x^2+1). Sangat menarik, tidak terdapat polynomial yang bersuku ganjil yang mempunyai x + 1 sebagai faktor dalam sistem modulus 2. Dengan membuat x + 1 sebagai faktor G(x), kita akan mendeteksi semua error yang terdiri dari bilangan ganjil dari bit yang diinversikan.

Untuk mengetahui bahwa polynomial yang bersuku ganjil dapat habis dibagi oleh x+1, anggap bahwa E(x) mempunyai suku ganjil dan dapat habis dibagi oleh x+1. Ubah bentuk E(x) menjadi (x+1)Q(x). Sekarang evaluasi E(1) = (1+1)Q(1). Karena 1+1=0 (modulus 2), maka E(1) harus nol. Bila E(x) mempunyai suku ganjil, pensubtitusian 1 untuk semua harga x akan selalu menghasilkan 1. Jadi tidak ada polynomial bersuku ganjil yang habis dibagi oleh x+1.

Terakhir, dan yang terpenting, kode polynomial dengan r buah check bit akan mendeteksi semua error letupan yang memiliki panjang <=r. Suatu error letupan dengan panjang k dapat dinyatakan oleh $x^i(x^{k-1} + ...+1)$, dimana i menentukan sejauh mana dari sisi ujung kanan frame yang diterima letupan itu ditemui. Bila G(x) mengandung suku x^0, maka G(x) tidak akan memiliki x^i sebagai faktornya. Sehingga bila tingkat ekspresi yang berada alam tanda kurung kurang dari tingkat G(x), sisa pembagian tidak akan pernah berharga nol.

Bila panjang letupan adalah r+1, maka sisa pembagian oleh G(x) akan nol bila dan hanya bila letupan tersebut identik dengan G(x). Menurut definisi letupan, bit awal dan bit akhir harus 1, sehingga apakah bit itu akan sesuai tergantung pada bit pertengahan r-1. Bila semua kombinasi adalah sama dan sebanding, maka probabilitas frame yang tidak benar yang akan diterima sebagai frame yang valid adalah $½^{r-1}$.

Dapat juga dibuktikan bahwa bila letupan error yang lebih panjang dari bit r+1 terjadi, maka probabilitas frame buruk untuk melintasi tanpat peringatan adalah $1/2^r$ yang menganggap bahwa semua pola bit adalah sama dan sebanding.

Tiga buah polynomial telah menjadi standard internasional:

- CRC-12 = $X^{12} + X^{11} + X^3 + X^2 + X^1 + 1$
- CRC-16 = $X^{16} + X^{15} + X^2 + 1$
- CRC-CCITT = $X^{16} + X^{12} + X^5 + 1$

Ketiganya mengandung x+1 sebagai faktor prima.CRC-12 digunakan bila panjang karakternya sama dengan 6 bit. Dua polynomial lainnya menggunakan karakter 8 bit. Sebuah checksum 16 bit seperti CRC-16 atau CRC-CCITT, mendeteksi semua error tunggal dan error ganda, semua error dengan jumlah bit ganjil,

semua error letupan yang mempunyai panjang 16 atau kurang, 99,997 persen letupan error 17 bit, dan 99,996 letupan 18 bit atau lebih panjang.

3.3 Kendali kesalahan

Tujuan dilakukan pengontrolan terhadap error adalah untuk menyampaikan frame-frame tanpa error, dalam urutan yang tepat ke lapisan jaringan. Teknik yang umum digunakan untuk error control berbasis pada dua fungsi, yaitu:

- Error detection, biasanya menggunakan teknik CRC (Cyclic Redundancy Check)
- Automatic Repeat Request (ARQ), ketika error terdeteksi, pengirim meminta mengirim ulang frame yang terjadi kesalahan.

Mekanisme Error control meliputi

- ◊ Ack/Nak : Provide sender some feedback about other end
- ◊ Time-out: for the case when entire packet or ack is lost
- ◊ Sequence numbers: to distinguish retransmissions from originals

Untuk menghindari terjadinya error atau memperbaiki jika terjadi error yang dilakukan adalah melakukan perngiriman message secara berulang, proses ini dilakukan secara otomatis dan dikenal sebagai Automatic Repeat Request (ARQ).
Pada proses ARQ dilakukan beberapa langkah diantaranya [(1)]:

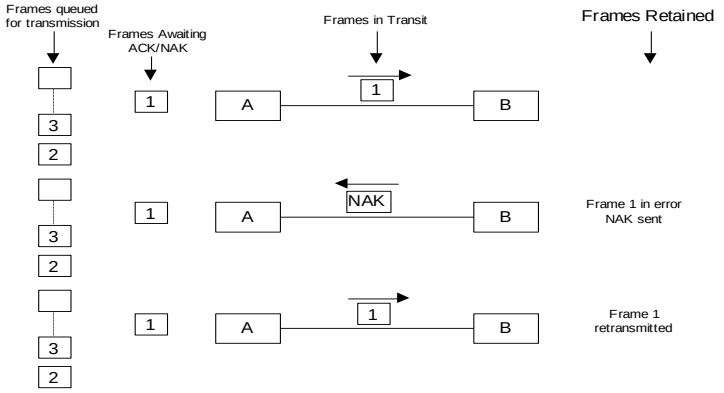
- ◊ Error detection
- ◊ Acknowledgment
- ◊ Retransmission after timeout
- ◊ Negative Acknowledgment

Macam-macam error control adalah:

3.3.1 Stop and Wait ARQ

Mekanisme ini menggunakan skema sederhana *stop and wait acknowledgment* dan dapat dijelaskan seperti tampak pada

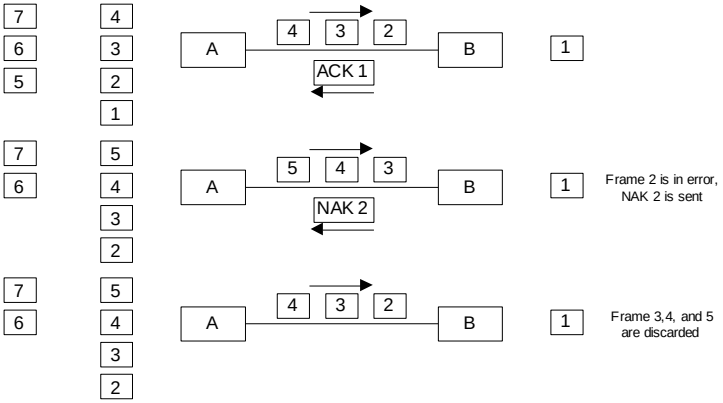
gambar 3.13 Stasiun pengirim mengirimkan sebuah frame dan kemudian harus menunggu balasan dari penerima. Tidak ada frame data yang dapat dikirimkan sampai stasiun penerima menjawab kedatangan pada stasiun pengirim. Penerima mengirim sebuah positive acknowledgment (ACK) jika frame benar dan sebuah negative acknoledgment jika sebaliknya.



Gambar 3.13 Stop and wait ARQ

3.3.2 Go Back N ARQ

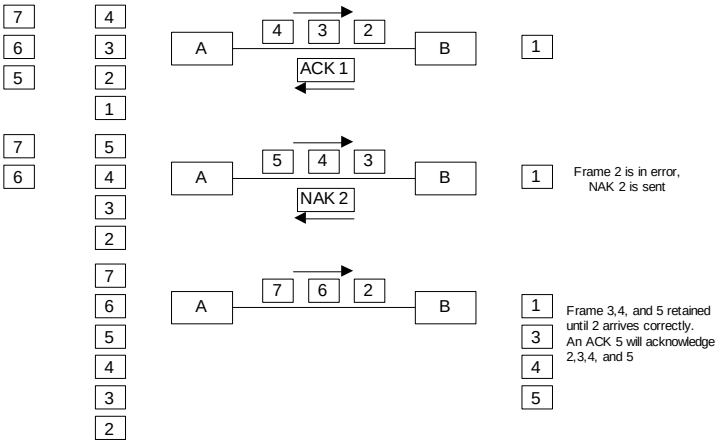
Gambar 3.14 menampilkan aliran frame untuk mekanisme go-back-and ARQ pada sebuah jalur full-duplex. Ketika frame 2,3, dan 4 ditransmisikan, dari stasiun A ke stasiun B, sebuah ACK dari penerimaan sebelumnya frame 1 mengalir dari B ke A. Beberapa waktu kemudian, frame 2 diterima dalam kondisi error. Frame-frame 2,3,4 dan 5 dikirimkan, stasiun B mengirim sebuah NAK2 ke stasiun A yang diterima setelah frame 5 dikirimkan tetapi sebelum stasiun A siap mengirim frame 6. Sekarang harus dilakukan pengiriman ulang frame-frame 2,3,4, dan 5 waluapun hanya pada frame 2 terjadinya kesalahan. Sekali lagi, catat bahwa stasiun A harus sebuah copy dari setiap unacknowledgment frame.



Gambar 3.14 Go-back-N ARQ

3.3.3 Selective-report ARQ

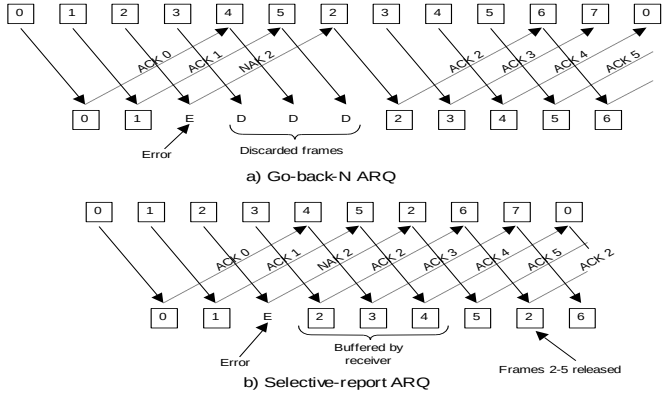
Pada mekanisme ini sebenarnya mirip dengan mekanisme go-back-N ARQ bedanya, pada selective-report ARQ yang dikirimkan hanyalah frame yang terjadi kesalahan saja. Gambar 3.14 menjelaskan mekanisme tersebut.



Gambar 3.14 Selective-report ARQ

3.3.4 Contoh Continuous ARQ

Untuk lebih memahami mekanisme error control dari kedua mekanisme terakhir dan mengetahui perbedaan diantara keduanya dapat dilihat tampilan pada gambar 3.15 yang memperlihatkan aliran frame-frame secara kontinyu.



Gambar 3.15 Contoh continuous ARQ

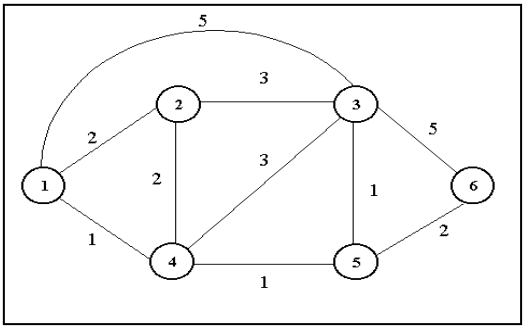
3.4. Referensi

1. Tanenbaum, AS, *Computer Networks*, Prentise Hall, 1996
2. Stallings, W. *Data and Computer Communications*, Macmillan Publishing Company, 1985.
3. Stallings, W. *Local Network*, Macmillan Publishing Company, 1985.
4. Black, U.D, *Data Communications and Distributed Networks*, Prentise Hall.
5. Raj Jain, Professor of CIS The Ohio State University Columbus, OH 43210 Jain@ACM.Org http://www.cis.ohio-state.edu/~jain/cis677-98/
6. Cisco Press http://www.cicso.com/cpress/cc/td/cpress/fund/ith2nd/it2401.html

4 Networking

Sebelum masuk ke pembahasan yang lebih mendalam, sebaiknya kita mengenal pengertian istilah packet switching, virtual circuit dan datagram. Selanjutnya fokus pembahasan bab ini meliputi mekanisme dan algoritma routing, traffic control, internetworking dan pembahasan tentang protokol internet

Untuk membantu pemahaman, beberapa pembahasan routing akan mengacu ke gambar jaringan berikut (gambar 4.1). Rute-rute pada jaringan tersebut menghubungkan 6 titik (node).



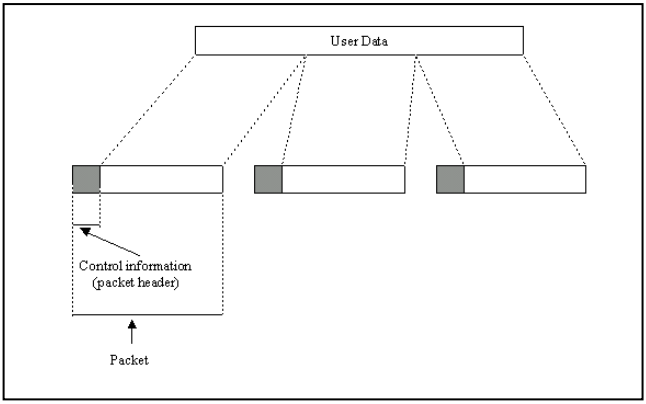
Gambar 4.1. Rute jaringan 6 titik

4.1 Prinsip *Packet Switching, Virtual Circuit* dan *Datagram*

Pada hubungan *Circuit Switching*, koneksi biasanya terjadi secara fisik bersifat point to point. Kerugian terbesar dari teknik ini adalah penggunaan jalur yang bertambah banyak untuk jumlah hubungan yang meningkat. Efek yang timbul adalah *cost* yang akan semakin meningkat di samping pengaturan switching menjadi sangat

komplek. Kelemahan yang lain adalah munculnya *idle time* bagi jalur yang tidak digunakan. Hal ini tentu akan menambah inefisiensi. Model *circuit switching*, karena sifatnya, biasanya mentransmisikan data dengan kecepatan yang konstan, sehingga untuk menggabungkan suatu jaringan dengan jaringan lain yang berbeda kecepatan tentu akan sulit diwujudkan.

Pemecahan yang baik yang bisa digunakan untuk mengatasi persoalan di atas adalah dengan metoda *data switching*. Dengan pendekatan ini, pesan yang dikirim dipecah-pecah dengan besar tertentu dan pada tiap pecahan data ditambahkan informasi kendali. Informasi kendali ini, dalam bentuk yang paling minim, digunakan untuk membantu proses pencarian rute dalam suatu jaringan ehingga pesan dapat sampai ke alamat tujuan. Contoh pemecahan data menjadi paket-paket data ditunjukkan pada gambar.



Gambar 4.2 Pemecahan Data menjadi paket-paket

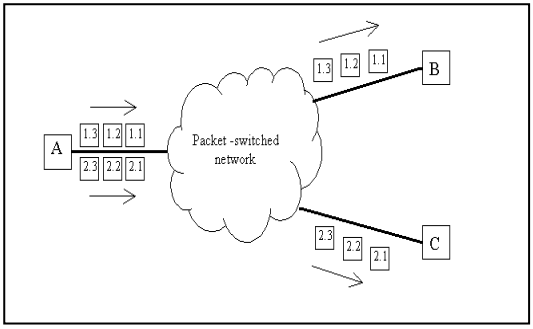
Penggunaan Data Switching mempunyai keuntungan dibandingkan dengan penggunaan Circuit switching antara lain :

1. Efisiensi jalur lebih besar karena hubungan antar node dapat menggunakan jalur yang dipakai bersama secara dianmis tergantung banyakanya paket yang dikirm.

2. Bisa mengatasi permasalah data rate yang berbeda antara dua jenis jaringan yang berbeda data rate-nya.
3. Saat beban lalulintas menignkat, pada model *circuit switching*, beberapa pesan yang akan ditransfer dikenai pemblokiran. Transmisi baru dapat dilakukan apabila beban lalu lintas mulai menurun. Sedangkan pada model *data switching*, paket tetap bisa dikirimkan, tetapi akan lambat sampai ke tujuan (delivery delay meningkat).
4. Pengiriman dapat dilakukan berdasarkan prioritas data. Jadi dalam suatu antrian paket yang akan dikirim, sebuah paket dapat diberi prioritas lebih tinggi untuk dikirm dibanding paket yang lain. Dalam hal ini, prioritas yang lebih tinggi akan mempunyai delivery delay yang lebih kecil dibandingkan paket dengan prioritas yang lebih rendah.

Virtual circuit eksternal dan internal

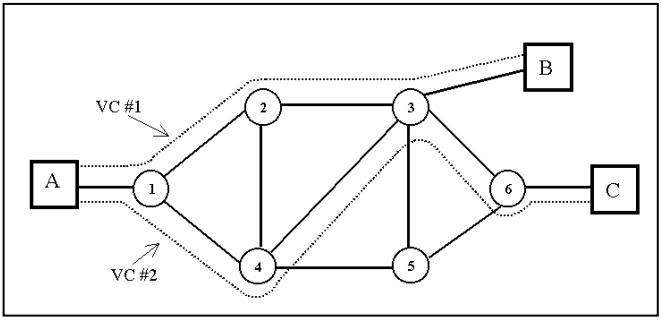
Virtual Circuit pada dasarnya adalah suatu hubungan secara logik yang dibentuk untuk menyambungkan dua stasiun. Paket dilabelkan dengan nomor sirkit maya dan nomor urut. Paket dikirimkan dan datang secara berurutan. Gambar berikut ini menjelaskan keterangan tersebut.



Gambar 5.3.Virtual Circuit eksternal

Stasiun A mengirimkan 6 paket. Jalur antara A dan B secara logik disebut sebagai jalur 1, sedangkan jalur antara A dan C disebut sebagai jalur 2. Paket pertama yang akan dikirimkan lewat jalur 1 dilabelkan sebagai paket 1.1, sedangkan paket ke-2 yang dilewatkan jalur yang sama dilabelkan sebagai paket 1.2 dan paket terakhir yang dilewatkan jalur 1 disebut sebagai paket 1.3. Sedangkan paket yang pertama yang dikirimkan lewat jalur 2 disebut sebagai paket 2.1, paket kedua sebagai paket 2.2 dan paket terakhir sebagai paket 2.3 Dari gambar tersebut kiranya jelas bahwa paket yang dikirimkan diberi label jalur yang harus dilewatinya dan paket tersebut akan tiba di stasiun yang dituju dengan urutan seperti urutan pengiriman.

Secara internal rangkaian maya ini bisa digambarkan sebagai suatu jalur yang sudah disusun untuk berhubungan antara satu stasiun dengan stasiun yang lain. Semua paket dengan asal dan tujuan yang sama akan melewati jalur yang sama sehingga akan samapi ke stasiun yang dituju sesuai dengan urutan pada saat pengiriman (FIFO). Gambar berikut menjelaskan tentang sirkit maya internal.

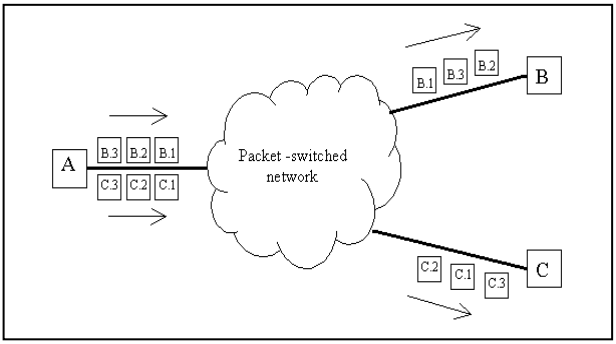


Gambar 4.4. *Virtual Circuit* internal

Gambar 4.4 menunjukkan adanya jalur yang harus dilewati apabila suatu paket ingin dikirimkan dari A menuju B (sirkit maya 1 atau *Virtual Circuit* 1 disingkat VC #1). Sirkit ini dibentuk denagan rute melewati node 1-2-3. Sedangkan untuk mengirimkan paket dari A menuju C dibentuk sirkit maya VC #2, yaitu rute yang melewati node 1-4-3-6.

Datagram eksternal dan internal

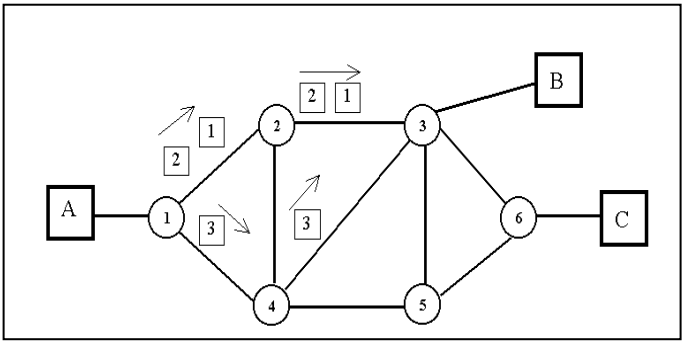
Dalam bentuk datagram, setiap paket dikirimkan secara independen. Setiap paket diberi label alamat tujuan. Berbeda dengan sirkit maya, datagram memungkinkan paket yang diterima berbeda urutan dengan urutan saat paket tersebut dikirim. Gambar 5.5 berikut ini akan membantu memperjelas ilustrasi.
Jaringan mempunyai satu stasiun sumber, A dan dua stasiun tujuan yakni B dan C. Paket yang akan dikirimkan ke stasiun B diberi label alamat stasiun tujuan yakni B dan ditambah nomor paket sehingga menjadi misalnya B.1, B.37, dsb. Demikian juga paket yang ditujukan ke stasiun C diberi label yang serupa, misalnya paket C.5, C.17, dsb.



Gambar 4.5 *Datagram* eksternal

Dari gambar 4.5, stasiun A mengirimkan enam buah paket. Tiga paket ditujukan ke alamat B. Urutan pengiriman untuk paket B adalah paket B.1, Paket B.2 dan paket B.3. sedangkan tiga paket yang dikirimkan ke C masing-masing secara urut adalah paket C.1, paket C.2 dan paket C.3. Paket-paket tersebut sampai di B dengan

urutan kedatangan B.2, paket B.3 dan terakhir paket B.1 sedangan di statiun C, paket paket tersebut diterima dengan urutan C.3, kemudian paket C.1 dan terakhir paket C.2. Ketidakurutan ini lebih disebabkan karena paket dengan alamat tujuan yang sama tidak harus melewati jalur yang sama. Setiap paket bersifat independen terhadap sebuah jalur. Artinya sebuah paket sangat mungkin untuk melewati jalur yang lebih panjang dibanding paket yang lain, sehingga waktu yang dibutuhkan untuk sampai ke alamat tujuan berbeda tergantung rute yang ditempuhnya. Secara internal datagram dapat digambarkan sebagai berikut



Gambar 4.6. Datagram internal

Sangat dimungkinkan untuk menggabungkan antara keempat konfigurasi tersebut menjadi beberapa kemungkinan berikut.

- *Virtual Circuit* eksternal, *virtual circuit* internal
- *Virtual Circuit* eksternal, *Datagram* internal
- *Datagram* eksternal, *datagram* internal
- *Datagram* eksternal, *virtual circuit* internal

4.2. *Routing*

Fungsi utama dari jaringan ***packet-switched*** adalah menerima paket dari stasiun pengirim untuk diteruskan ke stasiun penerima. Untuk keperluan ini, suatu jalur atau rute dalam jaringan tersebut harus dipilih, sehingga akan muncul lebih dari satu kemungkinan rute untuk mengalirkan data. Untuk itu fungsi dari routing harus diwujudkan. Fungsi routing sendiri harus mengacu kepada nilai nilai antara lain : tanpa kesalahan, sederhana, kokoh, stabil, adil dan optimal disamping juga harus mengingat perhitungan faktor efisiensi.

Untuk membentuk routing, maka harus mengetahui unsur-unsur routing, antara lain (lebih jelas lihat Stalling, 1994) :

- Kriteria Kinerja :
  - Jumlah hop
  - Cost
  - Delay
  - Througput
- Decision Time
    - Paket (datagram)
    - Session (virtual Circuit)
- Decision Place
  - Each Node (terdistribusi)
  - Central Node (terpusat)
  - Originating Node
- Network Information source
    - None
    - Local
    - Adjacent nodes
    - Nodes along route
    - All Nodes
- Routing Strategy
    - Fixed
    - Flooding
    - Random
    - Adaptive
- Adaptive Routing Update Time
    - Continuous
    - Periodic

- Major load change
- Topology change

Algoritma Routing

Forward-search algorithm dinyatakan sebagai menentukan jarak terpendek dari node awal yang ditentukan ke setiap node yang ada.Algoritma diungkapkan dalam stage. Dengan k buah stage, jalur terpendek node k terhadap node sumber ditentukan. Node-node ini ada dalam himpunan N. Pada stage ke (k+1), node yang tidak ada dalam M yang mempunyai jarak terpendek terhadap sumber ditambahkan ke M. Sebagai sebuah node yang ditambahkan dalam M, maka jalur dari sumber menjadi terdefinisi.

Algoritma ini memiliki 3 tahapan :

1. Tetapkan M={S}. Untuk tiap node $n \in N-S$, tetapkan $C_1(n)=l(S,n)$.
2. Cari $W \in N-M$ sehingga $C_1(W)$ minimum dan tambahkan ke M. Kemudian $C_1(n) = MIN[C_1(n), C_1(W) + l(W,n)$ untuk tiap node $n \in N-M$. Apabila pada pernyataan terakhir bernilai minimum, jalur dari S ke n sebagai jalur S ke W memotong link dari W ke n.
3. Ulang langkah 2 sampai M=N.

Keterangan :
N = himpunan node dalam jaringan
S = node sumber
M = himpunan node yang dihasilkan oleh algoritma
l(I,J) = link cost dari node ke I sampi node ke j, biaya bernilai ∞ jika node tidak secara langsung terhubung.
C1(n) : Biaya dari jalur biaya terkecil dari S ke n yang dihasilkan pada saat algoritma dikerjakan.

Tabel berikut ini memperlihatkan hasil algoritma terhadap gambar di muka. Dengan menggunakan S=1.

Tabel 4.1 Hasil *forward search algorithm*

Iterasi	M	$C_1(2)$	Path	$C_1(3)$	Path	$C_1(4)$	Path	$C_1(5)$	Path	$C_1(6)$	Path
1	{1}	2	1-2	5	1-4	1	1-4	∞~	--	~∞	--
2	{1,4}	2	1-2	4	1-4	1	1-4	2	1-4-5	∞	--
3	{1,2,4}	2	1-2	4	1-4	1	1-4	2	1-4-5	∞	--
4	{1,2,4,5}	2	1-2	3	1-4	1	1-4	2	1-4-5	4	1-4-5-6
5	{1,2,3,4,5}	2	1-2	3	1-4	1	1-4	2	1-4-5	4	1-4-5-6
6	{1,2,3,4,5,6}	2	1-2	3	1-4	1	1-4	2	1-4-5	4	1-4-5-6

Backward search algorithm

Menentukan jalur biaya terkecil yang diberikan node tujuan dari semua node yang ada. Algoritma ini juga diproses tiap stage. Pada tiap stage, algoritma menunjuk masing-masing node.
Definisi yang digunakan :
N = Himpunan node yang terdapat pada jaringan
D= node tujuan
l(i,j) = seperti keterangan di muka
$C_2(n)$ = biaya dari jalur biaya terkecil dari n ke D yang dihasilkan saat algoritma dikerjakan.

Algoritma ini juga terdiri dari 3 tahapan :

1. Tetapkan $C_2(D)=0$. Untuk tiap node $n \in N-D$, tetapkan $C_2(n) = \infty$.
2. Untuk tiap node $n \in N-D$, tetapkan $C_2(n)=MIN\ W \in N[C_2(n), C_2(W) + l(n,W)]$. Apabila pada pernyataan terakhir bernilai minimum, maka jalur dari n ke D saat ini merupakan link dari n ke W dan menggantikan jalur dari W ke D
3. Ulangi langkah ke –2 sampai tidak ada cost yang berubah.

Tabel berikut adalah hasil pengolahan gambar 1 dengan D=1

Tabel 4.1 Hasil *backward search algorithm*

Iterasi	$C_2(2)$	Path	$C_2(3)$	Path	$C_2(4)$	Path	$C_2(5)$	Path	$C_2(6)$	Path
1	∞	--	∞	--	∞	--	∞	--	∞	--
2	2	2-1	5	3-1	1	4-1	2	5-4-1	4	6-5-4-1
3	2	2-1	3	3-5-4-1	1	4-1	2	5-4-1	4	6-5-4-1
4	2	2-1	3	3-5-4-1	1	4-1	2	5-4-1	4	6-5-4-1

Strategi *Routing*

Terdapat beberapa strategi untuk melakukan routing, antara lain :

- ***Fixed Routing***

  Merupakan cara routing yang paling sederhana. Dalam hal ini rute bersifat tetap, atau paling tidak rute hanya diubah apabila topologi jaringan berubah. Gambar berikut (mengacu dari gambar 1) memperlihatkan bagaimana sebuah rute yang tetap dikonfigurasikan.

CENTRAL ROUTING DIRECTORY

From Node \ To node	1	2	3	4	5	6
1	-	2	4	4	4	4
2	1	-	3	4	4	4
3	5	2	-	5	5	5
4	1	2	5	-	5	5
5	4	4	3	4	-	6
6	5	5	5	5	5	-

Gambar 4.7. Direktori untuk *fixed routing*

Kemungkinan rute yang bisa dikonfigurasikan, ditabelkan sebagai berikut :

Node 1 Directory

Destination	Next node
2	2
3	4
4	4
5	4
6	4

Node 2 Directory

Destination	Next node
1	1
3	3
4	4
5	4
6	4

Node 3 Directory

Destination	Next node
1	5
2	2
4	5
5	5
6	5

Node 4 Directory

Destination	Next node
1	1
2	2
3	5
5	5
6	5

Node 5 Directory

Destination	Next node
1	4
2	4
3	3
4	4
6	6

Node 6 Directory

Destination	Next node
1	5
2	5
3	5
4	5
5	5

Gambar 4.8 Direktori masing-masing node

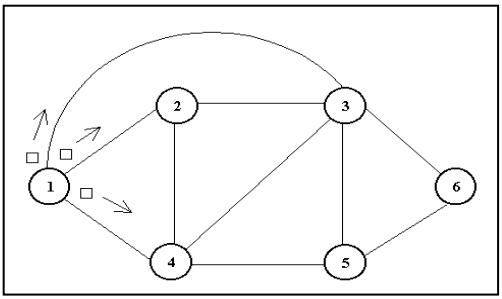
Tabel ini disusun berdasar rute terpendek (menggunakan least-cost algorithm). Sebagai misal direktori node 1. Dari node 1 untuk mencapai node 6, maka rute terpendek yang bisa dilewati adalah rute dari node 1,4,5,6. Maka pada tabel direktori node 1 dituliskan destination = 6, dan next node = 4.

Keuntungan konfigurasi dengan rute tetap semacam ini adalah bahwa konfigurasi menajdi sederhana. Pengunaan sirkit maya atau datagram tidak dibedakan. Artinya semua paket dari sumber menuju titik tujuan akan melewati rute yang sama. Kinerja yang bagus didapatkan apabila beban bersifat tetap. Tetapi pada beban yang bersifat dinamis, kinerja menjadi turun. Sistem ini tidak memberi tanggapan apabila terjadi error maupun kemacetan jalur.

- ***Flooding***

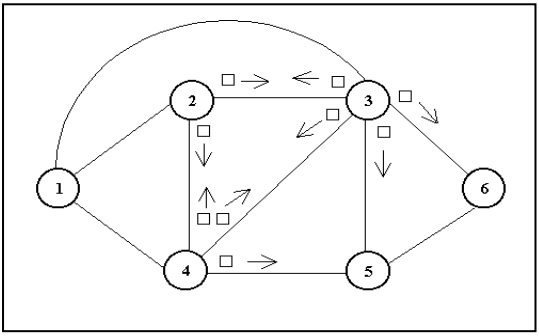
Teknik routing yang lain yang dirasa sederhana adalah ***flooding.*** Cara kerja teknik ini adalah mengirmkan paket dari suatu sumber ke seluruh node tetangganya. Pada tiap node, setiap paket yang datang akan ditransmisikan kembali ke seluruh link yang dipunyai kecuali link yang dipakai untuk menerima paket tersebut. Mengambil contoh rute yang sama, sebutlah bahwa node 1 akan mengirimkan paketnya ke node 6. Pertamakali node

1 akan mengirimkan paket keseluruh tetangganya, yakni ke node 2, node 4 dan node 5 (gambar 5.9)



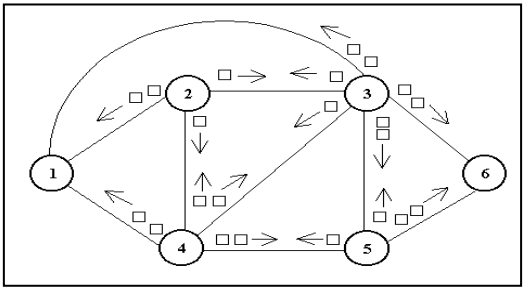
Gambar 4.9. Hop pertama.

Selanjutnya operasi terjadi pada node 2, 3 dan 4. Node 2 mengirimkan paket ke tetangganya yaitu ke node 3 dan node 4. Sedangkan node 3 meneruskan paket ke node 2,4,5 dan node 6. Node 4 meneruskan paket ke node 2,3,5. Semua node ini tidak mengirimkan paket ke node 1. Ilustrasi tersebut digambarkan pada gambar 4.10.



Gambar 4.10 Hop kedua

Pada saat ini jumlah copy yang diciptakan berjumlah 9 buah. Paket-paket yang sampai ke titik tujuan, yakni node 6, tidak lagi diteruskan.
Posisi terakhir node-node yang menerima paket dan harus meneruskan adalah node 2,3,4,5. Dengan cara yang sama masing-masing node tersebut membuat copy dan memberikan ke mode tetangganya. Pada saat ini dihasilkan copy sebanyak 22.



Gambar 4.11. Hop ketiga

Terdapat dua catatan penting dengan penggunaan teknik flooding ini, yaitu :

1. Semua rute yang dimungkinkan akan dicoba. Karena itu teknik ini memiliki keandalan yang tinggi dan cenderung memberi prioritas untuk pengiriman-pengiriman paket tertentu.
2. Karena keseluruhan rute dicoba, maka akan muncul paling tidak satu buah copy paket di titik tujuan dengan waktu paling minimum. Tetapi hal ini akan menyebakan naiknya bebean lalulintas yang pada akhirnya menambah delay bagi rute-rute secara keseluruhan.

Random Routing

Prinsip utama dari teknik ini adalah sebuah node memiliki hanya satu jalur keluaran untuk menyalurkan paket yang datang kepadanya. Pemilihan terhadap sebuah jalur keluaran bersifat acak. Apabila link yang akan dipilih memiliki bobot yang sama, maka bisa dilakukan dengan pendekatan seperti teknik *round-robin*.

Routing ini adalah mencari probabilitas untuk tiap-tiap *outgoing link* dan memilih link berdasar nilai probabilitasnya. Probabilitas bisa dicari berdasarkan data rate, dalam kasus ini didefisinikan sebagai

$$P_i = \frac{R_i}{\Sigma_i R_i}$$

Di mana :

P_i = probabilitas pemilihan i

R_j = *data rate* pada link j

Penjumlahan dilakukan untuk keseluruhan *link outgoing*. Skema seperti ini memungkinkan distribusi lalulintas yang baik. Seperti teknik flooding, Random routing tidak memerlukan informasi jaringan, karena rute akan dipilih dengan cara random.

Adaptive Routing

Strategi routing yang sudah dibahas dimuka, tidak mempunyai reaksi terhadap perubanhan kondisi yang terjadi di dalam suatu jaringan. Untuk itu pendekatan dengan strategi adaptif mempunyai kemapuan yang lebih dibandingkan dengan beberapa hal di muka. Dua hal yang penting yang menguntungkan adalah :

- Strategi routing adaptif dapat meningkatkan performance seperti apa yang keinginan user
- Strategi adaptif dapat membantu kendali lalulintas.

Akan tetapi, strategi ini dapat menimbulkan beberapa akibat, misalnya :

- Proses pengambilan keputusan untuk menetapkan rute menjadi sangat rumit akibatnya beban pemrosesan pada jaringan meningkat.
- Pada kebanyakan kasu, strategi adaptif tergantung pada informasi status yang dikumpulkan pada satu tempat tetapi

digunakan di tempat lain. Akibatnya beban lalu lintas meningkat

- Strategi adaptif bisa memunculkan masalah seperti kemacetan apabila reaksi yang terjadi terlampau cepat, atau menjadi tidak relevan apabila reaksi sangat lambat.

Kategori Strategi Adaptif dapat dibagi menjadi :

- *Isolated adaptive* : informasi lokal, kendali terdistribusi
- *Distributed Adaptive* : informasi dari node yang berdekatan, kendali terdistribusi
- *Centralized Adaptive* : informasi dari selluruh node, kendali terpusat

Kendali lalu lintas

Konsep kendali lalulintas dalam sebuah jaringan *packet-switching* adalah komplek dan memiliki pendekatan yang banyak. Mekanisme kendali lalulintas sendiri mempunyai 3 tipe umum, yaitu *flow control, congestion control* dan *deadlock avoidance.*

Flow Control digunakan untuk mengatur aliran data dari dua titik. *Flow control* juga digunakan untuk hubungan yang bersifat *indirect*, seperti misal dua titik dalam sebuah jaringan *packet-switching* di mana kedua *endpoint*-nya merupakan sirkit maya. Secara fundamental dapat dikatakan bahwa fungsi dari *flow control* adalah untuk memberi kesempatan kepada penerima (receiver) agar dapat mengendalikan laju penerimaan data, sehingga ia tidak terbanjiri oleh limpahan data.

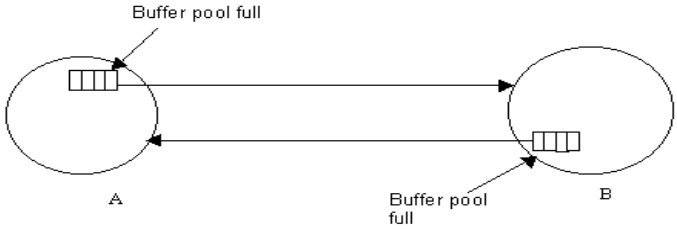
Congestion Control digunakan untuk menangani terjadinya kemacetan. Terjadinya kemacetan bisa diterangkan lewat uraian berikut. Pada dasarnya, sebuah jaringan packet-switched adalah jaringan antrian. Pada masing-masing node, terdapat sebuah antrian paket yang akan dikirimkan ke kanal tertentu. Apabila kecepatan datangya suatu paket dalam sebuah antrian lebih besar dibandingkan kecepatan pentransferan paket, maka akan muncul efek bottleneck. Apabila antrian makin panjang dan jumlah node yang menggunakn kanal juga bertambah, maka kemungkinan terjadi kemacetan sangat besar.

Permasalahan yang serius yang diakibatkan efek congestion adalah *deadlock*, yaitu suatu kondisi di mana sekelompok node tidak bisa meneruskan pengiriman paket karena tidak ada buffer yang tersedia. Teknik *deadlock avoidance* digunakan untuk mendisain jaringan sehingga *deadlock* tidak terjadi.

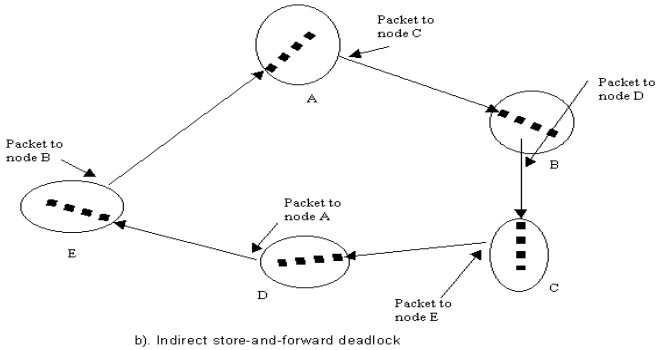
Bentuk *deadlock* yang paling sederhana adalah *direct store-and-forward deadlock.* Pada gambar 5.12(a) memperlihatkan situasi bagaimana antara node A dan node B berinteraksi di mana kedua buffer penuh dan deadlock terjadi.

Bentuk deadlock kedua adalah *indirect store-and-forward deadlock*(gambar 512(b)). Hal ini terjadi tidak pada sebuah link tunggal seperti bentuk deadlock di muka. Pada tiap node, antrian yang ditujukan untuk node terdekatnya bersifat searah dan menjadi penuh.

Bentuk deadlock yang ketiga adalah reassembly deadlock.Situasi ini digambarkan pada 5.12(c) di mana node C memiliki 4 paket terdiri dari paket 1 tiga buah dan sebuah paket 3. Seluruh buffer penuh dan tidak mungkin lagi menerima paket baru.



a). Direct store-and-forward deadlock



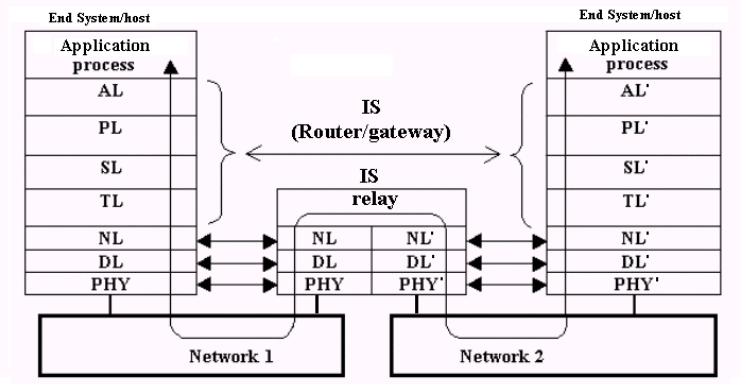
Gambar 4.12 Tipe-tipe deadlock

4.3 Internetworking

Ketika dua atau lebih jaringan bergabung dalam sebuah aplikasi, biasanya kita sebut ragam kerja antar sistem seperti ini sebagai sebauh internetworking. Penggunaaan istilah ***internetwork*** (atau juga ***internet***) mengacu pada perpaduan jaringan, misalnya LAN- WAN-LAN, yang digunakan. Masing-masing jaringan (LAN atau WAN) yang terlibat dalam internetwork disebut sebagai ***subnetwork*** atau ***subnet***.

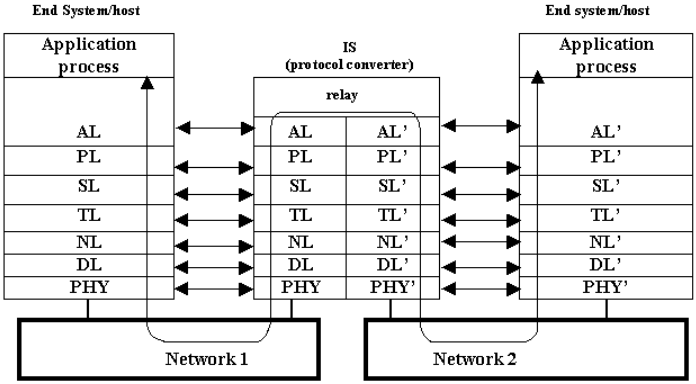
Piranti yang digunakan untuk menghubungkan antara dua jaringan, meminjam istilah ISO, disebut sebagai ***intermmediate system*** (IS) atau sebuah ***internetworking unit*** (IWU). Selanjutnya apabila fungsi utama dari sebuah *intermmediate system* adalah

melakukan routing, maka piranti dimaksud disebut sebagai ***router***, sedangkan apabila tugas piranti adalah menghubungkan antara dua tipe jaringan, maka disebut sebagai ***gateway.***



Gambar 4.13 Router /gateway

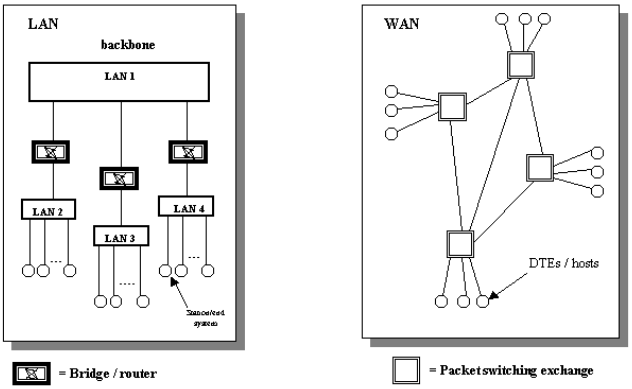
Sebuah ***protocol converter*** adalah sebuah IS yang menghubungkan dua jaringan yang bekerja dengan susunan protokol yang sangat berlainan, misalnya menghubungkan antara sebuah susunan protokol standar ISO dengan susunan protokol khusus dari vendor dengan susunan tertentu. *Protocol converter* dapat digambarkan seperti berikut ini :



Gambar 4.14 *Protocol converter*

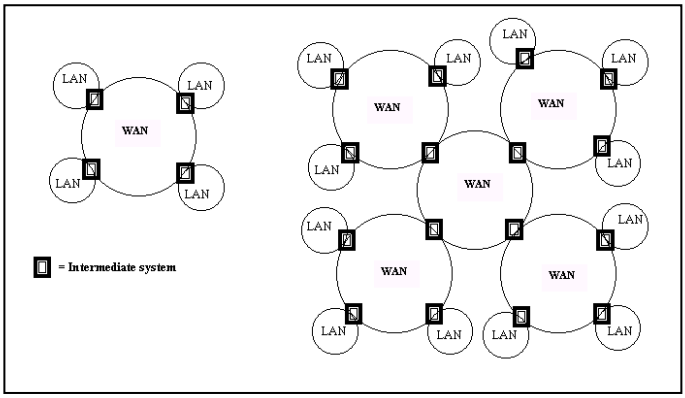
Arsitektur internetworking

Arsitektur internetwork diperlihatkan pada gambar berikut ini. Gambar 4.15 memperlihatkan dua contoh dari tipe jaringan tunggal. Yang pertama (gambar 4.15a) adalah site-wide LAN yang menggabungkan LAN satu gedung atau perkantoran yang terhubung lewat sebuah jaringan *backbone*. Untuk menggabungkan LAN dengan tipe yang sama menggunakan piranti bridge sedangkan untuk jaringan yang bertipe beda menggunakan router.
Contoh yang kedua (gambar 4.15b) adalah sebuah WAN tunggal, seperti jaringan X.25. Pada kasus ini, setiap pertukaran paket (DCE/PSE) melayani set DCE sendiri, yang secara langsung lewat sebuah PAD, dan tiap PSE terinterkoneksi oleh jaringan switching dengan topologi mesh.



Gambar (a) Gambar (b)

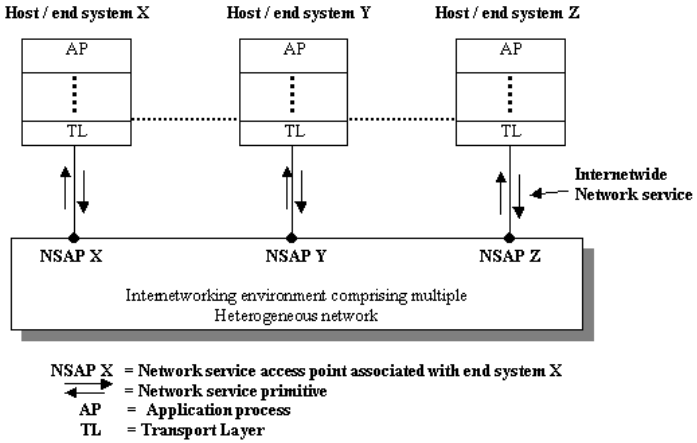
Gambar 4.15. Arsitektur internetwork



Gambar 4.16. Contoh Interkoneksi LAN/WAN

Network service

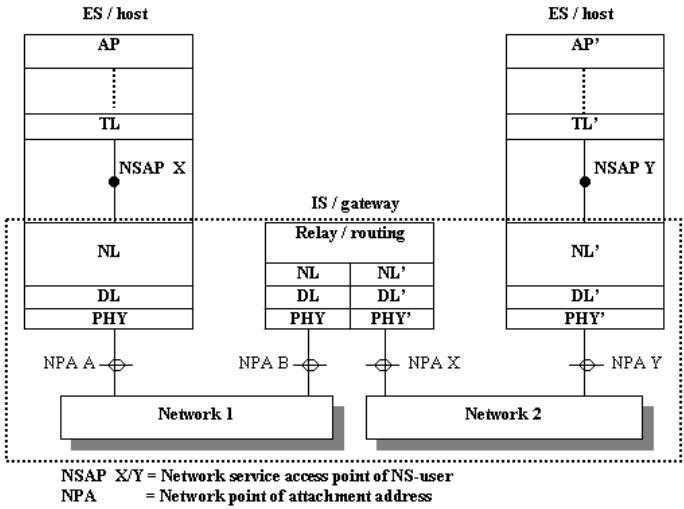
Pada sebuah LAN, Alamat sublayer MAC digunakan untuk mengidentifikasi ES (stasiun / DTE), dengan menggunakan untuk membentuk rute bagi frame antar sistem. Selebihnya, karena tunda transit yang pendek dan laju kesalahan bit yang kecil pada LAN, sebuah protokol jaringan tak terhubung sederhana biasanya digunakan. Artinya, kebanyakan LAN berbasis jaringan ***connectionless network access (CLNS)***
Berbeda dengan LAN, alamat-alamat lapisan link pada kebanyakan WAN lapisan network digunakan untuk mengidentifikasi ED dan membentuk rute bagi paket didalam suatu jaringan. Karena WAN mempunyai transit yang panjang dan rentan terhadap munculnya error, maka protokol yang berorientasi hubungan (koneksi) lebih tepat untuk digunakan. Artinya, kebanyakan WAN menggunakan ***connection-oriented network service (CONS)***



Gambar 4.17 Skema pelayanan jaringan internet

Pengalamatan

Alamat Network Service Access Point (NSAP) dipakai untuk mengidentifikasi sebuah NS_user dalam suatu end system (ES) adalah sebagai alamat network-wide unik yang membuat user teridentifikasi secara unik dalam keseluruhan jaringan. Dalam sebuah LAN atau WAN, alamat NSAP harus unik (dengan suatu batasan) di dalam domain pengalamatan jaringan tunggal. Alamat NSAP dari NS_user dibangun dari alamat point of attachtment (PA) yang digabung dengan LSAP (link) dan selector alamat interlayer NSAP (network) dalam sistem.



Gambar 4.18 Hubungan antara alamat NSAP dan NPA

Untuk sebuah internet yang terbentuk dari beberapa jaringan dengan tipe yang berlainan, sebgai contoh LAN dengan X.25 WAN, mempunyai fornmat (susunan) dan sintaks yang berbeda dengan alamat PA dari end system atau ES (dalam hal ini juga IS). Apabila terdapat beberapa jaringan yang terhubung, maka alamat network point of attatchment (NPA) tidak bisa digunakan sebagai dasar

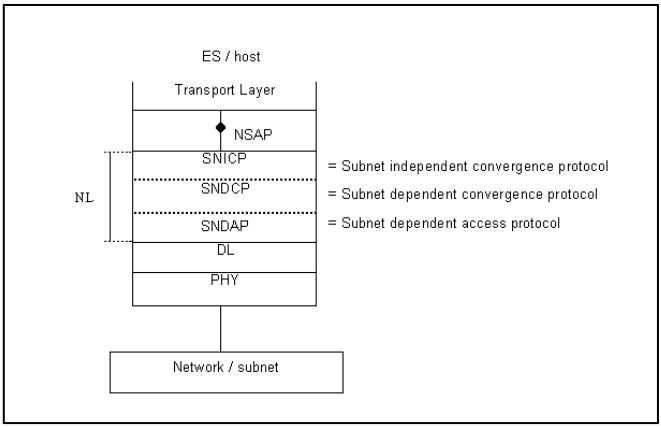
alamat NSAP dari NS_user. Untuk pembentukan sebuah open system internetworking environment (OSIE), maka NSAP dengan susunan yang berbeda harus digunakan untk mengidentifkasi NS_user. Pengalamatan baru ini bersifat independen dari alamat NPA. Hubungan antara alamat NSAP dan NPA ditunjukkan pada gambar 4.18. Terlihat bahwa terdapat dua alamat yang sama sekali berbeda untuk masing-masing ESyang terhubung ke internet yaitu NPA dan NSAP. Almat NPA memungkinkan sistem melakukan pengiriman dan penerimaan NPDU dilingkungan lokal, sedangkan alamat NSAP berlaku untuk identifikasi NS_user dalam sebuah jaringan yang lebih luas (internetwide atau keseluruhan OSIE). Apabila sebuah IS terhubung ke lebih dari sebuah jaringan, ia harus memiliki alamat sesuai dengan NPA untuk masing-masing jaringan yang dimasukinya.

Susunan Lapisan Network

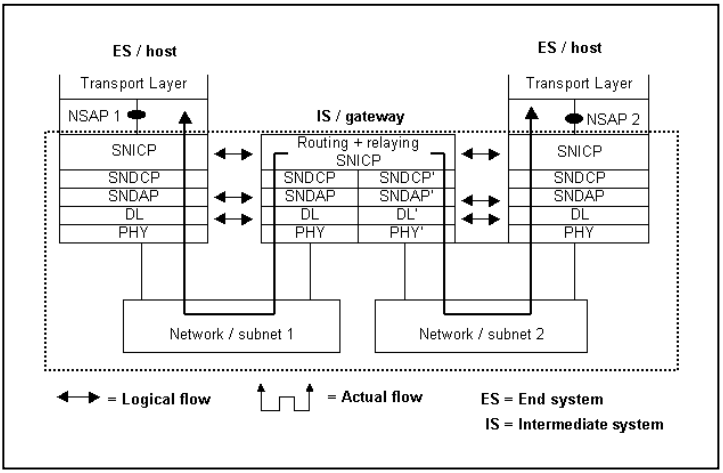
Aturan dari lapisan jaringan untk tiap-tiap End System adalah untuk membentuk hubungan end to end. Bisa jadi hubgunan ini berbentuk CON atau CLNS. Dalam kedua bentuk tersebut, NS_user akan berhubungan tidak peduli berapa banyak tipe jaingan yang terlibat. Untuk itu diperlukan router.
Untuk mencapai tujuan interkloneksi yang demikian ini, maka sesuai model referensi OSI, lapisan network tiap-tiap ES dan IS tidak hanya terdiri dari sebuah protokol tetapi paling tidak tiga (sublayer) protokol. Masing-=masing protokol ini akan membentuk aturan yang lengkap dalam sistem pelayanan antar lapisan jaringan. Dalm terminologi ISO, masing-masing jaringan yang membangun internet yang dikenal sebagai subnet, memliki tiga protokol penting yaitu :

- *Subnetwork independent convergence Protocol (SNICP)*
- *Subnetwork dependent convergence protocol (SNDCP)*
- *Subnetwork dependent access protocol (SNDAP)*

Susunan ketiga protokol tersebut dalam ES digambarkan dalam gambar 4.19. Gambar 4.19(a) memperlihatkan bagian-bagian protokol tersebut dalam lapisan network (NL), sedangkan gambar 4.19(b) memeperlihatkan hubungannya dengan sebuah IS.



Gambar 4.19(a). Tiga buah protokol dalam NL



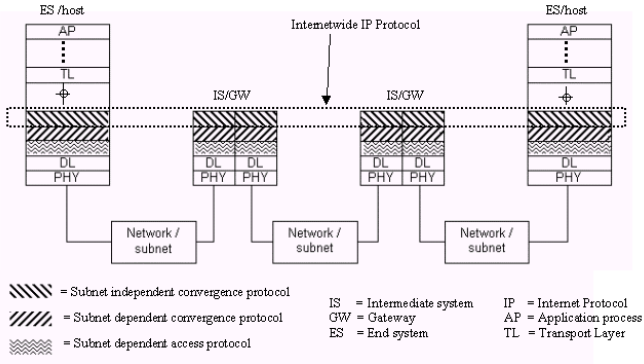
Gambar 4.19(b). Struktur IS

4.4. Standar Protokol Internet

Beragam WAN tipe X.25 dapat diinterkoneksikan dengan gateway berbasis X.75. Penggunaan sebuah standar yang mespesifikasikan

operasi protokol lapisan paket X.25 dalam LAN berarti sebuah pendekatan internetworking dengan mengadopsi X.25 sebagai sebuah protokol *internetwide* yang pada akhirnya dapat bekerja dalam modus *connection-oriented* atau mode *pseudoconnectionless*. Pemecahan ini menarik karena fungsi-fungsi *internetworking* terkurangi. Kerugian pendekatan ini adalah munculnya *overhead* pada paket X.25 menjadi tinggi dan *throughput* paket untuk jaringan ini menjadi rendah.

Pemecahan tersebut mengadopsi ISO berdasar pada pelayanan *internet connectionless (connectionles internet service)* dan sebuah *associated connectionless* SNICP. SNICP didefinisikan dalam ISO 8475. Pendekatan ini dikembangkan oleh US *Defense Advanced Research Project Agency* (DARPA). Internet yang dibangun pada awalnya diberi nama ARPANET, yang digunakan untuk menghubungkan beberapa jaringan komputer dengan beberapa situs penelitian dan situs universitas.



Gambar 4.20 Skema IP internetwide

Protokol internet hanyalah sebuah protokol yang berasosiasi dengan deretan protokol lengkap (stack) yang digunakan galam internet. Deretan protokol yang lengkap ini dikenal dengan istilah **TCP/IP**, meliputi protokol aplikasi dan protokol transport. Dua protokol yang menarik untuk dikaji adalah jenis protokol *Internet Protocol* atau dikenal sebagai **IP** dan *ISO Internet Protocol* atau dikenal sebagai

ISO-IP atau **ISO CLNP**. Secara umum pendekatan dua protokol ini dapat digambarkan pada gambar 4.20.

Internet Protocol merupakan protokol internetwide yang dapat menghubungkan dua entitas protokol transport yang berada pada ES atau *host* yang berbeda agar dapat saling menukarkan unit-unit pesan (NSDU). Protokol jenis ini sangat luas digunakan untuk internet jenis komersial maupun riset.

Jenis yang kedua yaitu **ISO-IP** atau **ISO CLNP** menggunakan acuan internetwide, connectionless dan subnetwork-independent convergence protocol. Protokol ini didefinisikan secara lengkap di ISO 8473. Dalam sebuah protokol internetworking yang lengkap, terdapat dua subnet yaitu *inactive network protocol* dan *nonsegmenting protocol*. Model protokol jaringan modus *connectionless* biasanya digunakan dalam LAN dan dginakankan untuk aplikasi-aplikasi jaringan tunggal (dalam hal ini sumber dan tujuan tergabung dalam sebuah jaringan. Sedangkan protokol *nonsegmenting* (dalam terminologi IP disebut *nonfragmenting*) digunakan dalam internet yang mengandung subnet dengan ukuran paket maksimum yang tidak boleh lebih dari yang dibutuhkan oleh NS_user untuk mentransfer data.

4.5 Referensi

1. Stallings, William, Data and Computer Communications, Macxmillan,1985
2. Stallings, William, Data and Computer Communications, Prentice Hall,1994
3. Halsall, Fred, Data Communications, Computer Networks and Open System, Addison-Wesley Pub.Co,1996

5 Keamanan Jaringan

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan sistem saat ini menjadi suatu garapan yang membutuhkan biaya penanganan dan proteksi yang sedemikian besar. Sistem-sistem vital seperti sistem pertahanan, sistem perbankan dan sistem-sistem setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan karena kemajuan bidang jaringan komputer dengan konsep open sistemnya sehingga siapapun, di manapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut.

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh person yang tidak diijinkan. Beberapa insinyur jaringan mengatakan bahwa hanya ada satu cara mudah dan ampuh untuk mewujudkan sistem jaringan komputer yang aman yaitu dengan menggunakan pemisah antara komputer dengan jaringan selebar satu inci, dengan kata lain, hanya komputer yang tidak terhubung ke jaringanlah yang mempunyai keamanan yang sempurna. Meskipun ini adalah solusi yang buruk, tetapi ini menjadi trade-off antara pertimbangan fungsionalitas dan memasukan kekebalan terhadap gangguan.

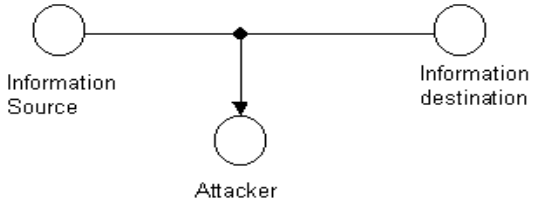
Protokol suatu jaringan sendiri dapat dibuat aman. Server-server baru yang menerapkan protokol-protokol yang sudah dimodifikasi harus diterapkan. Sebuah protokol atau layanan (service) dianggap cukup aman apabila mempunyai kekebalan ITL klas 0 (tentang ITL akan dibahas nanti). Sebagai contoh, protokol seperti FTP atau Telnet, yang sering mengirimkan password secara terbuka melintasi jaringan, dapat dimodifikasi dengan menggunakan teknik enkripsi. Jaringan daemon, seperti sendmail atau fingerd, dapat dibuat lebih aman oleh pihak vendor dengan pemeriksaan kode dan patching. Bagaimanapun, permasalahan mis-konfigurasi, seperti misalnya spesifikasi yang tidak benar dari netgroup, dapat

menimbulkan permasalahan kekebalan (menjadi rentan). Demikian juga kebijakan dari departemen teknologi informasi seringkali memunculkan kerumitan pemecahan masalah untuk membuat sistem menjadi kebal.

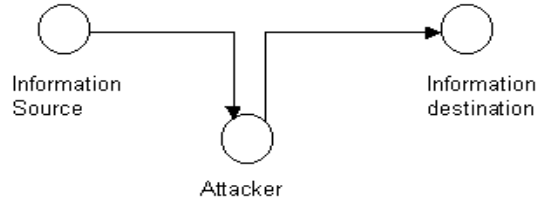
Tipe *Threat*

Terdapat dua kategori threat yaitu ***threat* pasif** dan ***threat* aktif**.

***Threat* pasif** melakukan pemantauan dan atau perekaman data selama data ditranmisikan lewat fasilitas komunikasi. Tujuan penyerang adalah untuk mendapatkan informasi yang sedang dikirimkan. Kategori ini memiliki dua tipe *yaitu release of message contain* dan *traffic analysis*. Tipe *Release of message contain* memungkinan penyusup utnuk mendengar pesan, sedangkan tipe *traffic analysis* memungkinan penyusup untuk membaca *header* dari suatu paket sehingga bisa menentukan arah atau alamat tujuan paket dikirimkan. Penyusup dapat pula menentukan panjang dan frekuensi pesan.



(a) Threat pasif



(b) Threat aktif

Gambar 5.1 Kategori threat

***Threat* aktif** merupakan pengguna gelap suatu peralatan terhubung fasilitas komunikasi untuk mengubah transmisi data atau mengubah isyarat kendali atau memunculkandata atau isyarat kendali palsu. Untuk kategori ini terdapat tida tipe yaitu : *message-stream modification, denial of message service* dan *masquerade*. Tipe *message-stream modification* memungkinan pelaku untuk memilih untuk menghapus, memodifikasi, menunda, melakukan reorder dan menduplikasi pesan asli. Pelaku juga mungkin untuk menambahkan pesan-pesan palsu. Tipe *denial of message service* memungkinkan pelaku untuk merusak atau menunda sebagian besar atau seluruh pesan. Tipe *masquerade* memungkinkan pelaku untuk menyamar sebagi host atau switch asli dan berkomunikasi dengan yang host yang lain atau switch untuk mendapatkan data atau pelayanan.

Internet Threat Level

Celah-celah keamanan sistem internet, dapat disusun dalam skala klasifikasi. Skala klasifikasi ini disebut dengan istilah skala Internet Threat Level atau skala ITL. Ancaman terendah digolongkan dalam ITL kelas 0, sedangkan ancaman tertinggi digolongkan dalam ITL kelas 9. Tabel 5.1 menjelaskan masing-masing kelas ITL.

Kebanyakan permasalahan keamanan dapat diklasifikasikan ke dalam 3 kategori utama, tergantung pada kerumitan perilaku ancaman kepada sistem sasaran, yaitu :

- Ancaman-ancaman lokal.
- Ancaman-ancaman remote
- Ancaman-ancaman dari lintas firewall

Selanjutnya klasifikasi ini dapat dipisah dalam derajat yang lebih rinci, yaitu :

- *Read access*
- *Non-root write and execution access*
- *Root write and execution access*

Table 5.1 Skala Internet Threat Level (ITL)

Kelas	Penjelasan
0	Denial of service attack—users are unable to access files or programs.
1	Local users can gain read access to files on the local system.
2	Local users can gain write and/or execution access to non–root-owned files on the system.
3	Local users can gain write and/or execution access to root-owned files on the system.
4	Remote users on the same network can gain read access to files on the system or transmitted over the network.
5	Remote users on the same network can gain write and/or execution access to non–root-owned files on the system or transmitted over the network.
6	Remote users on the same network can gain write and/or execution access to root-owned files on the system.
7	Remote users across a firewall can gain read access to files on the system or transmitted over the network.
8	Remote users across a firewall can gain write and/or execution access to non–root-owned files on the system or transmitted over the network.
9	Remote users across a firewall can gain write and/or execution access to root-owned files on the system.

Seberapa besar tingkat ancaman dapat diukur dengan melihat beberapa faktor, antara lain :

- Kegunaan sistem
- Kerahasiaan data dalam sistem.
- Tingkat kepetingan dari integritas data

- Kepentingan untuk menjaga akses yang tidak boleh terputus
- Profil pengguna
- Hubungan antara sistem dengan sistem yang lain.

ENKRIPSI

Setiap orang bahwa ketika dikehendaki untuk menyimpan sesuatu secara pribadi, maka kita harus menyembunyikan agar orang lain tidak tahu. Sebagai misal ketika kita megirim surat kepada seseorang, maka kita membungkus surat tersebut dengan amplop agar tidak terbaca oleh orang lain. Untuk menambah kerahasiaan surat tersebut agar tetap tidak secara mudah dibaca orang apabila amplop dibuka, maka kita mengupayakan untuk membuat mekanisme tertentu agar isi surat tidak secara mudah dipahami.

Cara untuk membuat pesan tidak mudah terbaca adalah enkripsi. Dalam hal ini terdapat tiga kategori enkripsi antara lain :

- Kunci enkripsi rahasia, dalam hal ini terdapat sebuah kunci yang digunakan untuk meng-enkripsi dan juga sekaligus men-dekripsi informasi.
- Kunci enksripsi public, dalam hal ini dua kunci digunakan, satu untuk proses enkripsi dan yang lain untuk proses dekripsi.
- Fungsi one-way, di mana informasi di-enkripsi untuk menciptakan “signature” dari informasi asli yang bisa digunakan untuk keperluan autentifikasi.

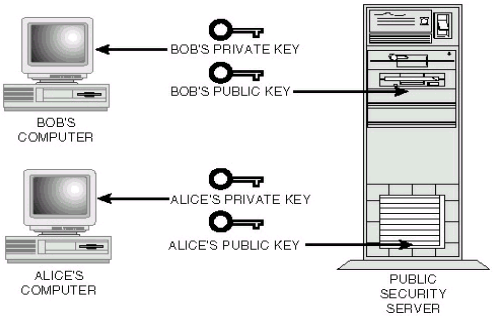
Enkripsi dibentuk dengan berdasarkan suatu algoritma yang akan mengacak suatu informasi menjadi bentuk yang tidak bisa dibaca atau tak bisa dilihat. Dekripsi adalah proses dengan algoritma yang sama untuk mengembalikan informasi teracak menjadi bentuk aslinya. Algoritma yang digunakan harus terdiri dari susunan prosedur yang direncanakan secara hati-hati yang harus secara efektif menghasilkan sebuah bentuk terenkripsi yang tidak bisa dikembalikan oleh seseorang bahkan sekalipun mereka memiliki algoritma yang sama.

Algoritma sederhana dapat dicontohkan di sini. Sebuah algoritma direncanakan, selanjutnya disebut algoritma (karakter+3), agar mampu mengubah setiap karakter menjadi karakter nomor tiga

setelahnya. Artinya setiap menemukan huruf A, maka algoritma kan mengubahnya menjadi D, B menjadi E, C menjadi F dan seterusnya. Sebuah pesan asli, disebut *plaintext* dalam bahasa kripto, dikonversikan oleh algoritma karakter+3 menjadi *ciphertext* (bahasa kripto untuk hasil enkripsi). Sedangkan untuk mendekripsi pesan digunakan algoritma dengan fungsi kebalikannya yaitu karakter-3

Metode enkripsi yang lebih umum adalah menggunakan sebuah algoritma dan sebuah kunci. Pada contoh di atas, algoritma bisa diubah menjadi karakter+x, di mana x adlah variabel yang berlaku sebagai kunci. Kunci bisa bersifat dinamis, artinya kunci dapt berubah-ubah sesuai kesepatan untuk lebih meningkatkan keamanan pesan. Kunci harus diletakkan terpisah dari pesan yang terenkripsi dan dikirimkan secara rahasia. Teknik semacam ini disebut sebagai symmetric (single key) atau secret key cryptography. Selanjutnya akan muncul permasalahn kedua, yaitu bagaimana mengirim kunci tersebut agar kerahasiaannya terjamin. Karena jika kunci dapat diketahui oeleh seseorang maka orang tersebut dapat membongkar pesan yang kita kirim.

Untuk mengatasi permasalahan ini, sepasang ahli masalah keamanan bernama Whitfield Diffie dan Martin Hellman mengembangkan konseppublic-key cryptography. Skema ini, disebut juga sebagai asymmetric encryption, secara konsep sangat sederhana, tetapi bersifat revolusioner dalam cakupannya. Gambar 5.2 memperlihatkan mekanisme kerja dari metode ini.



Gambar 5.2 Public key cryptography.

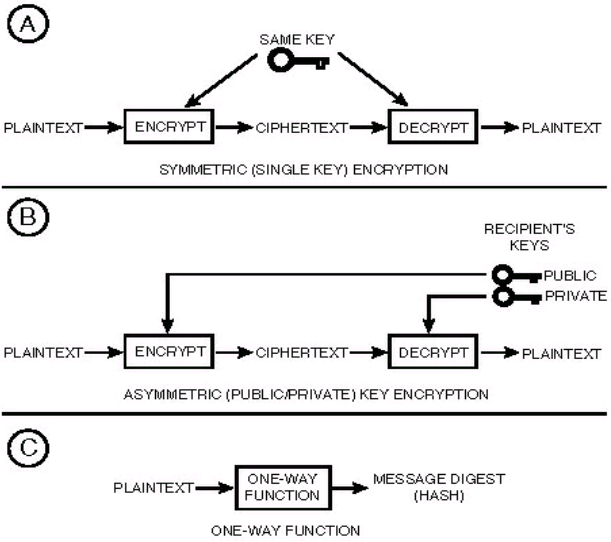
- Seperti terlihat pada gambar 6.2, masing-masing person mempunyai sepasang kunci, kunci privat dan kunci publik, yang secara matematis berasosiasi tetapi beda dalam fungsi.
- Dari dua kunci tersebut, sebuah disimpan secara pribadi (kunci privat) dan yang satunya dipublikasikan (kunci publik)

Kunci privat dijaga kerahasiaanya oleh pemiliknya atau diterbitkan pada server kunci publik apabila dihendaki. Apabila kita menginginkan untuk mengirimkan sebuah pesan terenkripsi, maka kunci publik dari penerima pesan harus diberitahukan untuk mengenkripsi pesan. Saat pesan tersebut sampai, maka penerima akan mendekripsi pesan dengan kunci privatnya. Jadi konsep sederhana yang diaplikasikan di sini adalah bahwa sebuah pesan hanya bisa didekripsi dengan sebuah kunci privat hanya apabila ia sebelumnya telah dienskripsi dengan kunci public dari pemilik kunci yang sama.

Enkripsi ini memiliki bersifat one-way function. Artinya proses enkripsi sangat mudah dilakukan, sedangkan proses dekripsi sangat sulit dilakukan apbila kunci tidak diketahui. Artinya untuk membuat suatu pesan terenkripsi hanya dibutuhkan waktu beberapa detik, sedangkan mencoba mendekripsi dengan segala kemungkinan membutuhkan waktu ratusan, tahuanan bahkan jutaan tahun meskipun menggunakan komuter yang handal sekalipun

Enkripsi one-way digunakan untuk bebearap kegunaan. Misalkan kita memliki dokumen yang akan dikirimkan kepada seseorang atau menyimpan untuk kita buka suatu saat, kita bisa menggunakan teknik one-way function yang akan menghasilkan nilai dengan panjang tertentu yang disebut hash.. Hash merupakan suatu signature yang unik dari suatu dokumen di mana kita bisa menaruh atau mengirimkan bersama dengan dokumen kita. Penerima pesan bisa menjalankan one-way function yang sama untuk menghasilkan hash yang lain. Selanjutnya hash tersebut saling dibanding. Apabila cocok, maka dokumen dapat dikembalikan ke bentuk aslinya.

Gambar 5.3 memperlihatkan tiga teknik utama kriptografi yaitu *symmetric cryptography*, *asymmetric cryptography*, dan *one-way functions.*



Gambar 5.3 Tiga teknik kriptografi

Tujuan Kriptografi

Tujuan dari sistem kriptografi adalah :

- Confidentiality : memberikan kerahasiaan pesan dan menyimpan data dengan menyembuyikan informasi lewat teknik-teknik enkripsi.
- Message Integrity : memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat ia dibuat samapai saat ia dibuka.
- Non-repudiation : memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang

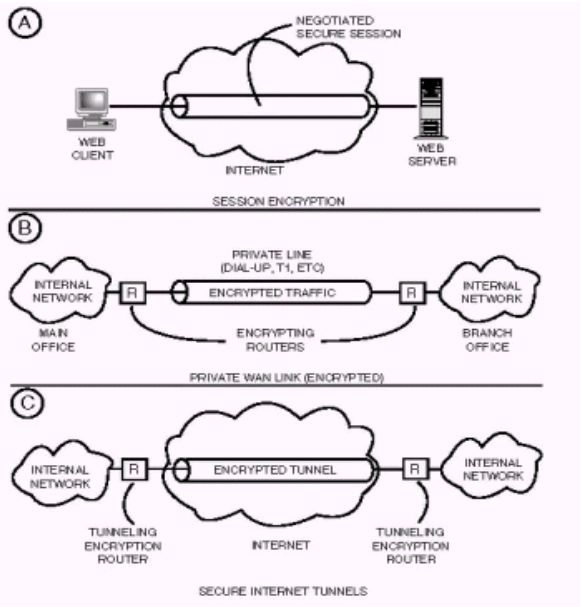
apabila ia mencoba menyangkal memiliki dokumen tersebut.

- Authentication : Memberikan dua layanan. Pertama mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikannya. Kedua untuk menguji identitas seseorang apabila ia kan memasuki sebuah sistem.

Dengan demikian menjadi jelas bahwa kriptografi dapat diterapkan dalam banyak bidang . Beberapa hal di antaranya :

- Certificates (Digital IDs) .
- Digital signatures.
- Secure channels.

Tiga contoh ini dapat dilihat pada gambar 5.4.



Gambar 5.4. Tiga tipe kanal aman yang dapat memberikan kerahasiaan data.

5.6 Referensi

1. Atkins, Derek,dan Paul Buis, Chris Hare, Robert Kelley, Carey Nachenberg, Anthony B. Nelson, Paul Phillips, Tim Ritchey, Tom Sheldom, Joel Snyder, *Internet Security Professional Reference*, Macmillan Computer Publishing,
2. Stallings, William, *Data and Computer Communications*, Macmillan,1985
3. Stallings, William, *Local Network*, Macmillan,1990
4. Stallings, William, *Data and Computer Communications*, Prentice Hall,1994
5. Halsall, Fred, Data Communications, *Computer Networks and Open System*, Addison-Wesley Pub.Co,1996

DAFTAR PUSTAKA

1. Tanenbaum, AS, *Computer Networks*, Prentise Hall, 1996
2. Stallings, W. *Data and Computer Communications*, Macmillan Publishing Company, 1985.
3. Stallings, W. *Local Network*, Macmillan Publishing Company, 1985.
4. Black, U.D, *Data Communications and Distributed Networks*, Prentise Hall.
5. Raj Jain, Professor of CIS The Ohio State University Columbus, OH 43210 Jain@ACM.Org http://www.cis.ohio-state.edu/~jain/cis677-98/
6. Cisco Press http://www.cicso.com/cpress/cc/td/cpress/fund/ith2nd/it2401.html
7. Atkins, Derek,dan Paul Buis, Chris Hare, Robert Kelley, Carey Nachenberg, Anthony B. Nelson, Paul Phillips, Tim Ritchey, Tom Sheldom, Joel Snyder, *Internet Security Professional Reference*, Macmillan Computer Publishing,