Dr. Agus Wibowo, M.Kom, M.Si, MM.

# Teknologi Jaringan Komputer

YAYASAN PRIMA AGUS TEKNIK

**TEKNOLOGI JARINGAN KOMPUTER**

**Penulis :**
Dr. Agus Wibowo, M.Kom, M.Si, MM.

**ISBN : 978-623-8642-14-4**

**Editor :**
Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

**Penyunting :**
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

**Desain Sampul dan Tata Letak :**
Irdha Yunianto, S.Ds., M.Kom.

**Penebit** :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

**Anggota IKAPI No:** 279 / ALB / JTE / 2023

**Redaksi :**
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

**Distributor Tunggal :**
**Universitas STEKOM**
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : info@stekom.ac.id

# KATA PENGANTAR

Puji Syukur kehadirat Tuhan Yang Maha Esa, atas berkat dan Rahmat-Nya, penulis dapat menyelesaiakan buku yang berjudul "***Teknologi Jaringan Komputer***", dengan baik dan maksimal. Buku ini dibuat untuk menambah wawasan pembaca dalam topik Jaringan pada Komputer. Jaringan komputer adalah suatu sistem yang terdiri dari beberapa perangkat komputer yang saling terhubung untuk berbagi sumber daya dan berkomunikasi dengan cara yang efektif dan efisien. Jaringan komputer dapat berupa jaringan lokal (LAN), jaringan wide area network (WAN), atau jaringan internet. Dalam jaringan komputer, setiap perangkat komputer disebut sebagai node, dan setiap node dapat berfungsi sebagai pengirim atau penerima data. Jaringan komputer menggunakan teknologi komunikasi data untuk mengirimkan data dari satu node ke node lainnya. Data yang dikirimkan dapat berupa teks, gambar, suara, atau video. Jaringan komputer juga menggunakan protokol komunikasi data untuk mengatur cara data dikirimkan dan diterima. Protokol ini memastikan bahwa data yang dikirimkan dapat diterima dengan benar dan tanpa kesalahan.

Dalam bab 1 buku ini membahas tentang konsep dasar jaringan komputer, tujuan utama pendirian jaringan, serta pentingnya jaringan komputer dalam konteks berbagi sumber daya, meningkatkan keandalan, menghemat biaya, dan meningkatkan kinerja sistem. Bacaan juga menjelaskan bahwa jaringan komputer dapat menggunakan berbagai teknologi transmisi seperti kabel, saluran telepon, gelombang radio, satelit, atau sinar inframerah. Selain itu, dibahas pula dua dimensi penting dalam mengklasifikasikan jaringan komputer, yaitu teknologi transmisi yang digunakan dan skala jaringan, baik itu jaringan lokal (LAN) maupun jaringan luas (WAN). Selanjutnya dalam bab ke 2 membahas konsep dasar tentang jaringan komputer yang terdiri dari tiga komponen utama: perangkat keras, protokol (perangkat lunak yang mengatur komunikasi), dan aplikasi (perangkat lunak yang berguna dalam jaringan). Konsep layer dalam jaringan juga dijelaskan, di mana setiap lapisan berfungsi sebagai antarmuka dan melindungi lapisan di atasnya, sehingga perubahan di satu lapisan tidak berdampak besar pada lapisan lainnya. Model OSI dengan tujuh lapisan menjadi dasar untuk memahami fungsi masing-masing lapisan dalam jaringan komputer. Selain itu, TCP/IP sebagai protokol utama dalam internet diuraikan, dimulai dari pengertiannya sebagai Transmisi Kontrol Protokol/Protokol Internet, hingga popularitasnya yang luas karena kemampuannya untuk menyediakan interoperabilitas komunikasi yang transparan di antara berbagai platform perangkat keras dan sistem operasi. Keunggulan TCP/IP yang membuatnya menjadi standar de facto dalam komunikasi global, termasuk dalam transfer file, email, dan layanan login jarak jauh, juga disoroti dalam bab ini. Dan Bab 3 buku ini membahas berbagai jenis media transmisi yang digunakan dalam jaringan komputer modern. Media tersebut termasuk kabel tembaga seperti twisted pair dan kabel koaksial, serta teknologi serat optik. Setiap jenis media memiliki karakteristik dan kegunaan yang berbeda, seperti twisted pair yang terbagi menjadi shielded (STP) dan unshielded (UTP), kabel koaksial dengan konduktor kawat tembaga berpelindung, dan serat optik yang mengirimkan data dalam bentuk cahaya melalui serat kaca untuk kecepatan dan keamanan yang tinggi. Pemilihan media transmisi yang sesuai penting untuk memastikan kinerja optimal dalam jaringan komputer.

Bab 4 membahas perkembangan media transmisi dalam komunikasi modern. Mulai dari evolusi dari kabel tembaga ke teknologi nirkabel dan serat optik yang lebih canggih, setiap jenis media menggantikan satu sama lain dengan cepat dalam era informasi. Diskusi mencakup penggunaan stasiun gelombang mikro sebagai pengganti kabel koaksial dalam PSTN, serta peran penting satelit dalam memperluas cakupan komunikasi jarak jauh meskipun dengan tantangan penundaan sinyal. Kabel serat optik kini menjadi pilihan utama untuk kecepatan dan kapasitas transfer data yang lebih tinggi. Bab 5 ini membahas berbagai perangkat penghubung dalam jaringan komputer. Hub digunakan untuk menghubungkan koneksi fisik, bridge untuk LAN pada lapisan data link, switch untuk koneksi point-to-point efisien, dan router untuk menghubungkan LAN yang berbeda dengan protokol perutean. Gateway melakukan konversi protokol antar jaringan yang berbeda di lapisan aplikasi OSI. Bab ini juga mencakup hub switching yang mendukung berbagai media transmisi, serta teknik switching seperti Circuit Switching, Packet Switching, Message Switching, dan Cell Switching untuk pengiriman data yang efektif dalam jaringan. Bab 6 ini menjelaskan konsep dasar dan teknik dalam transmisi data dan komunikasi. Sirkuit adalah jalur fisik atau nirkabel untuk mengirim sinyal antara titik-titik dalam jaringan, sementara sirkuit virtual adalah jalur logis dari berbagai jalur fisik yang tersedia. Multiplexing menggabungkan beberapa saluran untuk transmisi efisien: FDM berdasarkan frekuensi, TDM dengan alokasi slot waktu. Teknik CDM menggunakan kode acak, WDM mengirim banyak sinyal optik dengan panjang gelombang berbeda dalam satu serat, dan SDMA memanfaatkan antena parabola untuk komunikasi satelit.

Bab 7 buku ini akan membahas tentang lapisan data link dalam jaringan komputer, yang bertugas mengelola akses saluran komunikasi dan memastikan transmisi data yang handal. Fungsinya meliputi pembingkaian data, deteksi kesalahan dengan metode seperti pemeriksaan paritas, checksum, dan CRC, serta kontrol aliran data. Lapisan ini menyediakan layanan tanpa koneksi yang tidak diakui, tanpa koneksi yang diakui, dan berorientasi koneksi yang diakui untuk keperluan komunikasi data. Selanjutnya bab ke 8 mengulas berbagai protokol efisiensi transmisi data seperti Stop and Wait, Go Back N, dan Selective Repeat dalam lapisan data link. Protokol ini menawarkan pendekatan yang berbeda terhadap manajemen bandwidth dan pengulangan frame. Selain itu, bab ini juga menjelaskan penggunaan teknologi nirkabel seperti Bluetooth untuk memfasilitasi konektivitas tanpa kabel antar perangkat, memungkinkan berbagi sumber daya seperti Internet broadband, printer, dan media digital secara efisien dalam jaringan area pribadi (PAN). Dan bab ke 9 mengulas peran lapisan jaringan dalam mengirimkan paket data melalui router. Lapisan ini menyediakan layanan independen terhadap teknologi router dan menjaga konsistensi pengalamatan jaringan. Bab juga membahas layanan jaringan berorientasi koneksi dan tanpa koneksi, serta berbagai algoritma perutean seperti Link State Routing dan algoritma vektor jarak. Hal ini membantu router dalam menentukan jalur terpendek ke tujuan dalam jaringan dengan efisien.

Bab 10 ini membahas tentang alamat IPv4 sebagai pengidentifikasi unik pada lapisan jaringan, yang digunakan untuk menandai sumber dan tujuan paket IP. Namun, karena keterbatasan jumlah alamat IPv4 yang tersedia, telah diperkenalkan versi IPv6 yang menggunakan alamat 128-bit. Selain itu, bab juga mengulas tentang kemacetan dalam jaringan yang terjadi ketika jumlah paket melebihi kapasitas subnet, serta perbedaan antara pengendalian kemacetan dan pengendalian aliran. Teori kendali jaringan, seperti loop terbuka dan loop tertutup, juga dibahas dalam konteks manajemen lalu lintas untuk memaksimalkan

efisiensi penggunaan sumber daya jaringan. Terakhir, algoritma leaky bucket dijelaskan sebagai metode untuk mengatur laju pembentukan lalu lintas dalam jaringan. Selanjutnya dalam bab 11 ini akan membahas membahas peran dan fungsi lapisan transport dalam model referensi OSI, yang menyediakan transfer data antara mesin sumber dan tujuan dengan menggunakan layanan jaringan seperti IP di bawahnya. Lapisan transport menawarkan komunikasi "peer to peer" dengan kontrol ujung ke ujung dan pemeriksaan kesalahan untuk memastikan pertukaran data yang lengkap. Selain itu, bab ini menyoroti kontrol aliran untuk mengatur transmisi data antar perangkat, multiplexing untuk menggabungkan data dari beberapa aplikasi ke satu tautan fisik, dan sirkuit virtual yang dikelola oleh lapisan transport. Protokol transport utama, TCP dan UDP, dibahas sebagai solusi untuk transmisi data yang andal dan tanpa koneksi dalam konteks jaringan TCP/IP.

Dalam bab 12 ini menguraikan berbagai aplikasi dan protokol yang beroperasi di lapisan aplikasi dalam model TCP/IP. Ini mencakup penggunaan antarmuka Socket untuk mengakses sumber daya jaringan, konsep aplikasi yang terbagi menjadi server dan klien, serta peran DNS dalam menerjemahkan alamat IP. Selain itu, pembahasan juga mencakup surat elektronik, aplikasi multimedia yang mengintegrasikan teks, gambar, video, dan suara, serta protokol seperti SMTP untuk mentransfer email dan HTTP untuk mentransfer halaman web. Penerapan multimedia di semua sektor masyarakat menunjukkan kontribusi besar terhadap evolusi Internet dan World Wide Web. Selanjutnya bab 13 ini akan membahas lapisan sesi dan presentasi dalam model OSI. Lapisan sesi bertanggung jawab untuk mengelola pembuatan, pengaturan, dan penghentian sesi komunikasi antara aplikasi di mesin sumber dan tujuan. Ini memfasilitasi dialog antara proses aplikasi, baik dalam mode duplex maupun half-duplex, dan menyediakan mekanisme seperti check-pointing dan penundaan untuk pengelolaan kesalahan dan restart. Dan bab 14 yang merupakan bab terakhir dalam buku ini akan membahas pentingnya keamanan data dalam jaringan komputer. Data harus dilindungi dari akses tidak sah dan intervensi yang dapat mengancam keutuhan dan kerahasiaannya. Ancaman termasuk serangan terhadap server, pencurian informasi pribadi, dan upaya sabotase terhadap infrastruktur organisasi melalui jaringan. Keamanan data melibatkan langkah-langkah seperti enkripsi untuk memastikan kerahasiaan pesan, otentikasi untuk memverifikasi identitas pengguna yang meminta layanan, dan integritas untuk memastikan bahwa pesan tidak diubah dalam perjalanan. Implementasi teknik enkripsi dan dekripsi di kedua ujung komunikasi adalah kunci untuk menjaga privasi data, dengan menggunakan kunci rahasia dan teknik kunci publik sebagai metode perlindungan.

Demikian akhir buku ini, harapan penulis supaya buku ini mejadi manfaat bagi para mahasiswa maupun Masyarakat umum, dan sebagai sumber ilmu dalam konteks jaringan komputer. Terima Kasih.

Semarang, Juni 2024
Penulis

Dr. Agus Wibowo, M.Kom, M.Si, MM

# DAFTAR ISI

# BAB 1
# PENGANTAR JARINGAN KOMPUTER

## 1.1 SEJARAH JARINGAN KOMPUTER

Berikut adalah sejarah singkat tonggak sejarah komputer, jaringan dan telekomunikasi:

- 1897: CRT (Cathode Ray Tube) dikreditkan ke Braun
- 1900–1915: Teletype (telegraf 5 bit)
- 1915–1020: ARQ (Permintaan Pengulangan Otomatis) dikreditkan ke Van Duuren
- 1930–1940: ENIAC dikreditkan ke DOD/MIT
- 1950an: SAGE (Lingkungan Tanah Semi-Otomatis) MIT 1950an
- 1960-an: Komputer Transistorisasi – Generasi ke-2
- 1961: CTSS (Sistem Pembagian Waktu yang Kompatibel) dikreditkan ke Cobato/MIT
- 1965: Teknik Penyetaraan Otomatis saluran telepon dikreditkan ke Lucky dkk.
- 1966: Fiber Glass dikreditkan ke Kao & Hockman
- 1967: Komputer Sirkuit Terpadu – Generasi ke-3
- 1968: Keputusan Carterfone–FCC di
- 1969: Sekelompok peneliti Departemen Pertahanan menghubungkan empat komputer di UCLA, SRI, Universitas Utah dan UCSB. Mereka menciptakan jaringan untuk berkomunikasi satu sama lain tentang proyek-proyek pemerintah. Jaringan tersebut merupakan bagian dari Badan Proyek Penelitian Lanjutan Departemen Pertahanan, dan dijuluki ARPAnet.
- 1972: Lebih dari 50 universitas dan lembaga militer terhubung dalam jaringan ini. Untuk jangka waktu singkat, ini adalah proyek pertahanan rahasia yang memastikan bahwa komputer dapat berkomunikasi satu sama lain jika terjadi serangan nuklir. Sistem komunikasi antar situs disebut email dan ditemukan oleh Ray Tomlinson dari Bolt, Berrank dan Newman.
- 1973: Hubungan proyek pertahanan diperluas ke Norwegia dan Inggris.
- 1974: Protokol Kendali Transmisi (TCP) diterbitkan dan hubungan militer dan pendidikan menjadi berbeda. Organisasi seperti NASA mulai bereksperimen dengan jaringan komputer, dan jaringan tersebut mulai saling berhubungan dan nama Internet diciptakan.
- 1976: Ratu mengirimkan email dari RSRE Malvern.
- 1983: TCP/IP menjadi standar protokol untuk ARPAnet. Scott Fahlman menciptakan smiley untuk menyampaikan emosi melalui email.
- 1984: Di AS, NSF membangun jalur berkecepatan tinggi dan jarak jauh yang menghubungkan situs superkomputer di seluruh AS. Ini akhirnya menggantikan ARPAnet asli. Belakangan, NSFnet bergabung dengan jaringan lain di puluhan universitas, laboratorium penelitian, dan perusahaan teknologi tinggi. Sistem untuk menetapkan nama ke komputer di jaringan diperkenalkan —DNS. JANet diluncurkan untuk menghubungkan Universitas-universitas Inggris.

- 1986: NSF membangun jaringannya sendiri yang lebih cepat, NSFnet dan Network News Transfer Protocol (NNTP) diperkenalkan sehingga diskusi interaktif online menjadi kenyataan. Kecepatan tulang punggung adalah 56 Kbps.
- 1987: RFC ke-1000 dan host ke-10.000.
- 1988: Robert Tappan Morris merilis Internet Worm pertama dan CERT didirikan untuk menanggapi hal ini. Kecepatan tulang punggung ditingkatkan menjadi 1,544 Mbps. IRC dikembangkan.
- 1989: tuan rumah ke-100.000. Cuckoo's Egg yang dirilis oleh Cliff Stoll menceritakan kisah nyata cracker Jerman Timur yang mengakses instalasi AS.
- 1990: ARPAnet tidak ada lagi dan Internet secara efektif mengambil perannya.
- 1991: Gopher, sebuah program perangkat lunak untuk mengambil informasi dari server di Internet disediakan oleh University of Minnesota. Pemerintah AS mengumumkan bahwa mereka tidak lagi bermaksud membatasi aktivitas di Internet untuk penelitian. Pergeseran kebijakan ini cukup bagi 12 perusahaan untuk bekerja sama dan memproduksi CIX. Phil Zimmerman merilis PGP. Kecepatan backbone ditingkatkan menjadi 44.736 Mbps.
- 1992: World Wide Web menjadi sebuah kemungkinan setelah CERN, di Swiss, merilis hypertext. Tuan Rumah ke-1.000.000. Penulis mendapatkan akun email dialup pertamanya dengan Demon Internet (November 1992).
- 1993: Mosaik, sebuah program perangkat lunak untuk menelusuri situs Web yang ditulis oleh Marc Andreesen, dirilis diikuti oleh Netscape.
- 1994: Pusat Perbelanjaan hadir di Internet. Departemen Keuangan Inggris mulai beroperasi dan bank siber pertama dibuka. Iklan spanduk pertama muncul untuk Zima (minuman) dan AT&T.
- 1995: Layanan dialup tradisional (AOL, CompuServe dll) mulai menyediakan layanan dialup. Vatikan sedang online. Sejumlah perusahaan Internet go public. Netscape memimpin dengan IPO terbesar yang pernah ada di NASDAQ. DEC meluncurkan AltaVista, yang mengklaim mengindeks setiap halaman HTML yang ada. Jeff Bezos meluncurkan Amazon.com. eBay diluncurkan.
- 1996: 9.272 organisasi tidak terdaftar setelah InterNIC menghentikan layanan nama mereka karena tidak membayar biaya nama domain. Berbagai ISP mengalami pemadaman layanan yang berkepanjangan, sehingga menimbulkan pertanyaan apakah mereka mampu menangani jumlah pengguna yang terus bertambah. AOL (19 jam), Netcom (13 jam), AT&T WorldNet (28 jam - hanya email). Tiongkok mewajibkan pengguna Internet untuk mendaftar ke Polisi. Arab Saudi membatasi penggunaan untuk universitas dan rumah sakit. Nama domain tv.com dijual ke CNET seharga US$15.000. Kecepatan tulang punggung ditingkatkan menjadi 622 Mbps.
- 1997: RFC ke-2000. 16 Juta host. Nama domain ke-1.000.000 terdaftar (6 Maret untuk Perusahaan Furnitur Bonny View Cottage).

- 1998: Nama domain ke-3.000.000 terdaftar. Otoritas Pos AS mengizinkan pembelian prangko secara online untuk diunduh dan dicetak. Standar Gigabit Ethernet diratifikasi. Google diluncurkan.
- 1999: Bank layanan penuh pertama dibuka di Internet (First Internet Bank of Indiana). Halaman web palsu pertama, mirip Bloomberg, meningkatkan saham sebuah perusahaan kecil sebesar 31% (7 April). Melissa menyerang. Nama domain ke 5.000.000 terdaftar. Perang Cyber pertama dimulai antara Serbia dan Kosovo. Shawn Fanning Meluncurkan Napster — label rekaman sangat marah.
- 2000: Nama domain ke-10.000.000 terdaftar. Pengadilan Perancis mewajibkan memorabilia 'kebencian' yang dijual di situs lelang Yahoo harus dihapus. Gnutella diluncurkan. ICANN memilih domain tingkat atas yang baru. Tulang punggung ditingkatkan ke IPv6.
- 2001: Meneruskan email menjadi ilegal di Australia (Digital Agenda Act). Napster terpaksa menghentikan layanan setelah tindakan hukum. Taliban melarang Internet di Afghanistan. Nimda dirilis di Internet.
- 2002: Serangan penolakan Layanan terdistribusi menyerang 13 server root DNS, menyebabkan masalah keamanan nasional.
- 2003: Pemilu online resmi Swiss yang pertama berlangsung di Anières (7 Jan), SQL Slammer (berkeliling dunia dalam 10 menit dan mematikan 3 dari 13 Server DNS). Diikuti oleh SoBig.F (19 Agustus) dan Blaster (11 Agustus).
- 2004: Lycos Europe merilis screen saver untuk membantu melawan spam dengan membuat server spam sibuk dengan permintaan (1 Des). Layanan dihentikan dalam beberapa hari setelah penyedia backbone memblokir akses ke situs pengunduhan dan layanan menyebabkan beberapa server mogok.

## 1.2 MENDEFINISIKAN JARINGAN

Jaringan terdiri dari dua atau lebih komputer yang dihubungkan untuk berbagi sumber daya (seperti printer dan CD-ROM), bertukar file atau memungkinkan komunikasi elektronik. Komputer-komputer dalam suatu jaringan dapat dihubungkan melalui kabel, saluran telepon, gelombang radio, satelit, atau sinar inframerah.

Istilah 'jaringan komputer' berarti kumpulan komputer otonom yang saling berhubungan.

(a) Dua komputer dikatakan saling berhubungan apabila mampu saling bertukar informasi.

(b) Persyaratan agar komputer menjadi otonom tidak termasuk dalam sistem definisi kami yang memiliki hubungan master/slave yang jelas.

Perbedaan utama antara jaringan komputer dan sistem terdistribusi:

- Dalam sistem terdistribusi, keberadaan beberapa komputer otonom bersifat transparan bagi pengguna. Sistem terdistribusi tampak seperti prosesor virtual bagi penggunanya.
- Dengan jaringan, pengguna harus secara eksplisit melakukan hal berikut:
  - masuk ke satu mesin (mis., rlogin),

- ♦ mengirimkan pekerjaan dari jarak jauh (mis., rsh),
- ♦ memindahkan file (misalnya, rcp, ftp, uucp), dan
- ♦ umumnya menangani semua manajemen jaringan secara pribadi.

Faktanya, sistem terdistribusi adalah kasus khusus dari sebuah jaringan, yang perangkat lunaknya memberikan tingkat keterpaduan dan transparansi yang tinggi.

## 1.3 KARAKTERISTIK JARINGAN KOMPUTER

Tujuan utama jaringan komputer adalah untuk berbagi sumber daya:

(a) Anda dapat memutar CD musik dari satu komputer sambil duduk di komputer lain.

(b) Anda mungkin memiliki komputer dengan penulis CD atau sistem cadangan namun komputer lain tidak memilikinya; Dalam hal ini, Anda dapat membakar CD atau membuat cadangan pada komputer yang memiliki salah satu dari ini namun menggunakan data dari komputer yang tidak memiliki penulis CD atau sistem cadangan.

(c) Anda mungkin memiliki komputer yang tidak memiliki pemutar DVD. Dalam hal ini, Anda dapat menempatkan DVD film di komputer yang memiliki pemutar DVD, lalu menonton film tersebut di komputer yang tidak memiliki pemutar DVD.

(d) Anda dapat menghubungkan printer (atau pemindai atau mesin faks) ke satu komputer dan membiarkan komputer lain dalam jaringan mencetak (atau memindai, atau memfaks) ke printer (atau pemindai, atau mesin faks) tersebut.

(e) Anda dapat menempatkan CD berisi gambar di satu komputer dan membiarkan komputer lain mengakses gambar tersebut.

Anda dapat membuat file dan menyimpannya di satu komputer, lalu mengakses file tersebut dari komputer lain yang terhubung dengannya.

## 1.4 TUJUAN JARINGAN

(a) Tujuan utama jaringan adalah berbagi Sumber Daya, dan membuat semua program, data, dan peralatan tersedia bagi siapa pun di jaringan tanpa memperhatikan lokasi fisik sumber daya dan pengguna.

(b) Tujuan kedua adalah memberikan keandalan yang tinggi dengan memiliki sumber pasokan alternatif. Misalnya, semua file bisa direplikasi pada dua atau tiga mesin, jadi jika salah satu dari mereka tidak tersedia, salinan lainnya bisa tersedia.

(c) Tujuan lainnya adalah menghemat uang. Komputer kecil memiliki rasio harga/kinerja yang jauh lebih baik daripada komputer besar. Mainframe kira-kira sepuluh kali lebih cepat daripada mikroprosesor chip tunggal tercepat, tetapi harganya ribuan kali lebih mahal. Ketidakseimbangan ini menyebabkan banyak perancang sistem membangun sistem yang terdiri dari komputer pribadi yang kuat, satu komputer per pengguna, dengan data disimpan di satu atau lebih mesin server file bersama. Tujuan ini mengarah pada jaringan dengan banyak komputer yang terletak di gedung yang sama. Jaringan seperti ini disebut LAN *(local area network).*

(d) Tujuan lain yang terkait erat adalah untuk meningkatkan kinerja sistem seiring dengan meningkatnya beban kerja hanya dengan menambahkan lebih banyak prosesor. Dengan mainframe pusat, ketika sistem sudah penuh, maka harus diganti dengan yang lebih besar, biasanya dengan biaya yang besar dan dengan gangguan yang lebih besar lagi bagi pengguna.

(e) Jaringan komputer menyediakan media komunikasi yang kuat. File yang telah diperbarui/dimodifikasi di suatu jaringan dapat langsung dilihat oleh pengguna lain di jaringan.

## 1.5 PERANGKAT KERAS JARINGAN

Ada dua dimensi penting untuk mengklasifikasikan jaringan teknologi transmisi dan skala. Teknologi transmisi dapat diklasifikasikan menjadi dua jenis:

1. Jaringan penyiaran.
2. Jaringan titik-ke-titik.

(a) Jaringan penyiaran: Jaringan ini mempunyai saluran komunikasi tunggal yang digunakan bersama oleh semua mesin di jaringan. Mereka bekerja sebagai berikut:

- ✓ Semua yang lain menerima paket yang dikirim oleh mesin mana pun.
- ✓ Bidang alamat di dalam paket menentukan untuk siapa paket tersebut dituju.
- ✓ Setelah menerima paket, mesin memeriksa kolom alamat. Jika ditujukan untuk dirinya sendiri, ia akan memproses paket tersebut; jika tidak, itu diabaikan saja.

Hal ini juga memungkinkan untuk mengatasi semua penyiaran atau multicasting pada subset mesin. Skema umum:

i. Alamat yang terdiri dari 1 bit seluruhnya dicadangkan untuk siaran.
ii. Semua alamat dengan bit orde tinggi yang disetel ke 1 dicadangkan untuk multicasting.
iii. Bit alamat yang tersisa membentuk peta bit yang sesuai dengan kelompoknya.
iv. Setiap mesin dapat berlangganan ke salah satu atau semua grup.

Jaringan point-to-point terdiri dari banyak koneksi antara sepasang mesin individual. Beberapa rute dan mesin perantara mungkin ada di antara sepasang mesin; jadi algoritma perutean memainkan peran penting di sini. Kriteria alternatif untuk mengklasifikasikan jaringan adalah skalanya, yaitu sebagai berikut:

**Jaringan Area Lokal (LAN)**

Tiga karakteristik yang dapat dibedakan untuk LAN:

(a) Ukuran: biasanya berdiameter tidak lebih dari beberapa kilometer, dengan waktu transmisi kasus terburuk yang diketahui dan terbatas, memungkinkan desain khusus dan pengelolaan sederhana.

(b) Teknologi transmisi: biasanya kabel bersama berjalan pada kecepatan 10 hingga 100 Mbps (dan bahkan lebih tinggi), dengan penundaan puluhan mikrodetik dan sedikit kesalahan.

(c) Alokasi saluran bersama:

- Setiap mesin secara statis diberi slot waktu untuk melakukan transmisi, dan mendapat gilirannya secara round robin.
- Setiap mesin secara dinamis dialokasikan slot waktu sesuai permintaan.
- Metode terpusat menggunakan unit arbitrase untuk menentukan siapa yang selanjutnya.
- Metode terdesentralisasi memungkinkan setiap mesin untuk memutuskan sendiri.

**Jaringan Area Metropolitan (MAN)**

MAN adalah versi LAN yang lebih besar dan menggunakan teknologi serupa. Ia menggunakan satu atau dua kabel tetapi tidak mengandung elemen switching. Ini mencakup seluruh kota dan mungkin terkait dengan jaringan TV kabel lokal.

Standar MAN - DQDB (Bus Ganda Antrean Terdistribusi) IEEE 802.6.

(a) Dua bus searah.
(b) Setiap bus mempunyai head-end, yang memulai aktivitas transmisi.
(c) Lalu lintas ke kanan menggunakan bus atas.
(d) Lalu lintas ke kiri menggunakan bus bawah.

**Jaringan Area Luas (WAN)**

WAN mencakup wilayah yang luas, seringkali suatu negara atau benua. WAN terdiri dari dua bagian:

(a) Bagian aplikasi: Mesin untuk menjalankan program pengguna disebut host.
(b) Bagian komunikasi: Host-host dihubungkan oleh subnet komunikasi, atau hanya subnet, yang tugasnya membawa pesan dari host ke host.

Subnet terdiri dari dua komponen:

- Jalur transmisi (sirkuit, saluran, atau saluran utama) memindahkan bit antar mesin.
- Elemen switching (router) adalah komputer khusus yang digunakan untuk menghubungkan dua atau lebih jalur transmisi.

**Karakter utama**

i. WAN berisi banyak kabel atau saluran telepon, masing-masing menghubungkan sepasang router.
ii. (ii) Bagi mereka yang tidak memiliki koneksi langsung, komunikasi terjadi secara tidak langsung melalui router lain.
iii. (iii) Ketika sebuah pesan (paket) dikirim dari satu router ke router lainnya, pesan tersebut diterima di setiap router perantara secara keseluruhan, disimpan di sana hingga jalur keluaran yang diperlukan bebas, dan kemudian diteruskan.

WAN juga dapat menggunakan saluran siaran, seperti satelit atau sistem radio darat.

**Jaringan Nirkabel**

Komputer seluler, seperti komputer notebook dan Personal Digital Assistants (PDS), adalah segmen industri komputer yang tumbuh paling cepat.

Aplikasi yang menggunakan jaringan nirkabel:

(a) Kantor portabel yang memungkinkan orang mengirim dan menerima panggilan telepon, faks dan email, membaca file jarak jauh atau masuk ke mesin jarak jauh, dll., dan melakukannya dari darat, laut atau udara.

(b) Bermanfaat besar bagi armada truk, taksi, dan petugas reparasi karena tetap berhubungan dengan rumah.
(c) Penting untuk menyelamatkan pekerja di lokasi bencana dan militer.

**Internetwork**

Kumpulan jaringan yang saling berhubungan disebut internetwork atau hanya Internet. Internet mengacu pada Internet spesifik di seluruh dunia yang banyak digunakan untuk menghubungkan universitas, kantor pemerintah, perusahaan, dan individu swasta.

## 1.6 KEGUNAAN JARINGAN KOMPUTER

Ada banyak kegunaan jaringan komputer. Tergantung pada jaringan pengguna, ia memiliki kegunaan berikut.

**Jaringan untuk Perusahaan**

(a) Berbagi Sumber Daya: Jaringan diperlukan karena keinginan untuk membuat semua program, data, dan peralatan tersedia bagi siapa pun di jaringan tanpa memperhatikan lokasi fisik sumber daya dan pengguna. Pembagian beban adalah aspek lain dari pembagian sumber daya.
(b) Keandalan Tinggi: Suatu jaringan mungkin memiliki sumber pasokan alternatif (misalnya, file yang direplikasi, banyak CPU, dll.). Jika terjadi kegagalan satu sumber daya, sumber daya lainnya dapat digunakan dan sistem terus beroperasi dengan kinerja yang berkurang. Ini adalah properti yang sangat penting untuk militer, perbankan, pengatur lalu lintas udara dan banyak aplikasi lainnya.
(c) Menghemat Uang: Sebuah jaringan dapat terdiri dari banyak komputer kecil yang kuat, satu per pengguna, dengan data disimpan pada satu atau lebih mesin server file bersama, yang menawarkan rasio harga/kinerja yang jauh lebih baik daripada mainframe.
(d) Skalabilitas: Kemampuan untuk meningkatkan kinerja sistem secara bertahap dengan menambahkan lebih banyak prosesor (peningkatan tambahan).
(e) Media Komunikasi yang Kuat: Jaringan membuat kerjasama antar kelompok masyarakat yang berjauhan menjadi mudah, hal yang sebelumnya tidak mungkin dilakukan.

Dalam jangka panjang, penggunaan jaringan untuk meningkatkan komunikasi antar manusia mungkin terbukti lebih penting daripada tujuan teknis seperti peningkatan keandalan.

CSCW (Pekerjaan Koperasi yang Didukung Komputer) adalah bidang multidisiplin yang berkembang pesat berdasarkan jaringan komunikasi.

**Jaringan untuk Manusia**

Mulai tahun 1990-an, jaringan komputer mulai memberikan layanan kepada individu di rumah.

**Akses ke Informasi Jarak Jauh**

(a) Reservasi rumah untuk pesawat, kereta api, hotel, restoran, teater dan sebagainya, dimanapun di dunia dengan konfirmasi instan.
(b) Perbankan rumah dan belanja.

(c) Surat kabar, jurnal, dan perpustakaan elektronik on-line dan terpersonalisasi.
(d) Akses ke WWW (*World Wide Web*) yang berisi informasi tentang banyak topik – terlalu banyak untuk disebutkan!

Semua aplikasi ini melibatkan interaksi antara seseorang dan database jarak jauh.
Komunikasi antar orang: Jawaban abad ke-21 terhadap telepon abad ke-19.

- Surat elektronik atau email untuk semua orang. Email mungkin berisi suara digital, gambar, gambar TV dan video bergerak (dan bahkan berbau!).
- Grup berita di seluruh dunia untuk masyarakat luas, dan meliput semua topik yang ada.
- Sistem CSCW real-time, seperti konferensi video dan lingkungan pertemuan virtual, memungkinkan pengguna jarak jauh berkomunikasi tanpa penundaan, dan mungkin juga saling melihat dan mendengar.

Ada kalanya dikatakan bahwa transportasi dan komunikasi sedang berlomba, dan siapa pun yang menang akan membuat yang lain ketinggalan zaman.
Hiburan interaktif adalah industri yang besar dan berkembang.

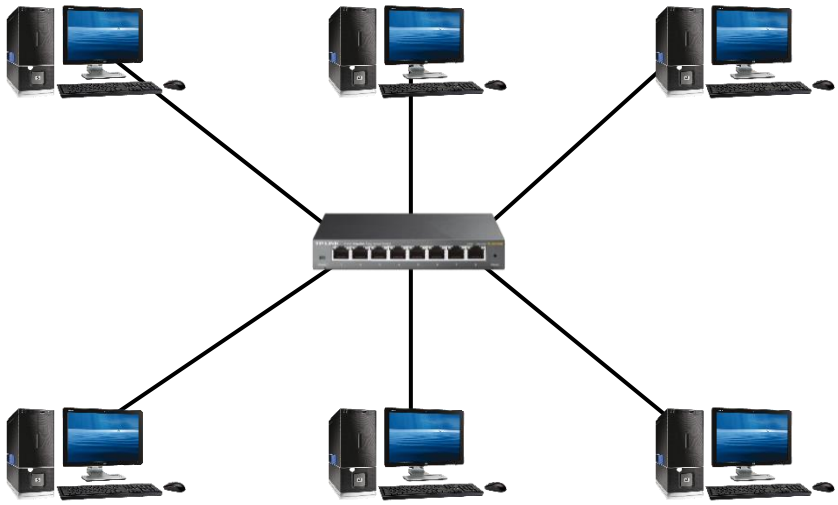
i. Video on demand (aplikasi pembunuh): Pengguna dapat memilih film atau program TV apa pun yang pernah dibuat, di negara mana pun, dan langsung menampilkannya di layar.
ii. Film interaktif: Pengguna dapat memilih skenario alternatif untuk arah cerita.
iii. TV langsung dan interaktif: Penonton dapat berpartisipasi dalam acara kuis dan sebagainya.
iv. Game real-time multi-orang (mungkin aplikasi pembunuh alternatif): Petak umpet, simulator penerbangan, dll.

Jika dilakukan dengan kacamata dan gambar bergerak berkualitas fotografi real-time 3 dimensi, kita memiliki semacam realitas virtual bersama di seluruh dunia. Kemampuan menggabungkan informasi, komunikasi dan hiburan tentunya akan melahirkan industri baru yang masif berbasis jaringan komputer. Revolusi informasi dapat mengubah masyarakat seperti halnya Revolusi Industri.

## 1.7 TOPOLOGI JARINGAN

Topologi jaringan adalah desain dasar jaringan komputer. Ini sangat mirip dengan peta jalan. Ini merinci bagaimana komponen jaringan utama seperti node dan link saling berhubungan. Topologi jaringan sebanding dengan cetak biru rumah baru di mana komponen seperti sistem kelistrikan, sistem pemanas dan pendingin udara, serta pipa ledeng diintegrasikan ke dalam desain keseluruhan. Diambil dari karya Yunani “Topos” yang berarti “Tempat,” Topologi, dalam kaitannya dengan jaringan, menggambarkan konfigurasi jaringan; termasuk lokasi stasiun kerja dan sambungan kabel. Pada dasarnya ini memberikan definisi komponen-komponen Jaringan Area Lokal (LAN). Topologi, yang merupakan pola interkoneksi antar node, mempengaruhi biaya dan kinerja jaringan. Ada tiga tipe utama topologi jaringan yang mengacu pada tata letak fisik dan logis dari pengkabelan Jaringan. Mereka:

1. **Topologi Star**: Semua perangkat yang terhubung dengan pengaturan Star berkomunikasi melalui Hub pusat melalui segmen kabel. Sinyal dikirim dan diterima melalui Hub. Ini adalah yang paling sederhana dan tertua dan semua saklar telepon didasarkan pada ini. Dalam topologi star, setiap perangkat jaringan memiliki rangkaian kabel kembali ke hub jaringan, sehingga setiap perangkat memiliki koneksi terpisah ke jaringan. Jadi, bisa ada banyak koneksi secara paralel.



**Gambar 1.1 Topologi Star**

**Keuntungan**

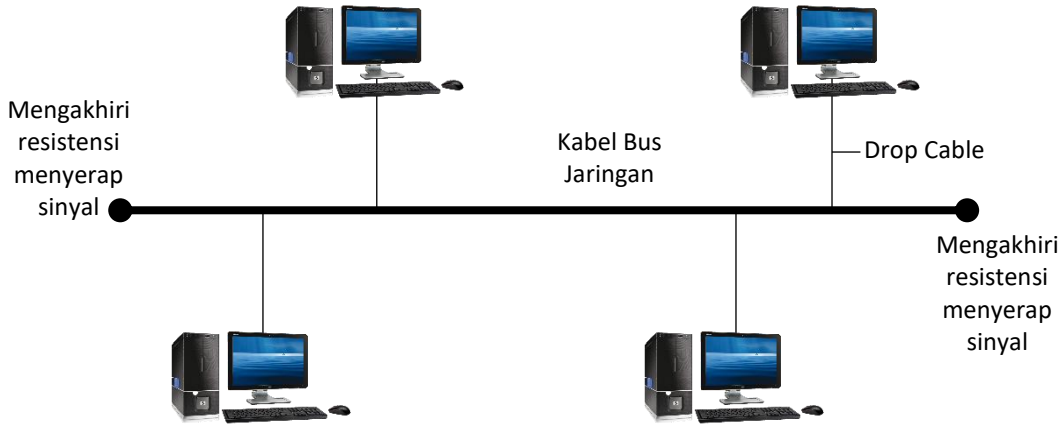
- ✓ Administrasi jaringan dan deteksi kesalahan lebih mudah karena masalah diisolasi ke node pusat.
- ✓ Jaringan berjalan bahkan jika satu host gagal.
- ✓ Ekspansi menjadi lebih mudah dan skalabilitas jaringan meningkat.
- ✓ Lebih cocok untuk jaringan yang lebih besar.

**Kekurangan**

- Penyiaran dan multicasting tidaklah mudah karena beberapa fungsi tambahan perlu disediakan ke hub pusat.
- Jika node pusat gagal, seluruh jaringan akan mati; sehingga membuat peralihan tersebut menjadi semacam hambatan.
- Biaya instalasi tinggi karena setiap node harus terhubung ke saklar pusat.

2. **Topologi Bus**: Topologi paling sederhana dan paling umum dari semua topologi, Bus terdiri dari satu kabel, yang disebut Backbone yang menghubungkan semua workstation di jaringan menggunakan satu jalur. Semua transmisi harus melewati setiap perangkat yang terhubung untuk menyelesaikan permintaan yang diinginkan. Setiap stasiun kerja memiliki sinyal tersendiri yang mengidentifikasinya dan memungkinkan data yang diminta dikembalikan ke pembuatnya yang benar. Di Jaringan Bus, pesan dikirim dua arah dari satu titik dan dibaca oleh node (komputer atau periferal di jaringan) yang diidentifikasi oleh kode dengan pesan tersebut.

Kebanyakan Jaringan Area Lokal (LAN) adalah Jaringan Bus karena jaringan akan terus berfungsi meskipun satu komputer mati. Topologi ini bekerja dengan baik baik untuk peer to peer atau client server.




**Gambar 1.2 Topologi Bus**

Tujuan dari terminator di kedua ujung jaringan adalah untuk menghentikan sinyal dipantulkan kembali.

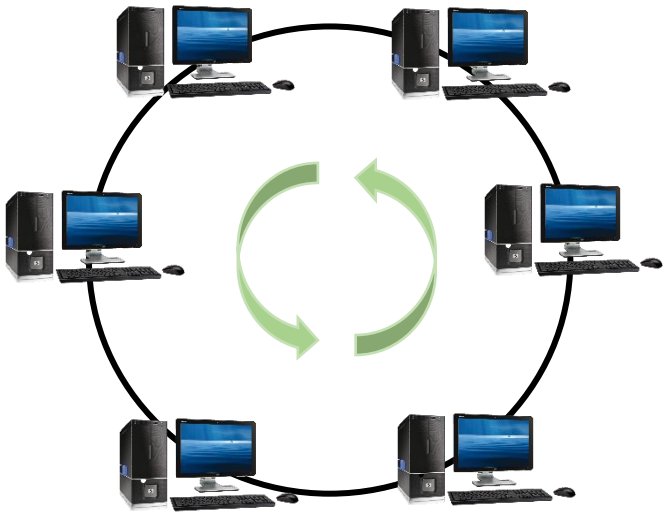
**Keuntungan**

- Penyiaran dan multicasting jauh lebih sederhana.
- Jaringan bersifat redundant dalam arti kegagalan satu node tidak mempengaruhi jaringan.
- Bagian lainnya mungkin masih berfungsi dengan baik.
- Paling murah karena jumlah kabel yang diperlukan lebih sedikit dan tidak diperlukan switch jaringan.
- Baik untuk jaringan kecil yang tidak memerlukan kecepatan lebih tinggi.

**Kekurangan**

- Pemecahan masalah dan deteksi kesalahan menjadi masalah karena, secara logika, semua node adalah sama.
- Kurang aman karena mengendus lebih mudah.
- Terbatas dalam ukuran dan kecepatan.

3. **Topologi Ring:** Semua node dalam Jaringan Ring terhubung dalam kabel lingkaran tertutup. Pesan yang dikirimkan berjalan mengelilingi ring hingga mencapai komputer yang dituju, sinyal disegarkan oleh setiap node. Dalam topologi ring, sinyal jaringan dilewatkan melalui setiap kartu jaringan dari setiap perangkat dan diteruskan ke perangkat berikutnya. Setiap perangkat memproses dan mentransmisikan ulang sinyal, sehingga mampu mendukung banyak perangkat dengan cara yang agak lambat namun sangat teratur. Ada fitur yang sangat bagus dimana setiap orang mendapat kesempatan untuk mengirim paket dan dijamin setiap node dapat mengirim paket dalam waktu yang terbatas.



**Gambar 1.3 Topologi Ring**

**Keuntungan**

- Penyiaran dan multicasting mudah karena Anda hanya perlu mengirimkan satu pesan.
- Lebih murah karena diperlukan lebih sedikit rekaman kabel.
- Dijamin bahwa setiap host akan mampu melakukan transmisi dalam interval waktu yang terbatas.
- Jaringan yang sangat teratur di mana setiap perangkat memiliki akses ke token dan peluang untuk melakukan transmisi.
- Berkinerja lebih baik daripada jaringan bintang di bawah beban jaringan yang berat.

**Kekurangan**

- ※ Kegagalan satu node menyebabkan seluruh jaringan down.
- ※ Deteksi kesalahan dan administrasi jaringan menjadi sulit.
- ※ Memindahkan, menambah dan mengubah perangkat dapat mempengaruhi jaringan.
- ※ Lebih lambat dari topologi star pada beban normal.

Secara umum, arsitektur bus lebih disukai daripada topologi lainnya tentu saja, ini adalah pendapat yang sangat subjektif dan desain akhir lebih bergantung pada kebutuhan jaringan daripada apa pun. Akhir-akhir ini sebagian besar jaringan beralih ke topologi star. Idealnya kita ingin merancang jaringan, yang secara fisik menyerupai topologi star, namun berperilaku seperti topologi bus atau ring.

**Ringkasan**

- Jaringan terdiri dari dua atau lebih komputer yang terhubung untuk berbagi sumber daya (seperti printer dan CD-ROM), bertukar file atau memungkinkan komunikasi elektronik. Komputer-komputer dalam suatu jaringan dapat dihubungkan melalui kabel, saluran telepon, gelombang radio, satelit, atau sinar inframerah.
- Tujuan utama jaringan komputer adalah untuk berbagi sumber daya. Tujuan utama jaringan adalah berbagi sumber daya. Tujuan kedua adalah memberikan keandalan yang tinggi dengan memiliki sumber pasokan alternatif. Tujuan lainnya adalah menghemat uang. Tujuan lain yang terkait erat adalah untuk meningkatkan kinerja

sistem seiring dengan meningkatnya beban kerja hanya dengan menambahkan lebih banyak prosesor. Dengan mainframe pusat, ketika sistem sudah penuh, maka harus diganti dengan yang lebih besar, biasanya dengan biaya yang besar dan dengan gangguan yang lebih besar lagi bagi pengguna. Jaringan komputer menyediakan media komunikasi yang kuat.

- Ada dua dimensi penting untuk mengklasifikasikan jaringan — teknologi transmisi dan skala.
- Teknologi transmisi dapat diklasifikasikan menjadi dua jenis:
  1. Jaringan broadcast.
  2. Jaringan peer-to-peer.
- Jaringan penyiaran: Jaringan ini mempunyai saluran komunikasi tunggal yang digunakan bersama oleh semua mesin di jaringan.
- Jaringan point-to-point terdiri dari banyak koneksi antar pasangan mesin. Beberapa rute dan mesin perantara mungkin ada di antara sepasang mesin; jadi algoritma perutean memainkan peran penting di sini.
- Kumpulan jaringan yang saling berhubungan disebut internetwork atau hanya Internet. Internet mengacu pada Internet spesifik di seluruh dunia yang banyak digunakan untuk menghubungkan universitas, kantor pemerintah, perusahaan, dan individu swasta.
- Topologi jaringan adalah desain dasar jaringan komputer. Ini merinci bagaimana komponen jaringan utama seperti node dan link saling berhubungan.
- Ada tiga tipe utama topologi jaringan yang mengacu pada tata letak fisik dan logis dari pengkabelan Jaringan. Yaitu topologi star, ring, dan bus.

**Latihan Soal**

Isilah bagian yang kosong:

1. Tujuan utama berjejaring adalah …….
2. Dalam sistem terdistribusi, keberadaan beberapa komputer otonom adalah ……. kepada pengguna.
3. Komputer-komputer pada…….dapat dihubungkan melalui kabel, saluran telepon, gelombang radio, satelit atau pancaran sinar inframerah.
4. Anda dapat membuat file dan menyimpannya dalam satu komputer, lalu ……. file-file itu dari komputer lain yang terhubung dengannya.
5. A……. sistem adalah kasus khusus dari suatu jaringan, yang perangkat lunaknya memberikan tingkat keterpaduan dan transparansi yang tinggi.

Nyatakan apakah pernyataan berikut ini benar atau salah:

1. Topologi, yang merupakan pola interkoneksi antar node, mempengaruhi biaya dan kinerja jaringan. (B/S)
2. Ada Lima tipe utama topologi jaringan yang mengacu pada tata letak fisik dan logis dari pengkabelan Jaringan. (B/S)

3. Bus adalah yang paling sederhana dan tertua dan semua saklar telepon didasarkan pada hal ini. (B/S)
4. Bus terdiri dari satu kabel yang disebut Backbone yang menghubungkan semua workstation pada jaringan menggunakan satu jalur. (B/S)
5. Tujuan dari terminator di kedua ujung jaringan adalah untuk menghentikan sinyal dipantulkan kembali. (B/S)

**Uraian**

1. Apa saja faktor utama yang menjadikan penggunaan jaringan komputer sebagai bagian integral dari bisnis?
2. Bagaimana klasifikasi jaringan komputer? Sebutkan beberapa alasan penting untuk klasifikasi jaringan komputer.
3. Bagaimana ciri-ciri LAN? Menjelaskan.
4. Apa sajakah teknologi berbeda yang tersedia untuk mengimplementasikan WAN?
5. Apa itu WAN? Apa bedanya dengan LAN dan MAN? Berikan setidaknya dua contoh WAN yang populer.

# BAB 2
# PERANGKAT LUNAK JARINGAN

## 2.1 ARSITEKTUR JARINGAN

Arsitektur jaringan mendefinisikan produk dan layanan komunikasi, yang memastikan bahwa berbagai komponen dapat bekerja sama. Pada masa awal sistem komunikasi data, sebagian besar komunikasi dilakukan antara DTE dan komputer host. Oleh karena itu, prosedur pengendalian transmisi saja sudah cukup sebagai protokol komunikasi. Namun, sistem komputer saat ini terhubung dengan sistem lain untuk membentuk jaringan, menghasilkan situasi di mana diperlukan protokol berbeda yang melayani tujuan berbeda. Oleh karena itu, arsitektur jaringan mewakili sistemisasi berbagai jenis protokol yang diperlukan untuk membangun jaringan.

Produsen komputer telah mengembangkan protokol berbeda sesuai kebutuhan. Artinya setiap jenis komputer memerlukan dukungan protokol yang berbeda-beda. Hal ini juga memerlukan biaya pengembangan dan pemeliharaan yang besar. Oleh karena itu, semua produsen komputer bekerja sama untuk menstandardisasi dan mensistematisasikan protokol untuk menghubungkan model mereka dan dengan demikian mengurangi biaya pengembangan dan pemeliharaan. Beginilah cara masing-masing pabrikan membangun arsitektur jaringannya sendiri. Sejak konsep arsitektur jaringan pertama kali diperkenalkan untuk menghubungkan komputer-komputer dari pabrikan yang sama, prosesnya menjadi lebih mudah. Namun, dari sudut pandang pengguna, bentuk arsitektur jaringan yang ideal adalah satu, yang memungkinkan mesin dari semua produsen terhubung satu sama lain. Oleh karena itu, perlunya standarisasi arsitektur jaringan.

## 2.2 MELAPISI PROSES KOMUNIKASI

Interkoneksi Sistem Terbuka (OSI) ditetapkan sebagai standar internasional untuk arsitektur jaringan untuk mengurangi kompleksitas desainnya. Oleh karena itu, sebagian besar jaringan disusun sebagai serangkaian lapisan atau level. Melapisi proses komunikasi berarti memecah proses komunikasi menjadi kategori-kategori yang lebih kecil dan lebih mudah ditangani, yang masing-masing memecahkan aspek penting dan berbeda dari proses pertukaran data. Setiap lapisan harus menawarkan layanan tertentu kepada lapisan yang lebih tinggi. Dengan demikian, lapisan pada satu komputer melakukan percakapan dengan lapisan yang sesuai pada komputer lain dalam jaringan. Aturan dan konvensi yang digunakan dalam komunikasi tersebut secara kolektif dikenal sebagai protokol lapisan. Entitas yang terdiri dari lapisan-lapisan yang sesuai pada komputer yang berbeda disebut rekan, yang berkomunikasi menggunakan protokol. Di antara setiap pasangan lapisan yang berdekatan terdapat antarmuka yang mendefinisikan operasi dan layanan primitif yang ditawarkan lapisan bawah ke lapisan atas.

Organisasi Internasional untuk Standardisasi (ISO) mengambil inisiatif dalam mendirikan OSI. OSI memiliki dua arti. Ini mengacu pada:

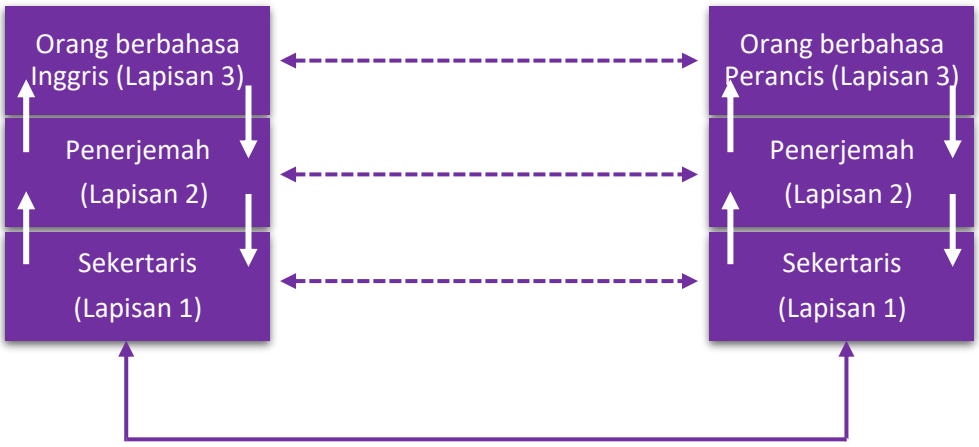
- Protokol yang disahkan oleh ISO
- Model referensi dasar OSI

Model referensi OSI membagi fungsi-fungsi yang diperlukan arsitektur jaringan menjadi beberapa lapisan dan mendefinisikan fungsi setiap lapisan. Kelompok lapisan dan protokol disebut arsitektur jaringan. Kelompok lapisan ini diberikan informasi yang cukup untuk memungkinkan implementasi perangkat lunak/perangkat keras, yang mematuhi protokol yang sesuai dengan benar.

Tujuan dari perincian ini adalah untuk mengembangkan pemahaman tentang kompleksitas dan kecanggihan yang telah dicapai teknologi ini, selain untuk mengembangkan konsep cara kerja berbagai komponen yang berkontribusi pada proses komunikasi data. Detail implementasi dan spesifikasi antarmuka tidak pernah menjadi bagian dari arsitektur karena tidak terlihat dari luar.

Fungsi arsitektur berlapis dapat dipahami dengan contoh konservasi yang terjadi antara dua orang dengan bahasa komunikasi yang berbeda, misalnya Inggris dan Perancis. Arsitektur tiga lapis seperti yang ditunjukkan pada Gambar 2.1 menjelaskan konsep tersebut. Garis putus-putus dari rekan ke rekan menunjukkan koneksi virtual.

- Dua orang (proses rekan di lapisan 3), yang satu berbicara bahasa Inggris dan yang lainnya berbicara bahasa Prancis, ingin berkomunikasi.
- Mereka menggunakan penerjemah (proses rekan di lapisan 2).
- Seorang sekretaris (proses rekan di lapisan 1) memfasilitasi setiap penerjemah untuk transmisi pesan.
- Orang Inggris menyampaikan pesannya dalam bahasa Inggris kepada penerjemahnya, yang menerjemahkannya ke dalam bahasa Prancis atau bahasa lain, bergantung pada protokol lapisan 2.




**Gambar 2.1 Fungsi Arsitektur Berlapis**

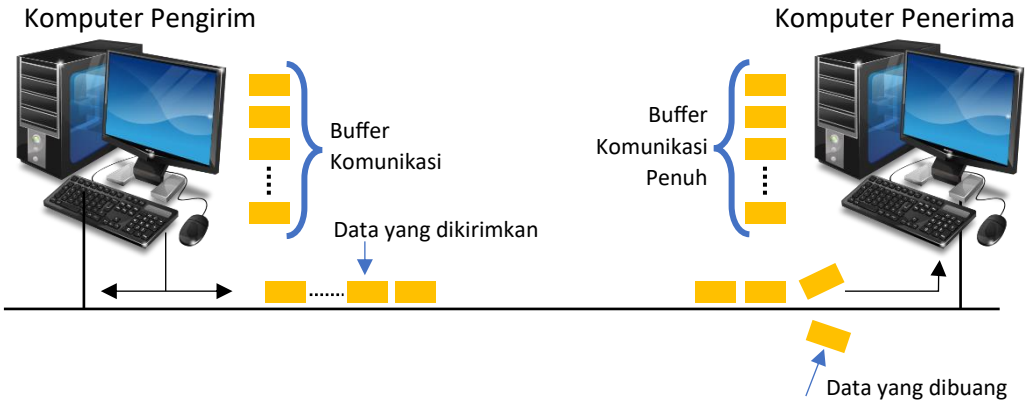
- Penerjemah kemudian meneruskan pesan ke sekretaris di lapisan 1 untuk mengirimkan pesan melalui telepon, email, atau cara lain, tergantung pada protokol lapisan 1.

- ❖ Ketika pesan sampai di tujuan, sekretaris sejawat meneruskan pesan tersebut ke penerjemah sejawat, yang menerjemahkannya ke dalam bahasa Prancis dan meneruskan 2/3 antarmuka ke orang yang berbahasa Prancis.
- ❖ Dengan demikian, percakapan yang efektif terjadi antara dua orang yang tidak memahami bahasa satu sama lain. Demikian pula, dua komputer di jaringan berbeda berkomunikasi satu sama lain.

**Masalah Desain untuk Lapisan**

Dalam pertukaran informasi antar komputer, proses komunikasi perlu memiliki hal-hal berikut untuk mencapai aspek proses pertukaran berikut:

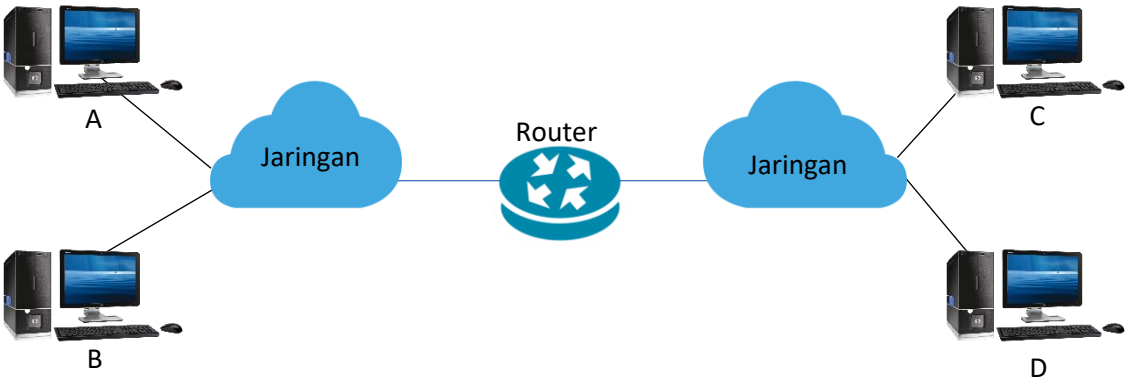
- Pengkodean Data Fisik: Pertukaran informasi antara dua komputer dilakukan secara fisik melalui sinyal listrik dengan asumsi metode pengkodean tertentu. Agar dua komputer dapat bertukar data dengan andal, mereka harus memiliki implementasi pengkodean dan interpretasi data yang kompatibel yang membawa sinyal listrik.
- Multiplexing: Ini menggunakan koneksi yang sama untuk beberapa percakapan yang tidak berhubungan. Misalnya, beberapa sirkuit fisik digunakan untuk semua koneksi virtual.
- Media Transmisi: Masalah ini berkaitan dengan jenis media yang digunakan (fiber, tembaga, nirkabel, dan sebagainya), yang ditentukan oleh bandwidth yang diinginkan, kekebalan terhadap kebisingan, dan sifat redaman. Faktor-faktor ini mempengaruhi panjang media maksimum yang diperbolehkan sambil tetap mencapai tingkat jaminan transmisi data yang diinginkan.
- Kontrol Aliran: Proses komunikasi data mengalokasikan sumber daya memori, yang biasa dikenal sebagai buffer komunikasi demi transmisi dan penerimaan data. Ini mencegah pengirim yang cepat membanjiri penerima yang lambat dengan data. Diperlukan semacam umpan balik dari penerima. Teknik pengendalian aliran data yang tepat menginginkan bahwa proses penerimaan dalam transmisi data harus mengirimkan sinyal “berhenti pengiriman” ke komputer pengirim setiap kali komputer tersebut tidak memiliki sumber daya untuk mengatasi kecepatan pengiriman data. Di sisi lain, ketika perangkat penerima memiliki sumber daya yang cukup, perangkat tersebut harus mengirimkan sinyal “lanjutkan pengiriman”. Sumber daya yang tersedia di pihak penerima untuk mengatasi komputer pengirim adalah ketersediaan buffer. Gambar 2.2 menunjukkan mekanisme kontrol aliran data.




**Gambar 2.2 Mekanisme Kontrol Aliran Data**

Komputer penerima harus mampu membedakan antara sinyal pembawa informasi dan kebisingan belaka.

- Mekanisme untuk mengidentifikasi pengirim dan penerima: Suatu bentuk pengalamatan untuk mesin dan proses untuk mendeteksi apakah sinyal pembawa informasi ditujukan untuk dirinya sendiri atau komputer lain di jaringan, atau suatu siaran (pesan yang ditujukan untuk semua komputer di jaringan).
- Pengendalian kesalahan: Pihak penerima setelah selesai menerima informasi juga harus mampu menangani dan mengenali kerusakan, jika ada, kerusakan ini dapat berupa kebisingan atau interferensi elektromagnetik. Kedua belah pihak harus memiliki kode pendeteksi kesalahan dan koreksi kesalahan yang sama. Selain itu, diperlukan suatu mekanisme untuk menunjukkan pesan mana yang telah diterima dengan benar dan mana yang belum.
- Saluran logis: Protokol harus menyediakan setidaknya dua saluran logis per koneksi.
- Urutan atau pengurutan pesan: Pesan dipecah menjadi beberapa bagian dan diberi nomor sebelum dikirim. Harus ada mekanisme untuk mengembalikannya ke pihak penerima. Paket-paket ini mungkin mengambil rute berbeda untuk sampai di komputer tujuan dan oleh karena itu tidak harus berurutan.
- Routing: Pendekatan routing memerlukan penerapan berbagai proses kooperatif, baik pada router maupun server, yang perhatian utamanya adalah memungkinkan pengiriman data secara cerdas ke tujuan akhirnya. Pertukaran data dapat terjadi antara dua stasiun kerja mana pun, baik keduanya berada dalam jaringan yang sama atau tidak seperti yang ditunjukkan pada Gambar 2.3.




**Gambar 2.5 Router Menghubungkan 2 jaringan**

- Kontrol dialog antar-proses: Ketika dua aplikasi terlibat dalam pertukaran data, mereka membuat sesi di antara keduanya. Akibatnya, timbul kebutuhan untuk mengontrol aliran dan arah aliran data di antara keduanya selama sesi berlangsung. Tergantung pada sifat aplikasi yang terlibat, tipe dialog mungkin mode komunikasi dupleks penuh, setengah dupleks, atau simpleks.
- Pemulihan Sesi: Kekhawatiran lain yang berorientasi pada aplikasi adalah kemampuan untuk memulihkan kegagalan secara andal dengan biaya minimum. Hal ini dapat dicapai dengan menyediakan mekanisme pemeriksaan, yang memungkinkan dimulainya kembali kegiatan sejak pos pemeriksaan terakhir. Pemeriksaan penunjuk menghindari persyaratan ini dengan hanya mengirimkan ulang file yang terpengaruh, sehingga menghemat waktu dan bandwidth.
- Masalah Presentasi: Setiap kali dua atau lebih aplikasi yang berkomunikasi berjalan pada platform yang berbeda, kekhawatiran lain muncul tentang perbedaan sintaksis data yang dipertukarkan. Menyelesaikan perbedaan ini memerlukan proses tambahan. Contoh yang baik dari masalah presentasi adalah ketidakcocokan antara standar pengkodean karakter ASCII dan EBCDIC, ketidakcocokan emulasi terminal, dan ketidakcocokan karena teknik enkripsi data.

## 2.3 ANTARMUKA DAN LAYANAN

Setiap lapisan memberikan layanan kepada lapisan yang berada tepat di atasnya. Ada beberapa istilah terkait yang sering digunakan:

※ Entitas: Mereka adalah elemen aktif. Misalnya proses, chip I/O, dll di setiap lapisan.
※ Entitas rekan: Mereka adalah entitas di lapisan yang sama pada komputer yang berbeda.
※ Penyedia layanan: Fungsi lapisan ini menyediakan layanan tertentu.
※ Pengguna layanan: Fungsi lapisan ini menggunakan layanan tertentu.
※ SAP (*Service Access Points*): Ini adalah titik dari mana layanan dapat diakses. Setiap SAP memiliki alamat unik.

**Layanan Berorientasi Koneksi dan Tanpa Koneksi**

Layanan berorientasi koneksi mirip dengan sistem telepon di mana saluran khusus dibuat antara pengirim dan penerima sebelum transmisi. Mereka cocok untuk komunikasi jangka panjang antara pengirim dan penerima. Namun, mereka terkenal karena pemborosan bandwidth. Dalam layanan berorientasi koneksi, setiap paket dikaitkan dengan koneksi sumber/tujuan. Paket-paket ini dirutekan sepanjang jalur yang sama, yang dikenal sebagai sirkuit virtual. Pelayanan connectionless mengadopsi mekanisme sistem pos. Setiap pesan dipecah menjadi beberapa paket dan dimasukkan ke dalam amplop. Amplop itu berisi alamat lengkap. Amplop tersebut kemudian dirutekan secara independen. Urutan paket tidak dijamin. Mereka cocok untuk mengirim pesan singkat dan terkenal menyediakan bandwidth dalam interval waktu singkat.

Dalam layanan connectionless, router memperlakukan setiap paket secara individual. Paket-paket tersebut dirutekan melalui jalur yang berbeda melalui jaringan sesuai dengan keputusan yang dibuat oleh router.

**Kualitas pelayanan**

Layanan yang andal menjamin pengiriman data, yang dilaksanakan dengan pengakuan. Namun, hal ini menimbulkan biaya tambahan dan dengan demikian mengurangi efisiensi. Dalam hal transfer file, kita memerlukan layanan berorientasi koneksi yang andal, sedangkan layanan berorientasi koneksi yang tidak dapat diandalkan cocok untuk lalu lintas suara digital.

Contoh: Email terdaftar adalah contoh layanan tanpa koneksi yang andal dengan pengakuan, sedangkan layanan tanpa koneksi yang tidak dapat diandalkan tanpa pengakuan cocok untuk email sampah. Mereka memiliki kemungkinan kedatangan yang tinggi tetapi tidak ada jaminan. Dalam model client-server, perintah request-reply adalah contoh lain dari layanan connectionless.

**Primitif Layanan**

Layanan berorientasi koneksi atau tanpa koneksi ditentukan oleh sekumpulan primitif yang tersedia bagi pengguna layanan untuk berinteraksi dengan penyedia layanan. Primitif ini memungkinkan penyedia layanan untuk melakukan beberapa tindakan atau melaporkan tindakan yang diambil oleh entitas rekan. Primitif memiliki parameter untuk menentukan kondisi. Misalnya, primitif permintaan dan respons, pengirim dan penerima dapat menegosiasikan beberapa kondisi seperti ukuran pesan. Mereka adalah bagian dari protokol. Layanan yang dikonfirmasi didefinisikan dengan permintaan, indikasi, respons, dan primitif konfirmasi. Layanan yang belum dikonfirmasi hanya memiliki permintaan dan indikasi primitif.

**Hubungan Layanan dengan Protokol**

Layanan dan protokol adalah konsep yang berbeda dan penting untuk membangun dan melepaskan koneksi antara pengirim dan penerima.

Layanan didefinisikan sebagai sekumpulan primitif yang tidak lain hanyalah tindakan atau operasi. Mereka diberikan ke lapisan atas oleh lapisan bawah langsung. Ini hanya mendefinisikan sifat tindakan yang dilakukan oleh lapisan di atas lapisan pemrakarsa layanan.

Sebuah protokol mendefinisikan seperangkat aturan untuk menggambarkan format dan arti dari frame, paket atau pesan yang dipertukarkan oleh entitas rekan dalam lapisan yang sama. Entitas menggunakan protokol untuk mengimplementasikan definisi layanannya.

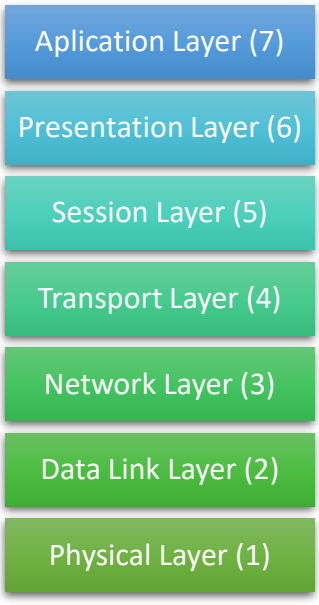
## 2.4 MODEL REFERENSI

**Model Referensi Interkoneksi Sistem Terbuka (OSI).**

Sekarang Anda akan mempelajari konsep Model Referensi OSI. Organisasi Standardisasi Internasional (ISO) mengembangkan model komunikasi data OSI pada tahun 1984. OSI menetapkan model tujuh lapisan seperti yang ditunjukkan pada Gambar 2.4. Selain menjadi dasar pengembangan protokol OSI sendiri, protokol ini juga digunakan oleh industri sebagai kerangka acuan ketika menjelaskan arsitektur protokol dan karakteristik fungsionalnya.

ISO, dalam upaya mendorong jaringan terbuka, mengembangkan model referensi interkoneksi sistem terbuka. Model tersebut secara logis mengelompokkan fungsi-fungsi dan menetapkan aturan-aturan, yang disebut protokol, yang diperlukan untuk membangun dan melakukan komunikasi antara dua pihak atau lebih. Model tersebut terdiri dari tujuh fungsi yang sering disebut sebagai lapisan seperti yang ditunjukkan pada Gambar 2.4.

Tiga lapisan terakhir terutama berkaitan dengan organisasi perangkat lunak terminal dan tidak secara langsung menjadi perhatian para insinyur komunikasi. Lapisan transport adalah lapisan yang menghubungkan proses komunikasi dengan protokol berorientasi perangkat lunak ini. Perangkat transmisi menggunakan lapisan atas, di mana data ditempatkan ke dalam sebuah paket, diawali dengan header. Data dan header, yang secara kolektif dikenal sebagai Protocol Data Unit (PDU), ditangani oleh masing-masing lapisan bawah secara berurutan saat data berjalan melintasi jaringan ke node penerima. Di node penerima, data berjalan ke atas model berlapis, lapisan yang lebih tinggi berturut-turut menghapus informasi header.




**Gambar 2.4 Model OSI**

Prinsip-prinsip dan pedoman mendasar yang diterapkan untuk mencapai tujuh lapisan tersebut diberikan di bawah ini:

1. Sebuah lapisan dibuat pada tingkat abstraksi yang berbeda.
2. Setiap lapisan ditugaskan untuk menjalankan fungsi yang ditentukan dengan baik.
3. Fungsi setiap lapisan didasarkan pada protokol berstandar internasional.
4. Batas lapisan dipilih untuk meminimalkan aliran informasi melintasi antarmuka.
5. Jumlah lapisan dijaga agar cukup besar sehingga fungsi yang berbeda mempunyai lapisan yang berbeda. Mereka juga dibuat cukup kecil sehingga arsitekturnya tidak menjadi berat.

**Lapisan Fisik (Lapisan 1)**

Lapisan ini menggambarkan media fisik atau saluran komunikasi di mana aliran bit akan ditransmisikan dengan tujuan bahwa ketika pihak pengirim mengirimkan 1 bit, maka diterima oleh pihak penerima sebagai 1 bit, bukan sebagai 0 bit. Oleh karena itu, ia mendefinisikan aspek listrik dan mekanik dari antarmuka ke media fisik untuk transmisi data, serta pengaturan, pemeliharaan, dan pemutusan hubungan fisik. Hal ini terutama berkaitan dengan perpindahan bit dari satu node ke node berikutnya melalui link fisik. Permasalahan yang berkaitan dengan lapisan fisik melibatkan amplitudo pulsa untuk menentukan level 1 dan 0, lebar pulsa dalam mikrodetik, jenis dan mode komunikasi, pembentukan dan pemutusan koneksi pada saat komunikasi, jenis konektor, dll.

Ia menerima data dari lapisan Data Link dalam aliran bit untuk transmisi selanjutnya melalui media fisik. Pada lapisan ini, karakteristik mekanis (tipe konektor), kelistrikan (level tegangan), fungsional (penetapan ping), dan prosedural (jabat tangan) ditentukan. RS-232C/D adalah contoh definisi lapisan fisik.

**Lapisan Data Link (Lapisan 2)**

Dibutuhkan bit yang diterima oleh lapisan fisik dan mendeteksi kesalahan. Hal ini menetapkan jalur komunikasi bebas kesalahan antara node jaringan melalui saluran fisik, membingkai pesan untuk transmisi, memeriksa integritas pesan yang diterima, mengelola akses dan penggunaan saluran, memastikan urutan data yang dikirimkan dengan benar. Oleh karena itu, lapisan ini bertanggung jawab atas transfer data yang andal melalui tautan Fisik. Tanggung jawabnya mencakup fungsi-fungsi seperti kontrol aliran data, pemecahan data masukan, pemformatan bingkai, transmisi bingkai secara berurutan, deteksi kesalahan, dan manajemen tautan, dll. Untuk memberikan layanan yang andal, ia juga menawarkan pemrosesan bingkai pengakuan, transmisi ulang frame yang hilang atau rusak, dll.

**Lapisan Jaringan (Lapisan 3)**

Lapisan jaringan terdiri dari perangkat lunak yang menangani PDU dan mengangkutnya ke tujuan akhir, menyiapkan jalur yang sesuai antara berbagai node. Oleh karena itu, tujuan utama dari lapisan ini adalah untuk mengontrol pengoperasian subnet. Ini adalah lapisan yang menyediakan Internet Protocol (IP) untuk menggunakannya. Hal ini terutama bertanggung jawab untuk menyediakan layanan routing dari sumber ke tujuan melalui Internet. Dengan melakukan hal ini, memungkinkan internetworking antara jaringan heterogen menggunakan

pengalamatan yang berbeda, panjang paket, protokol, dll. Peruteannya mungkin statis atau dinamis. Lapisan jaringan juga memainkan peran penting dalam pengendalian kemacetan.

Ini juga melindungi lapisan di atas dari rincian tentang jaringan yang mendasarinya (topologi jaringan dan peta jalan) dan teknologi perutean yang mungkin digunakan untuk menghubungkan jaringan yang berbeda secara bersamaan. Selain routing, lapisan ini bertanggung jawab untuk membangun dan memelihara koneksi. Dalam jaringan penyiaran, masalah peruteannya sederhana, sehingga lapisan jaringan seringkali tipis atau bahkan tidak ada sama sekali. Tiga lapisan berikutnya berorientasi pada tugas dan berkaitan dengan operasi yang dilakukan oleh pengguna, bukan dengan jaringan.

**Lapisan Transportasi (Layer 4)**

Lapisan ini menjamin pengiriman data yang teratur dan andal antar sistem akhir setelah menerima data dari lapisan sesi. Data diterima dari lapisan Sesi dan dibagi menjadi unit-unit yang lebih kecil, jika diperlukan. Lapisan sesi meneruskan data ke lapisan Jaringan dan memastikan bahwa paket tiba dengan benar di sisi penerima.

Pada dasarnya, ia melakukan manajemen koneksi berdasarkan kondisi throughput. Dalam kondisi normal, satu koneksi jaringan berhubungan dengan beberapa koneksi transport. Dalam kondisi throughput tinggi, satu koneksi transport berhubungan dengan beberapa koneksi jaringan. Rangkaian protokol paling populer TCP/IP menggunakan lapisan ini. Lapisan transport juga melakukan fungsi tambahan seperti multiplexing dan de-multiplexing data. Lapisan ini membagi pesan transmisi menjadi paket-paket dan menyusunnya kembali di pihak penerima. Layanan yang ditawarkan pada lapisan ini mencakup saluran point-to-point bebas kesalahan untuk menyampaikan pesan sesuai urutan pengirimannya. Lapisan transport adalah lapisan sumber-ke-tujuan atau lapisan ujung-ke-akhir yang sebenarnya. Kontrol aliran antar host juga diperlukan tetapi berbeda dengan antar router (prinsip serupa akan berlaku untuk keduanya).

**Lapisan Sesi (Lapisan 5)**

Lapisan sesi bertanggung jawab untuk membangun, memelihara, dan menengahi dialog antara aplikasi yang berkomunikasi. Ia juga menyediakan layanan yang ditingkatkan yang berguna dalam beberapa aplikasi, misalnya, login jarak jauh, transfer file jarak jauh, dll. Ia juga bertanggung jawab atas pemulihan yang teratur dari kegagalan dengan menerapkan mekanisme penunjuk pemeriksaan yang sesuai.

**Lapisan Presentasi (Layer 6)**

Lapisan presentasi menjalankan fungsi yang berkaitan dengan sintaksis dan semantik informasi yang dikirimkan termasuk pemformatan dan tampilan data yang diterima oleh terminal dan printer. Hal ini berkaitan dengan perbedaan sintaks data yang digunakan oleh aplikasi yang berkomunikasi. Lapisan ini bertanggung jawab untuk memperbaiki perbedaan tersebut dengan menggunakan mekanisme yang mengubah sintaksis lokal (khusus untuk platform yang dimaksud) menjadi sintaksis umum untuk tujuan pertukaran data.

Misalnya, ia melakukan pengkodean data dalam standar yang disepakati dengan cara untuk memfasilitasi pertukaran informasi antara sistem heterogen menggunakan kode string yang berbeda, misalnya, konversi antara kode karakter ASCII dan EBCDIC. Ini memfasilitasi

kompresi data untuk mengurangi jumlah bit yang akan dikirim dan mengenkripsi data untuk privasi dan otentikasi, jika diperlukan.

**Lapisan Aplikasi (Lapisan 7)**

Lapisan aplikasi menyediakan layanan dukungan untuk tugas pengguna dan aplikasi. Ini menentukan bagaimana pengguna akan menggunakan jaringan data. Ini memungkinkan pengguna untuk menggunakan jaringan. Misalnya, ia menyediakan layanan berbasis jaringan kepada pengguna akhir. Contoh layanan jaringan adalah database terdistribusi, surat elektronik, berbagi sumber daya, transfer file, akses file jarak jauh, dan manajemen jaringan. Lapisan ini mendefinisikan sifat tugas yang akan dilakukan.

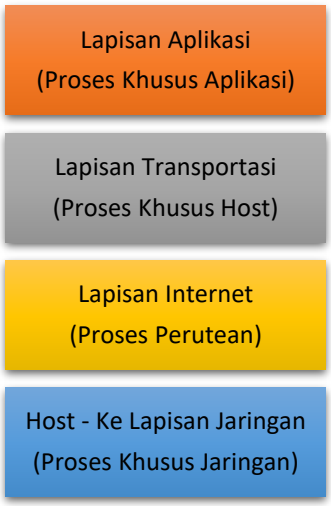
**Model Referensi TCP/IP**

Model TCP/IP dianggap sebagai protokol tertua dari semua jaringan komputer seperti ARPANET dan penerusnya Internet. TCP/IP adalah singkatan dari Transmision Control Protocol/Internet Protocol. Ini dikembangkan dengan tujuan untuk menentukan serangkaian protokol yang mampu menyediakan layanan interoperabilitas komunikasi transparan antara komputer dari semua ukuran, terlepas dari platform perangkat keras atau sistem operasi yang mendukungnya. Selama bertahun-tahun, TCP/IP telah menjadi protokol yang paling tersebar luas saat ini. Salah satu alasan popularitas TCP/IP adalah ketersediaan spesifikasi protokolnya untuk umum. Dalam hal ini, TCP/IP dapat dianggap sebagai sistem terbuka. Sebagian besar pengguna mengandalkan TCP/IP untuk tujuan transfer file, surat elektronik (e-mail), dan layanan login jarak jauh.

Model TCP/IP ditujukan untuk menghubungkan beberapa jaringan bersama-sama dengan cara yang mulus bahkan jika terjadi kerusakan pada perangkat keras subnet. Tidak hanya menyediakan komunikasi yang lancar, namun juga menyediakan arsitektur fleksibel yang dapat mendukung aplikasi dengan kebutuhan berbeda, mulai dari transfer file hingga transmisi ucapan real-time. Tujuan ini dapat dicapai karena dimasukkannya penelitian tentang jaringan packet-switching ke ARPAnet.

TCP berhubungan dengan lapisan keempat model referensi OSI. IP sesuai dengan lapisan ketiga dari model yang sama. TCP menyediakan layanan jenis koneksi. Artinya, koneksi logis harus dibuat sebelum komunikasi untuk terus mengirimkan data dalam jumlah besar dengan pengakuan. IP adalah layanan tipe tanpa koneksi dan sebelum transmisi data, tidak diperlukan koneksi logis.

TCP/IP mendefinisikan serangkaian protokol komunikasi dan aplikasi dalam struktur lapisan, dengan setiap lapisan menangani layanan komunikasi yang berbeda. TCP/IP mendefinisikan model empat lapisan seperti yang ditunjukkan pada Gambar 2.5 yang terdiri dari lapisan internet, lapisan transport, lapisan aplikasi dan lapisan host-ke-jaringan. Arsitektur ini didasarkan pada tiga rangkaian proses yang saling bergantung, yaitu proses spesifik aplikasi, proses spesifik host, dan proses spesifik jaringan.




**Gambar 2.5 Arsitektur Komunikasi TCP/IP**

**Lapisan Internet**

Format paket dan protokol pada lapisan ini disebut Internet Protocol (IP). IP adalah layanan tipe tanpa koneksi yang memasukkan paket IP ke jaringan mana pun. Paket-paket tersebut bergerak secara independen ke tujuan. Sebelum transmisi data, tidak diperlukan koneksi logis. Lapisan Internet TCP/IP sesuai dengan lapisan jaringan model referensi OSI dalam hal fungsionalitas, seperti yang ditunjukkan pada Gambar 2.5

**Lapisan Transportasi**

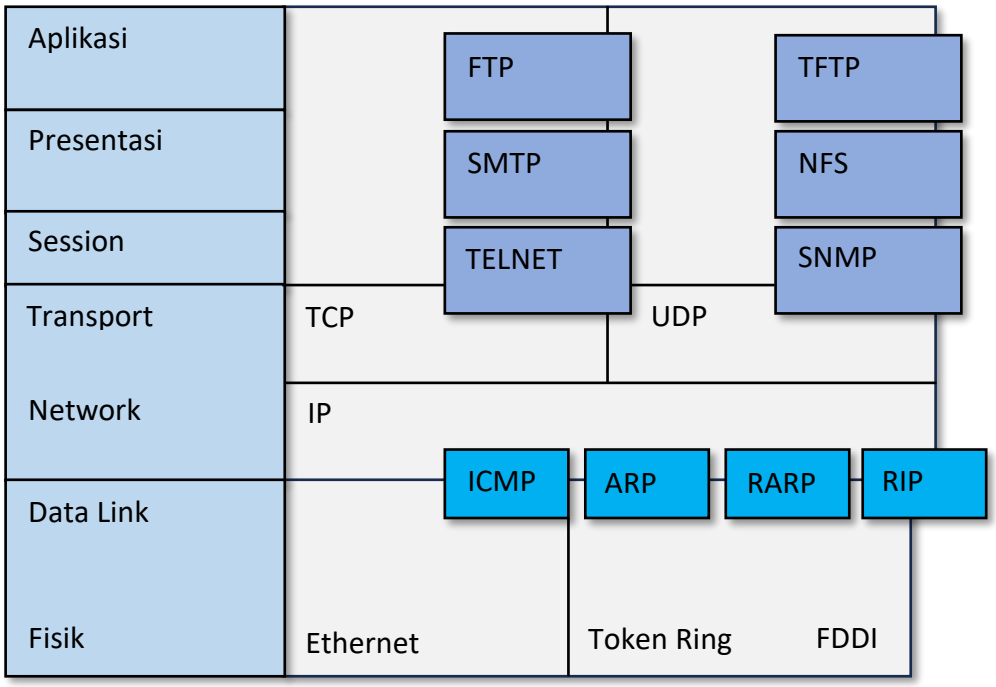
Lapisan transport model TCP/IP sesuai dengan lapisan transport model referensi OSI. Ini diwakili oleh dua protokol end-to-end yaitu TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol). TCP adalah protokol berorientasi koneksi yang andal dan UDP adalah protokol tanpa koneksi yang tidak dapat diandalkan.

**Lapisan Aplikasi**

Model TCP/IP adalah model pertama dari jenisnya dan oleh karena itu tidak mengandung lapisan sesi atau presentasi karena sedikit kegunaannya pada sebagian besar aplikasi. Lapisan ini memiliki semua protokol tingkat yang lebih tinggi, seperti yang ditunjukkan pada Gambar 2.5.

**Lapisan Host-ke-jaringan**

Lapisan di bawah lapisan Internet tidak ditentukan dan bervariasi dari host dan jaringan ke jaringan. Model TCP/IP menyarankan bahwa host harus terhubung ke jaringan menggunakan beberapa protokol sehingga dapat mengirimkan paket IP melalui jaringan tersebut.




**Gambar 2.6 Model TCP/IP dan Model OSI**

**Perbandingan Model Referensi OSI dan TCP/IP**

Di bagian ini, Anda akan mengetahui perbedaan antara Model Referensi OSI dan TCP/IP. Gambar 2.6 menunjukkan kesamaan antara model referensi TCP/IP dan OSI. Kedua model tersebut dikembangkan berdasarkan konsep tumpukan protokol independen dengan fungsi lapisan yang serupa. Terlepas dari kesamaan antara kedua model, keduanya juga memiliki perbedaan dalam fungsi yang disediakan oleh layanan, antarmuka, dan protokol. Model referensi OSI membedakannya dengan jelas sedangkan model TCP/IP tidak membedakannya secara eksplisit. Perbedaan lainnya adalah:

- Model OSI memiliki tujuh lapisan dan model TCP/IP hanya memiliki empat lapisan.
- Model OSI dikembangkan sebelum protokol dirancang. Model TCP/IP dikembangkan setelah pengembangan protokol.
- Model OSI memiliki komunikasi berorientasi koneksi dan tanpa koneksi pada lapisan jaringan dan komunikasi berorientasi koneksi pada lapisan transport. Model TCP/IP mendukung mode connectionless di lapisan Internet dan kedua mode di lapisan transport.

**Ringkasan**

- Tiga komponen dasar yaitu; perangkat keras, protokol (perangkat lunak) dan aplikasi (perangkat lunak yang berguna) adalah wajib untuk mengimplementasikan jaringan komputer. Dijelaskan juga bahwa konsep layer penting dalam jaringan.
- Setiap lapisan dengan dua lapisan berfungsi sebagai antarmuka dan melindungi lapisan atas sehingga setiap lapisan dapat berubah dengan dampak minimal pada lapisan atas.

Dalam beberapa kasus, perlindungan ini sangat baik sehingga aplikasi mungkin tidak mengetahui bahwa aplikasi tersebut berjalan pada perangkat keras yang berbeda.

- Model jaringan OSI memiliki tujuh lapisan.
- TCP/IP adalah singkatan dari Transmisi Kontrol Protokol/Protokol Internet. Ini dikembangkan dengan tujuan untuk menentukan serangkaian protokol yang mampu menyediakan layanan interoperabilitas komunikasi transparan antara komputer dari semua ukuran, terlepas dari platform perangkat keras atau sistem operasi yang mendukungnya.
- Selama bertahun-tahun, TCP/IP telah menjadi protokol yang paling tersebar luas saat ini. Salah satu alasan popularitas TCP/IP adalah ketersediaan spesifikasi protokolnya untuk umum. Dalam hal ini, TCP/IP dapat dianggap sebagai sistem terbuka. Sebagian besar pengguna mengandalkan TCP/IP untuk tujuan transfer file, surat elektronik (email), dan layanan login jarak jauh.

**Latihan Soal**

1) Lapisan TCP/IP..... sesuai dengan lapisan jaringan model referensi OSI dalam hal fungsionalitas.
2) TCP adalah.....protokol dan UDP adalah protokol tanpa koneksi yang tidak dapat diandalkan.
3) Model referensi OSI membagi fungsi-fungsi yang diperlukan dari..... menjadi beberapa lapisan dan mendefinisikan fungsi setiap lapisan.
4) .....adalah entitas pada lapisan yang sama pada komputer yang berbeda.
5) .....adalah titik dari mana layanan dapat diakses.

Nyatakan apakah pernyataan berikut ini benar atau salah:

1. Entitas yang terdiri dari lapisan terkait pada komputer berbeda disebut klien.
2. Organisasi Internasional untuk Standardisasi (ISO) mengambil inisiatif dalam mendirikan OSI.
3. Proses komunikasi data mengalokasikan sumber daya memori, yang biasa disebut buffer komunikasi untuk kepentingan transmisi dan penerimaan data.
4. Pertukaran informasi antara dua komputer dilakukan secara fisik melalui sinyal kimia dengan asumsi metode pengkodean tertentu.
5. Model referensi OSI membagi fungsi-fungsi yang diperlukan arsitektur jaringan menjadi lima lapisan dan mendefinisikan fungsi setiap lapisan.

**Uraian**

1. Apa isu desain penting untuk pertukaran informasi antar komputer?
2. Apa fungsi utama lapisan jaringan pada model ISO-OSI? Apa perbedaan fungsi pengiriman paket pada lapisan jaringan dengan lapisan data link?
3. Apa tujuan isolasi lapisan dalam model referensi OSI?
4. Mengapa model Referensi OSI diadopsi secara luas? Apa yang menjadikannya sebagai standar komunikasi data?
5. Soroti perbedaan antara model referensi OSI dan model TCP/IP.

# BAB 3
# LAPISAN FISIK

## 3.1 KONSEP DAN KETENTUAN TRANSMISI

Sebelum membahas macam-macam media transmisi, ada baiknya kita mengetahui sedikit tentang konsep dasar dan terminologi yang berhubungan dengan transmisi suatu sinyal.

- Spektrum Frekuensi:

**Tabel 3.1 Spektrum Frekuensi**

| Nama Band | Rentang Frekuensi | Panjang Gelombang | Penggunaan |
|---|---|---|---|
| Terdengar | 20Hz-20kHz | >100 Km | Suara |
| Radio Frekuensi Sangat/ Sangat Rendah (ELF/VLF) | 3kHz-30kHz | 100 - 10 Km | Navigasi radio, cuaca, komunikasi kapal selam |
| Radio Frekuensi Rendah (LF) | 30Hz-300kHz | 10 - 1 Km | Navigasi radio, komunikasi maritim |
| Radio Frekuensi Menengah (MF) | 300kHz-3MHz | 1 km – 100 m | Navigasi radio, radio AM |
| Frekuensi Tinggi (HF) | 3MHz-30MHz | 100 - 10 m | Radio band warga (CB) |
| Radio Frekuensi Sangat Tinggi (VHF) | 30MHz-300MHz | 10 - 1 m | Radio amatir (HAM), TV VHF, radio FM |
| Frekuensi Ultra Tinggi (UHF) | 300MHz-3GHz | 1m – cm | Microwave, satelit, Tv UHF |
| Radio Frekuensi Super (SHF) | 3GHz-30GHz | 10 - 1 cm | Microwave, satelit |
| Radio Frekuensi Sangat Tinggi (EHF) | 30GHZ-300GHz | 1 cm – 1mm | Microwave, satelit |
| Cahaya Inframerah | 103-105GHz | 300 – 3 µ | Inframerah |
| Cahaya Tampak | 1013-1015GHz | 1–.3µ | Serat optik |
| Sinar X | 1015-1018BGHz | 103–107 µ | T/A |
| Sinar Gamma Dan Kosmik | >1018GHz | <017 µ | T/A |

Simbol-simbol pada Tabel 3.1 mempunyai arti sebagai berikut:

**K (Kilo)** = 1.000,
**M (Mega)** = 1.000.000 (1 juta),
**G (Giga)** = 1.000.000 (1 miliar)
**T (Tera)** = 1.000.000.000 (1 triliun)
**cm** = sentimeter (1/100 meter)
**mm** = milimeter (1/1.000 meter)
**µ** = mikron (1/1.000.000 meter)

Dalam transmisi data, rentang frekuensi pembawa bergantung pada sifat media dan kebutuhan aplikasi yang didukung. Oleh karena itu, spektrum frekuensi dapat didefinisikan sebagai rentang frekuensi yang didukung oleh media transmisi tertentu. Rentang frekuensi sebenarnya yang mendukung komunikasi tertentu dikenal sebagai pass band. Ini diberikan pada Tabel 3.1.

- **Bandwidth**: Secara umum, kita dapat mengatakan bahwa bandwidth adalah perbedaan, yang dinyatakan dalam Hertz, antara frekuensi tertinggi dan terendah dalam suatu pita. Secara umum, semakin tinggi bandwidth, semakin besar pula kecepatan transmisi data atau throughputnya. Perlu dicatat bahwa bandwidth dan kecepatan transmisi data saling berhubungan erat satu sama lain. Jelasnya, setiap sistem transmisi menjadi lebih menarik jika bandwidth yang tersedia lebih besar, kesalahan yang ditimbulkan lebih sedikit, dan jarak maksimum antara berbagai elemen jaringan (penguat, repeater, dan antena) lebih besar.
- **Jarak**: Sinyal frekuensi yang lebih tinggi menawarkan bandwidth yang lebih besar; mereka juga umumnya lebih menderita karena redaman sinyal dibandingkan frekuensi yang lebih rendah. Fakta ini menghasilkan lebih banyak kesalahan dalam transmisi, kecuali amplifier/repeater ditempatkan lebih berdekatan. Ini dengan jelas menunjukkan hubungan yang erat dan langsung antara bandwidth, jarak, dan kinerja kesalahan. Bandwidth, dalam konteks ini, mengacu pada jumlah bandwidth mentah yang didukung media. Kinerja kesalahan mengacu pada jumlah atau persentase kesalahan yang terjadi dalam proses transmisi. Jarak mengacu pada pemisahan spasial minimum dan maksimum antar perangkat melalui suatu tautan, dalam konteks sirkuit ujung ke ujung yang lengkap.
- **Penundaan propagasi**: Penundaan propagasi mengacu pada lamanya waktu yang dibutuhkan sinyal untuk berpindah dari pemancar ke penerima melalui sistem transmisi. Sedangkan energi elektromagnetik bergerak dengan kecepatan kira-kira kecepatan cahaya (30.000 Kms per detik) di ruang bebas. Sebaliknya, kecepatan propagasi untuk kabel twisted pair atau koaksial hanya sebagian kecil dari angka ini. Sifat sistem transmisi akan mempunyai dampak yang besar terhadap tingkat penundaan propagasi. Dengan kata lain, panjang total rangkaian secara langsung mempengaruhi lamanya waktu yang dibutuhkan sinyal untuk mencapai penerima.

- **Keamanan**: Keamanan, dalam konteks sistem transmisi, membahas perlindungan data dari intersepsi saat melintasi jaringan. Khususnya dalam hal jaringan data, akses ke sistem jarak jauh dan data yang ada di dalamnya juga harus dibatasi pada pengguna yang berwenang; oleh karena itu, beberapa metode autentikasi harus digunakan untuk memverifikasi bahwa permintaan akses tersebut sah dan autentik.
- **Ketahanan terhadap kondisi lingkungan**: Ketahanan terhadap kondisi lingkungan terutama berlaku pada sistem kabel. Kabel twisted pair, coaxial, dan serat optik dimanipulasi secara fisik saat dipasang dan dikonfigurasi ulang. Jelasnya, masing-masing mempunyai batasan fisik tertentu terhadap jumlah tekukan dan puntiran (kekuatan lentur) yang dapat ditoleransi, serta jumlah beban atau tegangan memanjang yang dapat ditopangnya (kekuatan tarik), tanpa patah (kekuatan patah). Kabel serat optik terkenal rentan dalam hal ini. Kabel yang digantung di tiang memuai dan berkontraksi seiring dengan perubahan suhu lingkungan; sementara kabel serat optik kaca mengembang dan berkontraksi relatif sedikit, kawat tembaga pasangan terpilin lebih ekspansif. Masalah ketahanan terhadap kondisi lingkungan juga berlaku pada sistem gelombang udara, karena piringan reflektif, antena, dan perangkat lain yang digunakan dalam teknologi gelombang mikro, satelit, dan inframerah harus dipasang dengan aman untuk menghadapi angin dan kekuatan alam lainnya. Selain itu, menara, dinding, dan atap tempat pemasangannya harus dibangun dan diperkuat dengan baik agar dapat menahan gaya tersebut.
- **Dimensi fisik**: Dimensi fisik sistem transmisi juga harus dipertimbangkan. Hal ini terutama berlaku, sekali lagi, dalam kasus sistem kabel. Tentu saja, beratnya sistem kabel harus dianggap sebagai salah satu upaya untuk menerapkannya secara efektif. Selain itu, ukuran besar (diameter) kabel juga penting, karena ruang saluran dan jalur balap sering kali mahal. Dimensi fisik sistem gelombang udara juga harus dipertimbangkan, karena ukuran dan berat piringan reflektif dan sistem pemasangan (misalnya braket dan menara) mungkin memerlukan dukungan.
- **Biaya dan kemudahan Instalasi**: Masalah biaya sering terjadi dalam pemilihan media transmisi yang tepat. Permasalahan tersebut mencakup biaya akuisisi, penerapan, pengoperasian, dan pemeliharaan (O&M), serta peningkatan atau penggantian. Tanpa diskusi panjang mengenai setiap masalah biaya, penting untuk membandingkan biaya penerapan media kabel dan nirkabel. Sistem transmisi kabel memerlukan jalur yang benar dan ini harus diamankan. Transmisi kabel melibatkan komponen biaya berupa infrastruktur. Prasarananya meliputi penggalian parit dan pembuatan lubang agar kabel dapat ditarik dan tiang dapat dipasang. Selain itu, amplifier atau repeater dapat ditempatkan. Biaya seperti ini bukanlah hal yang sepele. Tidak seperti sistem kabel, sistem nirkabel memerlukan jalur dan antena yang aman. Dapat disimpulkan bahwa penerapan sistem kabel tentunya menimbulkan serangkaian masalah biaya yang seringkali menjadi lebih bermasalah.
- **Kriteria pemilihan**: Ketika memilih media transmisi yang paling efektif, pertimbangkan karakteristik transmisi yang disebutkan di atas yang tercantum di bawah ini:

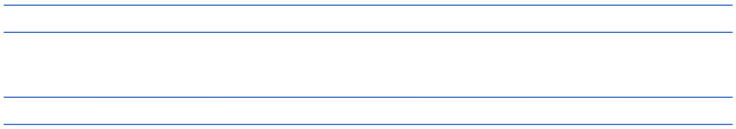
- Bandwidth/Tingkat Transmisi
- Wahai Jarak
- Keterlambatan propagasi
- Wahai Keamanan
- Ketahanan terhadap kondisi lingkungan
- HAI Dimensi fisik
- Biaya dan kemudahan pemasangan

## 3.2 MEDIA YANG DIBATASI

Media terikat atau sistem transmisi kabel menggunakan media fisik yang berwujud. Juga dikenal sebagai sistem konduksi, media kabel umumnya menggunakan konduktor logam atau kaca yang berfungsi untuk menghantarkan, suatu bentuk energi elektromagnetik. Misalnya, sistem kabel twisted pair dan koaksial menghantarkan energi listrik menggunakan media tembaga. Sistem serat optik menghantarkan cahaya atau energi optik, umumnya menggunakan konduktor kaca. Istilah media yang dibatasi atau dipandu berarti bahwa sinyal terkandung dalam jalur fisik tertutup. Hal ini juga mengacu pada fakta bahwa beberapa bentuk pelindung, kelongsong, dan/atau insulasi digunakan untuk mengikat sinyal di dalam media inti, sehingga meningkatkan kekuatan sinyal dalam jarak jauh dan meningkatkan kinerja sistem transmisi dalam prosesnya. Sistem kabel twisted pair (tidak berpelindung dan berpelindung), sistem kabel koaksial dan serat optik termasuk dalam kategori ini.

**Twisted Pair (Konduktor Tembaga)**

Twisted pair seperti terlihat pada Gambar 3.1 adalah sepasang kawat tembaga dengan diameter 0,4-0,8 mm, dipilin menjadi satu dan dibungkus dengan lapisan plastik. Memutar meningkatkan kekebalan kebisingan listrik, dan mengurangi tingkat kesalahan transmisi data. Setiap konduktor diisolasi secara terpisah oleh zat tahan asap dan api yang rendah. Polietilen, polivinil klorida, resin flouropolimer dan Teflon adalah beberapa zat yang digunakan untuk tujuan isolasi.



**Gambar 3.1 Garis Terbuka 2 Kabel**

Proses puntiran ini berfungsi untuk meningkatkan kinerja medium dengan menahan medan elektromagnetik di dalam pasangan. Dengan demikian, radiasi energi elektromagnetik berkurang dan kekuatan sinyal di dalam kabel ditingkatkan dari jarak jauh. Jelasnya, pengurangan energi radiasi ini juga berfungsi untuk meminimalkan dampak pada pasangan kabel yang berdekatan dalam konfigurasi beberapa kabel. Hal ini sangat penting dalam aplikasi bandwidth tinggi, karena sinyal frekuensi tinggi cenderung kehilangan daya lebih cepat seiring jarak. Selain itu, medan elektromagnetik yang terpancar cenderung lebih besar pada frekuensi

yang lebih tinggi, sehingga berdampak lebih besar pada pasangan yang berdekatan. Secara umum, semakin banyak lilitan per kaki, semakin baik kinerja kawatnya.

Ini populer untuk jaringan telepon. Aliran energinya ada pada media terpandu. Kabel logam digunakan hampir secara eksklusif dalam jaringan telekomunikasi selama 90 tahun terakhir, hingga berkembangnya sistem komunikasi gelombang mikro dan radio satelit. Oleh karena itu, kawat tembaga kini menjadi teknologi yang matang, kokoh dan murah. Dalam aplikasi tertentu, digunakan konduktor baja berlapis tembaga, paduan tembaga, tembaga berlapis nikel dan/atau emas, dan bahkan logam aluminium.

Kecepatan transmisi maksimum dibatasi dalam hal ini. Konduktor tembaga yang membawa data analog dapat digunakan untuk membawa data digital juga jika dihubungkan dengan modem. Modem merupakan suatu alat untuk mengubah sinyal digital menjadi sinyal analog dan sebaliknya. Kecepatan data dalam kategori ini dibatasi sekitar 28 Kbps. Pengenalan Jaringan Digital Layanan Terpadu (ISDN) mengarah pada penggunaan skema modulasi dan pengkodean yang lebih baik serta kecepatan data hingga 128 Kbps. Jaringan Area Lokal (LAN) juga menggunakan twisted pair. Jaringan ini juga ditingkatkan untuk mendukung multimedia real-time dengan kecepatan bit tinggi. Teknologi Asymmetric Digital Subscriber Lines (ADSL) ditujukan untuk menggunakan dua loop kawat tembaga dengan kecepatan data 1,544 Mbps dalam jaringan ke arah pengguna dan sekitar 600 Kbps dari pengguna ke jaringan. Kabel twisted pair dapat didefinisikan dalam dua kategori berdasarkan pelindung dan tanpa pelindung.

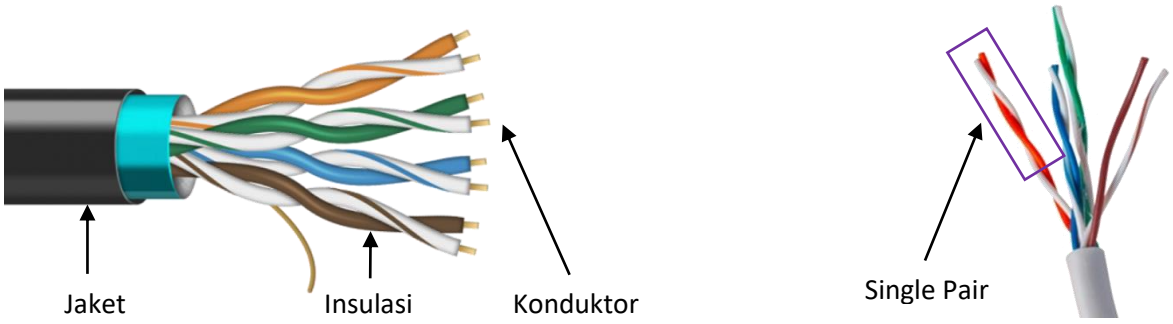
**Pasangan Berpilin Tanpa Pelindung (UTP)**

UTP seperti digambarkan pada Gambar 3.2 adalah media tembaga, yang diwarisi dari telepon, yang digunakan untuk kecepatan data yang semakin tinggi, dan dengan cepat menjadi standar de facto untuk kabel horizontal. Pengkabelan horizontal menentukan sambungan antara, dan termasuk, stopkontak dan terminasi di ruang komunikasi. Horizontalnya dibatasi maksimal 90 meter. Hal ini tidak bergantung pada jenis media sehingga ruang komunikasi bersifat umum untuk semua media dan semua aplikasi yang beroperasi melalui media tersebut. Selain itu, terdapat kelonggaran 3 meter di area kerja dan 6 meter untuk cross connection di lemari sehingga totalnya 99 meter.

Media dan konektor yang direkomendasikan untuk horizontal adalah sebagai berikut:

- Pasangan terpilin tak berpelindung 100 ohm - 4 pasang, konektor modular 8-pin (ISDN)
- Pasangan terpilin berpelindung 150 ohm - 2 pasang (konektor IBM atau RJ45)
- coax 50 ohm (tipis) - IEEE 10BASE2, konektor BNC standar
- Serat multi mode 62,5/125

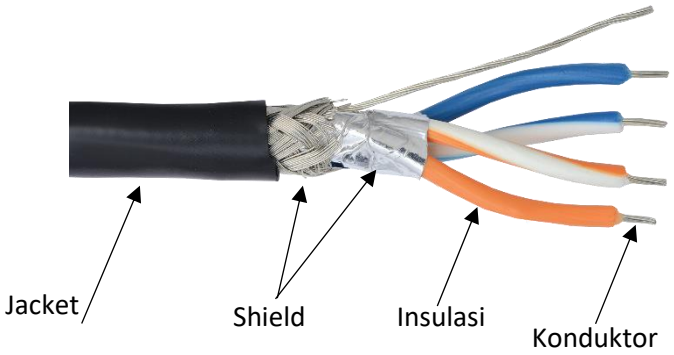
Kabel UTP berisi 2 hingga 4200 pasangan terpilin. Kelebihan UTP adalah fleksibilitas, biaya media yang rendah, dan dapat digunakan baik untuk komunikasi suara maupun data. Kerugian terbesarnya adalah terbatasnya bandwidth, yang membatasi transmisi jarak jauh dengan tingkat kesalahan yang rendah.




**Gambar 3.2 Unshieded Twisted Pair (UTP)**

**Tembaga Terlindung atau STP**

Pasangan terpilin terlindung (STP) berbeda dari UTP karena pelindung atau layar logam mengelilingi pasangan, yang mungkin terpelintir atau tidak. Seperti diilustrasikan pada Gambar 3.3, pasangan tersebut dapat dilindungi secara individual. Sebuah pelindung tunggal dapat mengelilingi kabel yang berisi beberapa pasang atau kedua teknik dapat digunakan secara bersamaan. Perisainya sendiri terbuat dari aluminium, baja, atau tembaga. Ini berbentuk foil logam atau jaring anyaman dan dibumikan secara listrik. Meskipun kurang efektif, pelindungnya terkadang berupa lapisan nikel dan/atau emas pada masing-masing konduktor.




**Gambar 3.3 konfigurasi Kabel Shielded Twisted Pair (STP)**

Tembaga terlindung menawarkan keuntungan berupa peningkatan kinerja karena alasan pengurangan emisi dan pengurangan interferensi elektromagnetik. Pengurangan emisi menawarkan keuntungan dalam menjaga kekuatan sinyal melalui pengurungan medan elektromagnetik di dalam konduktor. Dengan kata lain, kehilangan sinyal berkurang. Manfaat tambahan dari pengurangan emisi ini adalah sinyal frekuensi tinggi tidak menimbulkan interferensi pada pasangan atau kabel yang berdekatan. Kekebalan terhadap interferensi diwujudkan melalui proses pelindung, yang mencerminkan kebisingan elektromagnetik dari sumber luar, seperti motor listrik, kabel dan kabel lainnya, dan sistem radio.

Sebaliknya, twisted pair terlindung memiliki beberapa kelemahan. Pertama, biaya perolehan bahan baku lebih besar karena biaya produksi media lebih mahal. Kedua, biaya penerapannya lebih besar karena bobot tambahan dari perisai membuatnya lebih sulit untuk

diterapkan. Selain itu, pengardean listrik pada pelindung memerlukan lebih banyak waktu dan tenaga.

**Sifat Umum Twisted Pair**

- **Gauge**: Gauge adalah ukuran ketebalan konduktor. Semakin tebal kabelnya, semakin kecil resistansinya, semakin kuat sinyalnya pada jarak tertentu, dan semakin baik kinerja medianya. Kabel yang lebih tebal juga memberikan keuntungan berupa kekuatan putus yang lebih besar. Nomor pengukur bersifat retrogresif. Dengan kata lain, semakin besar angkanya, semakin kecil konduktornya.
- **Konfigurasi**: Dalam konfigurasi pasangan tunggal, pasangan kabel dibungkus dalam selubung atau jaket yang terbuat dari polietilen, polivinil klorida, atau Teflon. Biasanya, beberapa pasangan dibundel untuk meminimalkan biaya penerapan yang terkait dengan menghubungkan beberapa perangkat (misalnya, perangkat telepon PBX atau KTS elektronik, terminal data, dan modem) di satu stasiun kerja.
- **Bandwidth**: Kapasitas efektif kabel twisted pair tergantung pada beberapa faktor, termasuk ukuran konduktor, panjang rangkaian dan jarak amplifier/repeater. Kita juga harus menyadari bahwa aplikasi bandwidth tinggi (frekuensi tinggi) dapat menyebabkan interferensi dengan sinyal lain pada pasangan lain yang berdekatan.
- **Kinerja Kesalahan**: Kualitas sinyal selalu penting, terutama yang berhubungan dengan transmisi data. Pasangan terpilin (twisted pair) sangat rentan terhadap dampak interferensi dari luar, karena kawat berisolasi tipis bertindak sebagai antena dan, dengan demikian, menyerap sinyal-sinyal yang salah tersebut. Sumber potensial Interferensi Elektro Magnetik (EMI) meliputi motor listrik, transmisi radio, dan kotak lampu neon. Ketika frekuensi transmisi meningkat, kinerja kesalahan tembaga menurun secara signifikan dengan redaman sinyal meningkat kira-kira sebesar akar kuadrat frekuensi.
- **Jarak**: Twisted pair memiliki jarak yang terbatas. Ketika jarak antar elemen jaringan meningkat, redaman (kehilangan sinyal) meningkat dan kualitas menurun pada frekuensi tertentu. Ketika bandwidth meningkat, frekuensi pembawa meningkat, redaman menjadi lebih menjadi masalah, dan amplifier/repeater harus ditempatkan lebih dekat.
- **Keamanan**: Twisted pair pada dasarnya merupakan media transmisi yang tidak aman. Relatif mudah untuk memasang tap fisik pada UTP. Selain itu, energi yang dipancarkan mudah dicegat melalui penggunaan antena atau kumparan induktif, tanpa memerlukan penempatan keran fisik.
- **Biaya**: Biaya akuisisi, penerapan dan penataan ulang UTP sangat rendah, setidaknya dalam aplikasi kabel dalam. Namun, dalam aplikasi berkapasitas tinggi dan jarak jauh, seperti trunking antar kantor, biaya relatifnya sangat tinggi, karena persyaratan untuk pembuatan parit atau pengeboran, penempatan saluran, dan penyambungan kabel multi-pasangan yang besar. Selain itu, terdapat batasan terbatas terhadap kapasitas dan karakteristik kinerja UTP lainnya, terlepas dari daya cipta para ahli teknologi. Oleh karena itu, popularitas alternatif seperti microwave dan kabel serat optik.

- **Aplikasi**: Biaya rendah UTP termasuk metode yang dikembangkan baru-baru ini untuk meningkatkan kinerjanya telah meningkatkan penerapannya dalam sistem distribusi jarak pendek atau aplikasi kabel dalam. Aplikasi saat ini dan yang berkelanjutan mencakup loop lokal, kabel dan kabel dalam, dan terminal-ke-LAN. Secara umum, UTP tidak lagi digunakan dalam sistem transmisi jarak jauh atau di luar lokasi.

Biaya tambahan dari tembaga berpelindung membatasi penerapannya pada aplikasi kawat dalam. Secara khusus, umumnya terbatas pada penerapan di lingkungan dengan kebisingan tinggi. Ini juga digunakan di mana sinyal frekuensi tinggi ditransmisikan dan ada kekhawatiran tentang kinerja jarak atau gangguan dengan pasangan yang berdekatan. Contohnya termasuk LAN dan transmisi gambar.

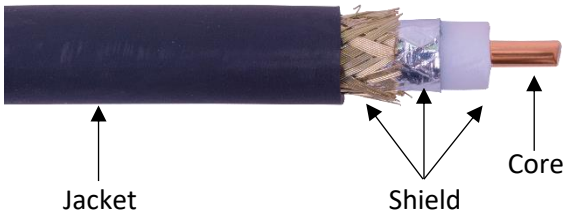
**Kabel Koaksial**

Faktor pembatas utama kabel twisted pair disebabkan oleh fenomena yang disebut efek kulit. Ketika frekuensi sinyal yang ditransmisikan meningkat, arus yang mengalir dalam kabel cenderung mengalir hanya pada permukaan luar kabel, sehingga menggunakan lebih sedikit penampang yang tersedia. Hal ini meningkatkan hambatan listrik kabel untuk sinyal frekuensi lebih tinggi yang menyebabkan redaman lebih tinggi. Selain itu, pada frekuensi yang lebih tinggi, lebih banyak kekuatan sinyal yang hilang akibat efek radiasi. Oleh karena itu untuk aplikasi yang memerlukan frekuensi lebih tinggi, jenis media transmisi lain harus digunakan. Kabel koaksial meminimalkan kedua efek ini.

Kabel Koaksial seperti yang ditunjukkan pada Gambar 3.4 adalah kabel dua konduktor kawat tembaga berpelindung yang sangat kuat di mana konduktor tengah padat berjalan secara konsentris (koaksial) di dalam konduktor melingkar luar padat. Ini membentuk perisai elektromagnetik di sekelilingnya yang berfungsi untuk meningkatkan kekuatan dan integritas sinyal. Kedua konduktor dipisahkan oleh isolasi. Lapisan bahan dielektrik (nonkonduktif), seperti PVC atau Teflon kemudian melindungi seluruh kabel.

Itu termasuk dalam kategori media terbatas dan masih merupakan media yang efektif untuk digunakan dalam komunikasi data. Kabel koaksial dilengkapi pelindung untuk meningkatkan kinerja dan oleh karena itu harganya mahal. Jaringan TV kabel menggunakan kabel koaksial. Jaringan Area Lokal dapat beroperasi melalui kabel koaksial dengan spesifikasi 10BASE5, 10BASE2 dan 10BASET. Secara umum, kabel koaksial memungkinkan transmisi jarak jauh dengan kecepatan data lebih tinggi dibandingkan kabel twisted pair namun lebih mahal. Ada dua jenis kabel koaksial:

- **Baseband**: Mengirimkan sinyal tunggal pada satu waktu dengan kecepatan sangat tinggi. Sinyal pada kabel baseband harus diperkuat pada jarak tertentu. Ini digunakan untuk jaringan area lokal.
- **Broadband**: Dapat mengirimkan banyak sinyal secara simultan menggunakan frekuensi berbeda.



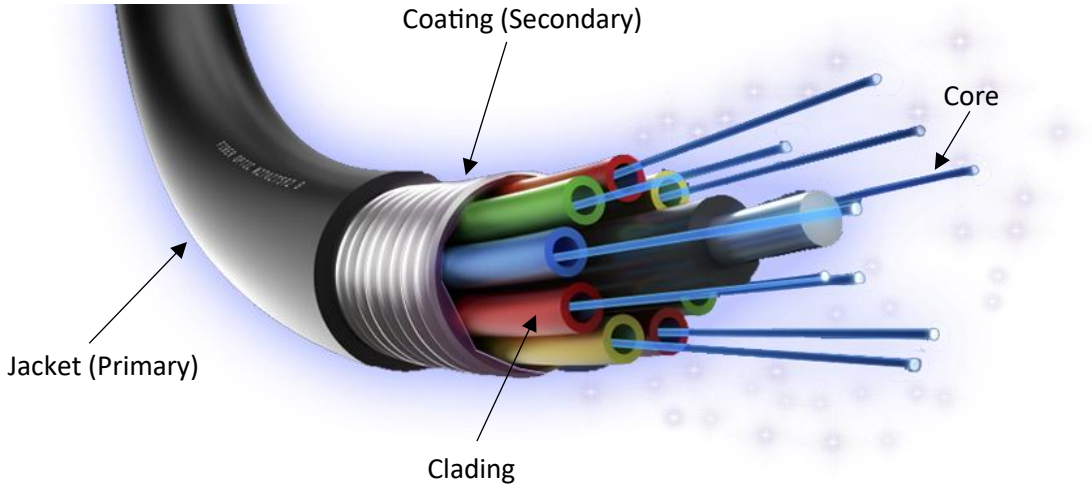

**Gambar 3.5 Konfigurasi Kabel Koaksial**

**Sifat Umum Kabel Koaksial**

- **Gauge**: Ukuran kabel koaksial lebih tebal dibandingkan kabel twisted pair. Meskipun hal ini meningkatkan bandwidth yang tersedia dan jarak transmisi, hal ini juga meningkatkan biaya. Kabel koaksial tradisional cukup tebal, berat dan besar seperti Ethernet LAN 10Base5 sebagai contohnya. Ethernet LAN 10Base2 memiliki dimensi yang jauh lebih kecil tetapi menawarkan kinerja yang lebih rendah.
- **Konfigurasi**: Kabel koaksial terdiri dari kawat tunggal dua konduktor, dengan konduktor tengah dan pelindung/konduktor luar, yang terbuat dari logam padat. Terkadang logam yang dikepang atau dipilin digunakan. Kabel aksial kembar berisi dua konfigurasi seperti itu dalam satu selubung kabel. Karena konduktor tengah membawa sinyal pembawa dan konduktor luar umumnya digunakan untuk grounding listrik. Konektivitas kabel koaksial dapat diperluas melalui penggunaan pasangan terpilin dengan konektor BALUN (BALanced/UNbalanced) yang berfungsi untuk mencapai antarmuka.
- **Bandwidth**: Kapasitas efektif kabel koaksial bergantung pada beberapa faktor, termasuk ukuran konduktor tengah, panjang rangkaian, dan jarak amplifier serta perangkat perantara lainnya. Bandwidth yang tersedia melalui kabel koaksial sangat signifikan; oleh karena itu digunakan dalam aplikasi berkapasitas tinggi, seperti transmisi data dan gambar.
- **Kinerja Kesalahan**: Kabel koaksial berkinerja sangat baik karena adanya pelindung luar. Oleh karena itu, sering digunakan dalam aplikasi data.
- **Jarak**: Kabel koaksial tidak sebatas UTP, meskipun amplifier atau perangkat perantara lainnya harus digunakan untuk memperluas transmisi frekuensi tinggi pada jarak yang signifikan.
- **Keamanan**: Kabel koaksial pada dasarnya cukup aman. Relatif sulit untuk memasang keran fisik pada kabel koaksial. Radiasi energinya juga minim sehingga intersepsi terhadapnya tidak mudah.
- **Biaya**: Biaya perolehan, penempatan, dan penataan ulang kabel koaksial sangat tinggi dibandingkan dengan UTP. Namun, dalam aplikasi data berkapasitas tinggi, biaya tersebut sering kali tidak sebanding dengan karakteristik kinerja positifnya.
- **Aplikasi**: Karakteristik kinerja kabel koaksial yang unggul menjadikannya media favorit dalam banyak aplikasi data jarak pendek dan intensif bandwidth. Aplikasi saat ini dan yang berkelanjutan mencakup tulang punggung LAN, host-to-host, host-to-peripheral dan CATV.

**Serat Optik**

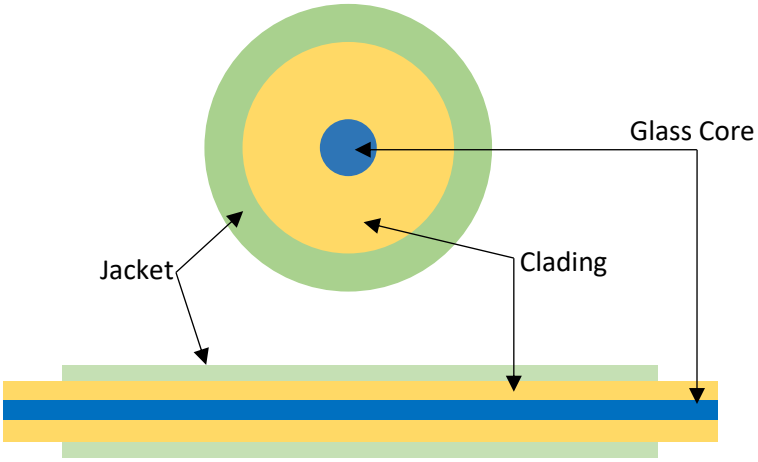
Kita telah melihat di bagian sebelumnya bahwa geometri kabel koaksial secara signifikan mengurangi berbagai efek pembatas, frekuensi sinyal maksimum, dan karenanya kecepatan informasi yang dapat ditransmisikan menggunakan konduktor padat, meskipun sangat tinggi, namun terbatas. Hal ini juga terjadi pada garis yang bengkok. Serat optik berbeda dari kedua media transmisi ini karena serat optik membawa informasi yang dikirimkan dalam bentuk berkas cahaya yang berfluktuasi dalam serat kaca, bukan sebagai sinyal listrik pada kabel. Jenis transmisi ini telah menjadi pendukung kuat jaringan digital karena kapasitasnya yang tinggi dan faktor-faktor lain yang mendukung komunikasi digital.




**Gambar 3.5 Struktur Fiber Optic**

Sistem transmisi serat optik bersifat opto-listrik. Dengan kata lain, kombinasi energi elektromagnetik optik dan listrik terlibat. Sinyal tersebut berasal dari sinyal listrik, yang diterjemahkan menjadi sinyal optik, yang kemudian diubah kembali menjadi sinyal listrik di sisi penerima. Serat kaca tipis seperti yang ditunjukkan pada Gambar 3.5 sangat jernih dan dirancang untuk memantulkan cahaya secara internal untuk transmisi yang efisien membawa cahaya dengan data yang dikodekan. Jaket plastik memungkinkan serat menekuk (sebagian!) tanpa putus. Dioda pemancar cahaya (LED) atau laser menyuntikkan cahaya ke dalam serat untuk transmisi. Penerima peka cahaya di ujung lain menerjemahkan cahaya kembali menjadi data.

Serat optik terdiri dari sejumlah substruktur seperti yang ditunjukkan pada Gambar 3.6. Dalam hal ini, lapisan kaca dengan indeks bias lebih rendah mengelilingi inti kaca, yang membawa sebagian besar cahaya. Ini membelokkan cahaya dan membatasinya pada inti. Inti dikelilingi oleh lapisan substrat (pada beberapa serat) kaca, yang tidak membawa cahaya, namun menambah diameter dan kekuatan serat. Lapisan penyangga primer dan lapisan penyangga sekunder untuk memberikan perlindungan mekanis menutupi semua ini.

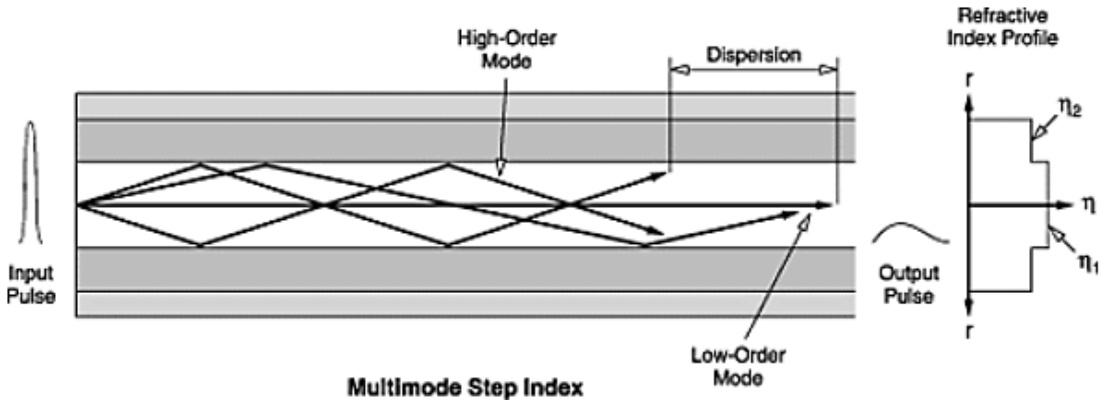



**Gambar 3.6 Kabel Fiber Optic, Tampak Penampang Samping**

Pulsa cahaya merambat ke inti tengah serat kaca. Di sekeliling inti bagian dalam terdapat lapisan pelapis kaca, dengan indeks bias yang sedikit berbeda. Kelongsong berfungsi untuk memantulkan gelombang cahaya kembali ke inti bagian dalam. Di sekeliling kelongsong terdapat lapisan lapisan plastik pelindung yang menyegel kabel dan memberikan perlindungan mekanis. Hal ini ditunjukkan pada Gambar 3.6. Biasanya, beberapa serat ditempatkan dalam satu selubung, yang mungkin berlapis baja. Cahaya merambat sepanjang inti serat optik melalui salah satu cara berikut, tergantung pada jenis dan lebar bahan inti yang digunakan.

**Serat Multimode**

Di sini, diameter inti relatif besar dibandingkan dengan panjang gelombang cahaya. Diameter inti berkisar antara 50 mikrometer (µm) hingga 1.000 µm, dibandingkan dengan panjang gelombang cahaya sekitar 1 µm. Ini berarti bahwa cahaya dapat merambat melalui serat dalam banyak jalur atau mode sinar yang berbeda, oleh karena itu dinamakan multimode. Serat multimode lebih murah untuk diproduksi dan kinerjanya lebih rendah karena diameter inti bagian dalam yang lebih besar. Ketika sinar cahaya merambat ke serat, sinar tersebut menyebar karena fenomena yang dikenal sebagai dispersi modal. Meskipun dipantulkan kembali ke inti bagian dalam melalui kelongsongnya, mereka menempuh jarak yang berbeda dan, oleh karena itu, tiba pada waktu yang berbeda. Dengan demikian, sinyal yang diterima memiliki lebar pulsa yang lebih lebar daripada sinyal input dengan penurunan kecepatan transmisi yang sesuai. Akibatnya, serat multimode diturunkan ke aplikasi yang melibatkan jarak yang relatif pendek dan kecepatan transmisi yang lebih rendah, misalnya LAN dan lingkungan kampus. Ada dua tipe dasar serat multimode. Jenis yang lebih sederhana dan lebih tua adalah serat “step index”, di mana indeks bias (kemampuan suatu bahan untuk membelokkan cahaya) adalah sama di seluruh inti serat.



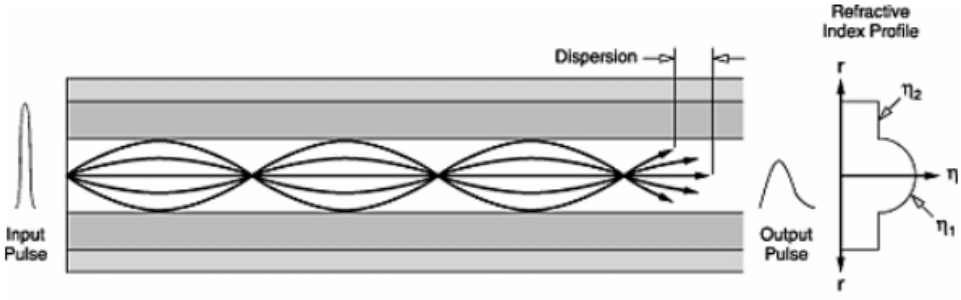

**Gambar 3.7 Multimode Step Indeks**

Hal ini ditunjukkan pada Gambar 3.7. Dengan semua jalur sinar atau mode propagasi yang berbeda ini, sinar yang berbeda menempuh jarak yang berbeda, dan memerlukan waktu yang berbeda pula untuk melintasi panjang serat. Oleh karena itu, jika pulsa cahaya pendek diinjeksikan ke dalam serat, berbagai sinar yang memancar dari pulsa tersebut akan tiba di ujung serat yang lain pada waktu yang berbeda, dan pulsa keluaran akan berdurasi lebih lama dibandingkan pulsa masukan. . Fenomena ini disebut “modal dispersion” (penyebaran pulsa), dan membatasi jumlah pulsa per detik yang dapat ditransmisikan melalui serat dan masih dapat dikenali sebagai pulsa terpisah di ujung lainnya. Oleh karena itu, hal ini membatasi bit rate atau bandwidth serat multimode. Untuk serat indeks langkah, dimana tidak ada upaya yang dilakukan untuk mengkompensasi dispersi modal, bandwidth biasanya 20 sampai 30 MHz pada panjang serat satu kilometer, dinyatakan sebagai “MHz - km”.

**Serat Multimode Indeks Bertingkat**

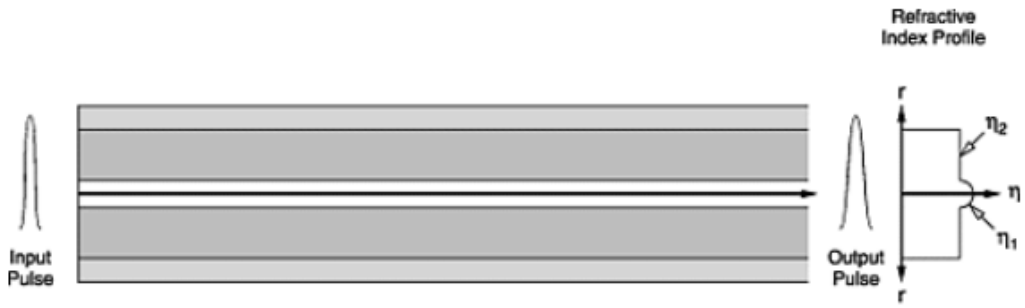
Dalam kasus serat multimode indeks bergradasi, indeks bias di seluruh inti diubah secara bertahap dari maksimum di pusat menjadi minimum di dekat tepi, oleh karena itu dinamakan indeks bergradasi. Desain ini memanfaatkan fenomena bahwa cahaya merambat lebih cepat pada material dengan indeks bias rendah dibandingkan pada material dengan indeks bias tinggi. Jika pulsa cahaya pendek diluncurkan ke dalam serat indeks bergradasi, gelombang cahaya tersebut mungkin akan menyebar selama transit serat tersebut, namun jauh lebih sedikit dibandingkan dengan serat indeks bertahap. Oleh karena itu, dispersi dapat dikurangi dengan menggunakan bahan inti yang memiliki indeks bias variabel. Dalam indeks multimode, cahaya serat dibiaskan dengan jumlah yang semakin besar ketika menjauh dari inti seperti yang ditunjukkan pada Gambar 3.8. Hal ini memiliki efek mempersempit lebar pulsa dari sinyal yang diterima dibandingkan dengan serat indeks bertahap, sehingga memungkinkan peningkatan kecepatan transmisi. Oleh karena itu, mereka dapat mendukung bit rate atau bandwidth yang jauh lebih tinggi.

Tahukah kamu? Bandwidth khas serat indeks bertingkat berkisar dari 100 MHz-km hingga lebih dari 1GHz-km. Bandwidth sebenarnya bergantung pada seberapa baik profil indeks serat tertentu meminimalkan dispersi modal, dan pada panjang gelombang cahaya yang diluncurkan ke serat.




**Gambar 3.8 Multimode Granded Indeks**

Serat Monomode/Singlemode: Ini memiliki inti bagian dalam yang lebih tipis. Dalam hal ini, diameter inti sekitar 9 µm jauh lebih dekat ukurannya dengan panjang gelombang cahaya yang disebarkan, sekitar 1,3 µm. Hal ini membatasi transmisi cahaya menjadi satu sinar atau mode cahaya yang merambat ke inti serat seperti yang ditunjukkan pada Gambar 3.9. Semua efek multi-mode atau multimode yang dijelaskan di atas dihilangkan. Namun, masih ada satu mekanisme penyebaran denyut nadi. Sama seperti pada serat multimode, panjang gelombang cahaya yang berbeda merambat dengan kecepatan berbeda, menyebabkan gelombang cahaya pendek yang disuntikkan ke dalam serat menyebar saat merambat. Fenomena ini disebut “dispersi kromatik”.




**Gambar 3.9 Propagasi step indeks Single mode**

Ia berkinerja lebih baik daripada serat multimode pada jarak yang lebih jauh dengan tingkat transmisi yang lebih tinggi. Karena berkurangnya diameter inti, semua cahaya yang dipancarkan merambat sepanjang satu jalur. Akibatnya sinyal yang diterima memiliki lebar yang sebanding dengan sinyal masukan. Meskipun lebih mahal, serat monomode digunakan untuk keuntungan dalam jangka panjang, dan terutama dalam aplikasi bandwidth tinggi.

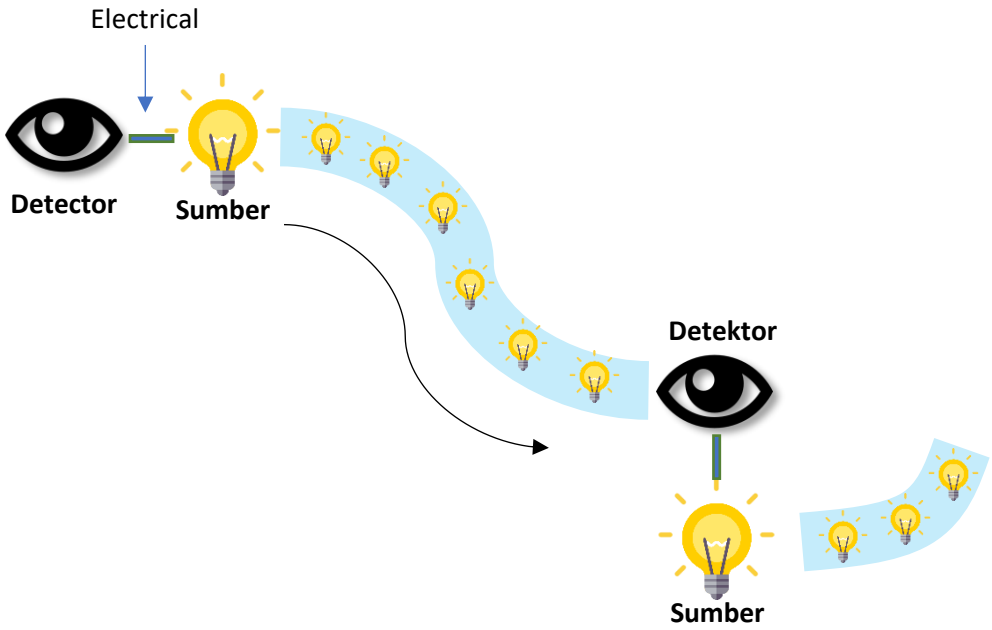
**Keunggulan Serat Optik**

- Kekebalan terhadap interferensi elektromagnetik dan crosstalk
- Tidak ada masalah ground loop atau korsleting listrik
- Ukuran kecil dan ringan
- Bandwidth besar untuk ukuran dan berat
- Aman di area yang mudah terbakar (tidak melengkung)
- Kekebalan terhadap petir dan muatan listrik
- Kabel yang lebih panjang antar repeater

- ❖ Fleksibilitas dan kekuatan tinggi
- ❖ Potensi pengoperasian pada suhu tinggi
- ❖ Aman dari kebocoran sinyal dan gangguan
- ❖ Tidak ada bahaya listrik jika terpotong atau rusak.

**Sifat Umum Serat Optik**

- **Konfigurasi**: Sistem serat optik terdiri dari sumber cahaya, kabel dan detektor cahaya, seperti digambarkan pada Gambar 3.10. Dalam konfigurasi sederhana, masing-masing digunakan. Dalam konfigurasi yang lebih kompleks pada jarak yang lebih jauh, banyak kumpulan elemen yang digunakan. Seperti halnya sistem transmisi lainnya, komunikasi optik jarak jauh melibatkan sejumlah repeater regeneratif. Dalam sistem serat optik, repeater adalah perangkat opto-listrik. Di sisi masuk repeater, detektor cahaya menerima sinyal optik, mengubahnya menjadi sinyal listrik, memperkuatnya, mengubahnya kembali menjadi sinyal optik, dan menempatkannya ke serat, dan seterusnya. Mungkin terdapat banyak repeater optik dalam sistem transmisi jarak jauh, meskipun biasanya jauh lebih sedikit daripada yang dibutuhkan menggunakan media transmisi lainnya.




**Gambar 3.10 Sistem Fiber Optic**

- **Bandwidth**: Fiber menawarkan bandwidth terbesar sejauh ini dibandingkan sistem transmisi mana pun, seringkali melebihi 2 Gbps pada jaringan operator jarak jauh. Sistem dengan 40 Gbps telah berhasil diuji pada banyak kesempatan. Kapasitas teoritis serat berada pada kisaran terabit (Tbps), dengan kapasitas serat monomode saat ini dapat diperluas ke tingkat tersebut.
- **Kinerja Kesalahan**: Serat bersifat dielektrik (nonkonduktor arus listrik searah), sehingga tidak rentan terhadap Interferensi Elektro Magnetik/Interferensi Frekuensi Radio (EMI/RFI). Ini juga tidak memancarkan EMI/RFI. Sinyal cahaya akan mengalami

redaman, meskipun lebih sedikit dibandingkan media lainnya. Hamburan sinyal optik, pembengkokan kabel serat, penerjemahan energi cahaya menjadi panas, dan sambungan pada sistem kabel dapat menyebabkan redaman optik tersebut.

- **Jarak**: Sistem serat optik monomode secara rutin mampu mentransmisikan sinyal pada jarak lebih dari 325 km. Oleh karena itu, relatif sedikit repeater optik yang diperlukan dalam sistem jarak jauh. Hal ini akan mengurangi biaya dan menghilangkan titik-titik potensi kegagalan.
- **Keamanan**: Fiber secara intrinsik aman, karena hampir tidak mungkin memasang keran fisik tanpa terdeteksi karena tidak ada cahaya yang terpancar di luar kabel. Oleh karena itu, intersepsi sinyal hampir tidak mungkin dilakukan. Selain itu, sistem serat optik mendukung volume lalu lintas yang begitu tinggi sehingga sulit untuk mencegat dan membedakan satu transmisi dari puluhan ribu transmisi lain yang mungkin menggunakan sistem kabel yang sama. Sifat digital dari sebagian besar serat ditambah dengan teknik enkripsi yang sering digunakan untuk melindungi dari intersepsi membuat serat menjadi sangat aman.
- **Biaya**: Meskipun biaya perolehan, penerapan, dan penataan ulang fiber relatif tinggi, bandwidth yang besar dapat melebihi biaya tersebut dalam aplikasi yang membutuhkan banyak bandwidth. Pada kecepatan Gbps, satu set serat dapat membawa transmisi digital dalam jumlah besar dalam jarak yang lebih jauh dibandingkan sistem alternatif, sehingga menurunkan biaya transportasi per bit dan biaya per percakapan hingga sepersekian sen per menit.
- **Aplikasi**: Aplikasi untuk sistem transmisi serat optik memerlukan bandwidth yang intensif. Aplikasi tersebut mencakup jaringan pembawa tulang punggung, kabel bawah laut internasional, LAN tulang punggung (FDDI), trunking antar kantor, jaringan distribusi komputer-ke-komputer (CATV dan Information Superhighway) dan serat ke desktop (Computer Aided Design).

**Bagan Perbandingan Media Berbatas**

**Tabel 3.2: Grafik Perbandingan Media Berbatas**

| Media | Kelebihan | Kelemahan |
|---|---|---|
| Kabel Twisted pair | Murah, Mudah diaplikasikan, Mudah untuk menambahkan Node | Sensitif terhadap kebisingan, jarak pendek, bandwidth terbatas, berbahaya karena mudah diretas |
| Kabel Coaxial | Bandwidth Tinggi, Jarak jauh, Kekebalan terhadap Noise | Dimensi fisik, keamanan lebih baik dibandingan kabel twisted pair |
| Kabel Fiber Optic | Bandwidth sangat tinggi, tahan gangguan, komunikasi jarak jauh, keamanan kecil, ukuran kecil | Koneksi dan Biaya |
| Berikan penjelasan singkat mengenai penerapan dan keterbatasan jenis media | | |

transmisi berikut:

1. Two-wire Open Lines
2. Kabel Twisted pair
3. Kabel Koaxial
4. Fiber Optik
5. Microwave

**Ringkasan**

- Ada beberapa macam media transmisi. Teknologi media mulai dari kabel tembaga hingga nirkabel dan serat optik telah berkembang begitu pesat dan menggantikan teknologi lainnya dengan sangat cepat di era informasi ini.
- Media transmisi secara umum dapat diklasifikasikan menjadi dua jenis: Media transmisi terpandu dan tidak terarah.
- Kabel twisted pair, kabel koaksial, dan serat optik termasuk dalam kategori media transmisi terpandu atau terikat.
- Twisted pair adalah sepasang kabel tembaga yang dipilin menjadi satu dan dibungkus dengan lapisan plastik. Ini terutama terdiri dari dua jenis: pasangan terpilin terlindung (STP) dan pasangan terpilin tidak terlindung (UTP).
- Shielded twisted pair (STP) berbeda dengan UTP karena terdapat pelindung atau layar logam yang mengelilingi pasangan tersebut, yang dapat dipelintir atau tidak.
- Kabel Koaksial adalah kabel dua konduktor kawat tembaga berpelindung yang sangat kuat di mana konduktor tengah padat berjalan secara konsentris (koaksial) di dalam konduktor melingkar luar padat.
- Serat optik membawa informasi yang dikirimkan dalam bentuk berkas cahaya yang berfluktuasi dalam serat kaca dan bukan sebagai sinyal listrik pada kabel. Ini dapat terdiri dari dua jenis: serat monomode dan multimode.

**Latihan Soal**

Isilah bagian yang kosong:

1) ..... secara garis besar dapat dikategorikan menjadi terbimbing dan media yang tidak terarah.
2) Rentang frekuensi sebenarnya yang mendukung komunikasi tertentu disebut .....
3) Secara umum, semakin tinggi ....., semakin besar pula kecepatan transmisi data atau throughputnya.
4) .....mengacu pada lamanya waktu yang diperlukan sinyal untuk berpindah dari pemancar ke penerima melalui sistem transmisi.
5) Bandwidth dapat didefinisikan sebagai kisaran ..... yang ditetapkan ke suatu saluran.

Nyatakan apakah pernyataan berikut ini benar atau salah:

1. Sistem kabel twisted pair (tidak berpelindung dan terlindung), koaksial, dan serat optik termasuk dalam kategori media transmisi terpandu.

2. Memutar menurunkan kekebalan kebisingan listrik, dan mengurangi tingkat kesalahan transmisi data.
3. Kabel UTP berisi 2 hingga 4200 pasangan terpilin.
4. Kabel koaksial pada dasarnya merupakan media transmisi yang tidak aman.
5. Jaringan Area Lokal dapat beroperasi melalui kabel koaksial dengan spesifikasi 10BASE5, 10BASE2 dan 10BASET

**Latihan Soal 3.2**

1. Media transmisi apa saja yang dapat digunakan oleh perangkat komunikasi data?
2. Apa batasan utama dari kabel twisted pair?
3. Jelaskan perbedaan komunikasi satelit dengan siaran radio?
4. Penerima dalam sistem serat optik memerlukan daya 5 mikrowatt. Panjang kabel adalah 5 Km dan menawarkan kehilangan atenuasi sebesar 2 dB/km. Ada kerugian sebesar 1 dB pada sumber dan penerima. Hitung tingkat daya optik yang diperlukan pada sumber optik.
5. Nyatakan dengan bantuan diagram berbagai komponen sambungan serat optik yang khas. Sebutkan berbagai komponen kehilangan sinyal.
6. Apa yang dimaksud dengan refleksi? Apa yang terjadi pada seberkas cahaya ketika merambat ke medium yang kurang rapat? Apa yang terjadi jika ia berpindah ke medium yang lebih padat?
7. Apa kelebihan kabel koaksial dibandingkan kabel twisted pair?
8. Bandingkan kabel fiber optic dengan kabel UTP jika digunakan sebagai media transmisi pada LAN.
9. Apa tujuan pelapisan pada serat optik? Diskusikan kepadatannya sehubungan dengan inti.
10. Apa efek kulit dan bagaimana pengaruhnya terhadap kinerja kabel TP?
11. Bagaimana kabel koaksial mengurangi masalah efek kulit dan menjadi media yang tepat untuk transmisi data frekuensi tinggi?
12. Jenis media transmisi apa yang banyak digunakan untuk transmisi digital dan mengapa?

# BAB 4
# JARINGAN NIRKABEL

**Pendahuluan**

Seperti yang Anda ketahui bahwa ada berbagai cara untuk mengirimkan sinyal. Cara-cara ini secara garis besar dapat dikategorikan menjadi media terbimbing dan tidak terarah. Media terpandu mencakup semua media berkabel, disebut juga media terkonduksi atau terikat. Anda telah mempelajari tentang media transmisi terbimbing/terbatas pada unit terakhir. Sekarang di unit ini Anda akan belajar tentang kategori kedua yang mencakup semua media nirkabel tradisional, juga disebut sebagai terpancar, atau tidak terbatas. Dalam transmisi sinyal, data dikodekan menjadi energi dan kemudian energi ditransmisikan. Demikian pula di sisi penerima, energi diterjemahkan kembali menjadi data. Energi ini dapat berupa listrik, cahaya, radio, dan lain-lain. Oleh karena itu, energi yang ditransmisikan ini dibawa melalui suatu media, yang bergantung pada jenis energi yang ditransmisikan. Setiap bentuk energi memiliki sifat dan persyaratan transmisi yang berbeda. Hal ini memerlukan perangkat keras khusus untuk pengkodean data dan koneksi ke media transmisi. Media dapat berupa tembaga, kaca dan udara, dll.

## 4.1 TRANSMISI NIRKABEL

Sistem transmisi nirkabel tidak menggunakan konduktor fisik, atau pemandu, untuk mengikat sinyal. Dalam hal ini, data ditransmisikan menggunakan gelombang elektromagnetik. Oleh karena itu, sistem ini juga dikenal sebagai sistem yang tidak terarah atau tidak terbatas. Energi berpindah melalui udara, bukan melalui tembaga atau kaca. Oleh karena itu istilah terpancar sering diterapkan pada transmisi nirkabel. Terakhir, sistem tersebut menggunakan energi elektromagnetik dalam bentuk gelombang radio atau cahaya yang dikirim dan diterima melintasi ruang angkasa, dan disebut sebagai sistem gelombang udara. Sistem transmisi yang termasuk dalam kategori ini meliputi gelombang mikro, satelit, dan inframerah. Ada beberapa teknik berbeda untuk mengonversi data yang cocok untuk mode komunikasi ini. Secara konseptual mirip dengan radio, TV, telepon seluler, gelombang radio dapat menembus dinding dan menembus seluruh bangunan. Mereka dapat melakukan perjalanan jarak jauh menggunakan komunikasi satelit atau jarak pendek menggunakan komunikasi nirkabel.

Penggunaan teknologi ini untuk pengiriman aplikasi real-time seperti materi multimedia harus dilakukan dengan hati-hati, karena link radio rentan terhadap pemudaran, interferensi, penundaan acak, dll. Penggunaan teknologi ini secara non-real-time kemungkinan besar akan berfungsi sebaik Ethernet saat ini. LAN.

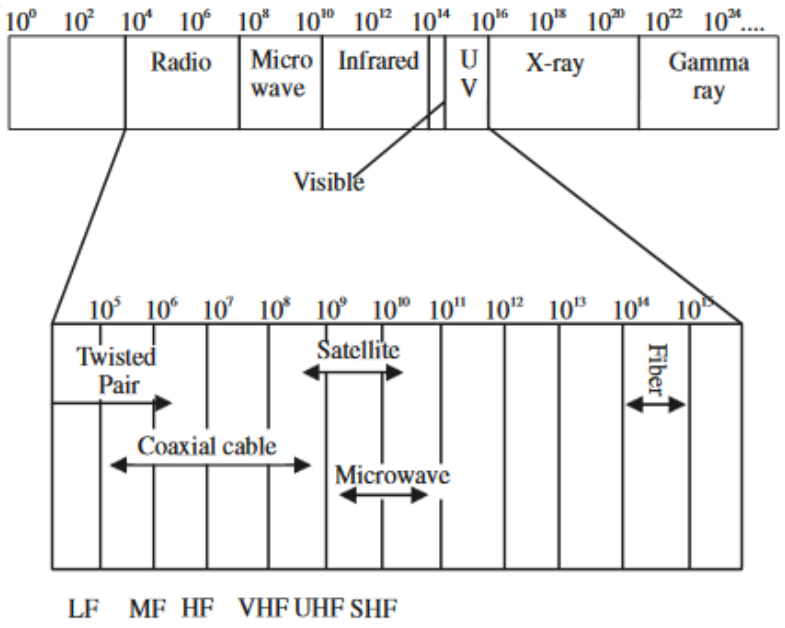
**Radio**

Ini adalah teknik di mana data ditransmisikan menggunakan gelombang radio dan oleh karena itu energi berpindah melalui udara, bukan melalui tembaga atau kaca. Secara konseptual, radio, TV, telepon seluler, dll. menggunakan transmisi radio dalam satu atau lain bentuk. Gelombang radio dapat menembus dinding dan seluruh bangunan. Tergantung pada

frekuensinya, mereka dapat melakukan perjalanan jarak jauh atau jarak pendek. Relai satelit merupakan salah satu contoh komunikasi jarak jauh. Oleh karena itu, setiap rentang frekuensi dibagi menjadi beberapa pita yang berbeda, yang memiliki rentang frekuensi tertentu dalam spektrum Frekuensi Radio (RF). RF dibagi dalam rentang yang berbeda mulai dari Frekuensi Sangat Rendah (VLF) hingga Frekuensi Sangat Tinggi (EHF). Gambar 4.1 menunjukkan setiap pita dengan batas frekuensi atas dan bawah yang ditentukan.

Dua pemancar tidak dapat berbagi pita frekuensi yang sama karena adanya interferensi timbal balik dan oleh karena itu penggunaan pita diatur. Tahukah kamu? Penggunaan spektrum radio secara internasional diatur oleh International Telecommunication Union (ITU). Penggunaan spektrum radio dalam negeri diatur oleh lembaga nasional seperti Perencanaan dan Koordinasi Nirkabel (WPC) di India. WPC menetapkan pita operasi, pola radiasi pemancar, dan daya pemancar maksimum pada setiap sumber transmisi.

Antena omni direction atau pengarah digunakan untuk menyiarkan gelombang radio tergantung pada pitanya. Unit transceiver, yang terdiri dari pemancar dan penerima beserta antena, menentukan kekuatan sinyal RF. Ciri-ciri gelombang radio lainnya adalah dalam ruang hampa semua gelombang elektromagnetik atau gelombang radio merambat dengan kecepatan yang sama yaitu dengan kecepatan cahaya yaitu sebesar 3×108 meter per detik. Dalam media apa pun, kecepatan ini berkurang dan juga bergantung pada frekuensi. Dalam kasus tembaga, kecepatan cahaya menjadi kira-kira dua pertiga kecepatan cahaya.




**Gambar 4.1 Frekuensi Radio dan Tipe Transmisi Data**

Ciri-ciri dasar gelombang radio adalah:

- Mereka mudah dihasilkan
- Kecepatannya sama dalam ruang hampa
- Mereka mungkin menempuh jarak yang jauh

- Mereka bersifat omni direction
- Mereka dapat menembus bangunan dengan mudah sehingga banyak digunakan dalam komunikasi baik di dalam maupun di luar ruangan
- Mereka bergantung pada frekuensi. Pada frekuensi rendah mereka dapat melewati rintangan dengan baik tetapi dayanya menurun tajam seiring dengan jarak dari sumber, karena daya berbanding terbalik dengan pangkat tiga jarak dari sumber. Di HF mereka melakukan perjalanan dalam garis lurus dan memantulkan rintangan.

**Frekuensi Sangat Rendah (VLF)**

Metode VLF memanfaatkan radiasi elektromagnetik yang dihasilkan pada pita frekuensi rendah 3-30 KHz oleh pemancar radio kuat yang digunakan dalam sistem komunikasi dan navigasi jarak jauh. Pada jarak yang jauh dari sumber, medan elektromagnetik berbentuk datar dan horizontal dan komponen listrik E terletak pada bidang vertikal yang tegak lurus komponen H dalam arah rambat dan mengikuti tanah. AM menggunakan pita VLF. Pita frekuensi ini tidak dapat digunakan untuk transfer data karena menawarkan bandwidth yang relatif rendah.

**Transmisi Gelombang Mikro**

Radio gelombang mikro, suatu bentuk transmisi radio yang menggunakan frekuensi ultra-tinggi, dikembangkan dari eksperimen dengan radar (pendeteksian dan jangkauan radio) selama periode sebelum Perang Dunia II. Ada beberapa rentang frekuensi yang ditetapkan pada sistem gelombang mikro, semuanya berada dalam rentang Giga Hertz (GHz) dan panjang gelombang dalam rentang milimeter. Panjang gelombang yang sangat pendek inilah yang memunculkan istilah gelombang mikro. Sinyal frekuensi tinggi seperti itu sangat rentan terhadap redaman dan oleh karena itu harus diperkuat atau diulangi setelah jarak tertentu. Untuk memaksimalkan kekuatan sinyal frekuensi tinggi dan, oleh karena itu, untuk meningkatkan jarak transmisi pada tingkat yang dapat diterima, pancaran radio sangat terfokus. Antena pemancar dipusatkan pada piringan logam cekung dan reflektif yang berfungsi untuk memfokuskan pancaran radio dengan efek maksimal pada antena penerima, seperti diilustrasikan pada Gambar 4.2. Demikian pula, antena penerima dipusatkan pada piringan logam cekung, yang berfungsi untuk mengumpulkan jumlah maksimum sinyal masuk.


**Gambar 4.2 Frekuensi Sinyal Microwave**

**Tabel 4.1 Frekuensi Sinyal Microwave**

| Pita Frekuensi | Pemisahan Antena Maksimum | Analog/Digital |
|---|---|---|
| 4–6 GHz | | Analog |
| 10-12 GHz | 16-24 Km | Digital |
| 18-23 GHz | 32-48 Km | Digital |

Ini adalah sistem transmisi point-to-point, bukan siaran. Selain itu, setiap antena harus berada dalam jarak pandang antena berikutnya. Mengingat kelengkungan bumi, dan masalah transmisi yang melaluinya, gelombang gelombang mikro umumnya dibatasi hingga 50 mil (80 km). Jika frekuensi lebih tinggi dalam pita gelombang mikro yang diberikan pada Tabel 4.1, dampaknya lebih besar dibandingkan frekuensi lebih rendah dalam pita yang sama.

**Sifat Umum Transmisi Gelombang Mikro**

- **Konfigurasi**: Radio gelombang mikro terdiri dari antena yang berpusat di dalam piringan reflektif yang dipasang pada struktur seperti menara atau bangunan. Kabel menghubungkan antena ke peralatan pengirim/penerima sebenarnya.
- **Bandwidth**: Microwave menawarkan bandwidth yang besar, seringkali melebihi 6Gbps.
- **Kinerja Kesalahan**: Microwave, khususnya microwave digital, berkinerja baik dalam hal ini, dengan asumsi desain yang tepat. Namun, radio frekuensi tinggi tersebut sangat rentan terhadap gangguan lingkungan, misalnya curah hujan, kabut, kabut asap, dan asap. Namun secara umum, microwave bekerja dengan baik dalam hal ini.
- **Jarak**: Jarak gelombang mikro jelas terbatas, terutama pada frekuensi yang lebih tinggi. Keterbatasan ini dapat diatasi melalui susunan antena khusus dan lebih kompleks yang menggabungkan keragaman spasial untuk mengumpulkan lebih banyak sinyal.
- **Keamanan**: Seperti halnya dengan semua sistem radio, gelombang mikro pada dasarnya tidak aman. Keamanan harus diberlakukan melalui enkripsi (pengacakan) sinyal.
- **Biaya**: Biaya perolehan, penempatan dan penataan ulang microwave bisa jadi tinggi. Namun, sistem ini sering kali lebih baik dibandingkan dengan sistem kabel, yang memerlukan jalur khusus, pembuatan parit, saluran, penyambungan, dan lain-lain.
- **Aplikasi**: Microwave awalnya digunakan untuk komunikasi suara dan data jarak jauh. Bersaing dengan operator jarak jauh, gelombang mikro ditemukan sebagai alternatif yang paling menarik dibandingkan sistem kabel, karena kecepatan dan biaya penerapan yang rendah jika memungkinkan, namun teknologi serat optik saat ini digunakan dalam hal ini. Aplikasi kontemporer mencakup jaringan pribadi, interkoneksi sakelar radio seluler, dan sebagai alternatif sistem kabel karena mempertimbangkan medan yang sulit.

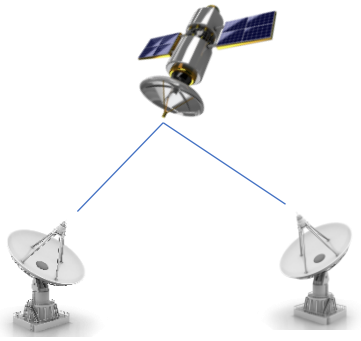
## 4.2 KOMUNIKASI SATELIT

Radio satelit, sederhananya, adalah sistem transmisi gelombang mikro non-terestrial yang memanfaatkan stasiun relai luar angkasa. Satelit telah terbukti sangat berharga dalam

memperluas jangkauan komunikasi suara, data, dan video ke seluruh dunia dan ke wilayah paling terpencil di dunia. Penerapan luar biasa seperti *Global Positioning System* (GPS) tidak akan terpikirkan tanpa manfaat satelit.

Sistem komunikasi satelit kontemporer melibatkan stasiun relai satelit yang diluncurkan ke orbit geostasioner, geosinkron, atau geostatik. Satelit semacam ini disebut satelit geostasioner. Orbit tersebut kira-kira 36.000 km di atas garis khatulistiwa seperti digambarkan pada Gambar 4.3. Pada ketinggian tersebut dan pada slot orbit khatulistiwa, satelit berputar mengelilingi bumi dengan kecepatan yang sama dengan kecepatan revolusi bumi dan mempertahankan posisi relatifnya pada titik yang sama di permukaan bumi. Akibatnya, stasiun bumi yang mengirim dan menerima dapat diarahkan dengan andal ke satelit untuk keperluan komunikasi.

Popularitas komunikasi satelit telah menimbulkan tuntutan besar pada regulator internasional untuk mengelola dan mengalokasikan frekuensi yang tersedia, serta terbatasnya jumlah slot orbit yang tersedia untuk penentuan posisi satelit yang dikelola di tingkat nasional, regional, dan internasional. Secara umum, satelit geostasioner diposisikan sekitar 2º terpisah untuk meminimalkan interferensi dari satelit yang berdekatan yang menggunakan frekuensi yang tumpang tindih.



**Gambar 4.3 satelit di Orbit bumi Geostasioner**

Sinyal frekuensi tinggi seperti itu sangat rentan terhadap redaman di atmosfer. Oleh karena itu, dalam komunikasi satelit, dua frekuensi berbeda digunakan sebagai frekuensi pembawa untuk menghindari interferensi antara sinyal masuk dan keluar, ini adalah:

1) **Frekuensi uplink**: Merupakan frekuensi yang digunakan untuk mengirimkan sinyal dari stasiun bumi ke satelit. Tabel 4.2 menunjukkan frekuensi tertinggi yang digunakan untuk uplink. Sinyal uplink dapat disesuaikan lebih kuat sehingga dapat mengatasi distorsi atmosfer dengan lebih baik. Antena pada sisi pemancar dipusatkan pada piringan cekung dan reflektif yang berfungsi untuk memfokuskan pancaran radio, dengan efek maksimal, pada antena satelit penerima. Demikian pula, antena penerima dipusatkan pada piringan logam cekung, yang berfungsi untuk mengumpulkan jumlah maksimum sinyal masuk.
2) **Frekuensi downlink**: Merupakan frekuensi yang digunakan untuk mengirimkan sinyal dari satelit ke stasiun bumi. Dengan kata lain, transmisi downlink difokuskan pada

tapak atau area cakupan tertentu. Frekuensi yang lebih rendah, yang digunakan untuk downlink, dapat menembus atmosfer bumi dan medan elektromagnetik dengan lebih baik, yang dapat membelokkan sinyal yang masuk seperti halnya pembelokan cahaya ketika memasuki genangan air.

3) **Siaran**: Sistem radio satelit yang luas memungkinkan sinyal disiarkan ke wilayah yang luas. Dengan demikian antena terestrial dalam jumlah berapa pun (secara teoritis jumlahnya tak terhingga) dapat menerima sinyal, kurang lebih secara bersamaan. Dengan cara ini, satelit dapat melayani kebutuhan jaringan point-to-multipoint melalui satu stasiun uplink dan beberapa stasiun downlink.

Baru-baru ini, satelit telah dikembangkan yang dapat melayani kebutuhan jaringan mesh, dimana setiap situs terestrial dapat berkomunikasi langsung dengan situs lainnya. Sebelumnya, semua komunikasi tersebut diperlukan untuk melakukan perjalanan melalui situs terpusat, yang dikenal sebagai head end. Jaringan mesh yang demikian tentu saja memberikan tingkat kesulitan tambahan pada jaringan dalam hal pengelolaan arus dan arah lalu lintas.

**Tabel 4.2 Contoh Frekuensi Satelit Uplink/Downlink**

| Pita Frekuesi | Rentang Frekuensi Uplink/Downlink | Contoh |
|---|---|---|
| C-Band | 6GHz/4GHz | Tv, Suara, Konferensi Vidio |
| Ku-Band | 14GHz/11GHz | Tv. Satelit Siaran Langsung/DSS |
| Ka-Band | 30GHz/20GHz | Suara Seluler |

**Sifat Umum Komunikasi Satelit**

- **Konfigurasi**: Sistem komunikasi satelit terdiri dari antena dan piringan reflektif, sama seperti gelombang mikro terestrial. Piringan berfungsi untuk memfokuskan sinyal dari antena pemancar ke antena penerima. Piringan pengirim/penerima yang membentuk segmen bumi memiliki ukuran yang bervariasi, bergantung pada tingkat daya dan pita frekuensi. Umumnya dipasang pada tripod atau penyangga jenis lain, yang ditambatkan ke tanah, bantalan atau atap, atau dilekatkan pada struktur seperti bangunan. Kabel menghubungkan antena ke peralatan pengirim/penerima sebenarnya. Antena terestrial mendukung pita frekuensi tunggal misalnya C–band, Ku–band atau Ka–band. Semakin tinggi pita frekuensi, semakin kecil kemungkinan ukuran antena parabola. Oleh karena itu, antena TV C-band cenderung berukuran besar, sedangkan antena TV DBS (Direct Broadcast Satellite) Ku-band cenderung berukuran sangat kecil. Tentu saja antena piringan segmen luar angkasa dipasang pada satelit. Satelit dapat mendukung beberapa antena pemancar/penerimaan, tergantung pada berbagai frekuensi, yang digunakan untuk mendukung berbagai aplikasi, dan bergantung pada apakah satelit tersebut mencakup seluruh tapak atau membagi tapak menjadi area cakupan yang lebih kecil melalui penggunaan titik fokus yang lebih rapat. balok. Repeater satelit berbentuk jumlah transponder. Transponder menerima sinyal

lemah yang masuk, memperkuatnya, beralih dari frekuensi uplink ke downlink, dan mengirimkan informasi ke stasiun bumi.

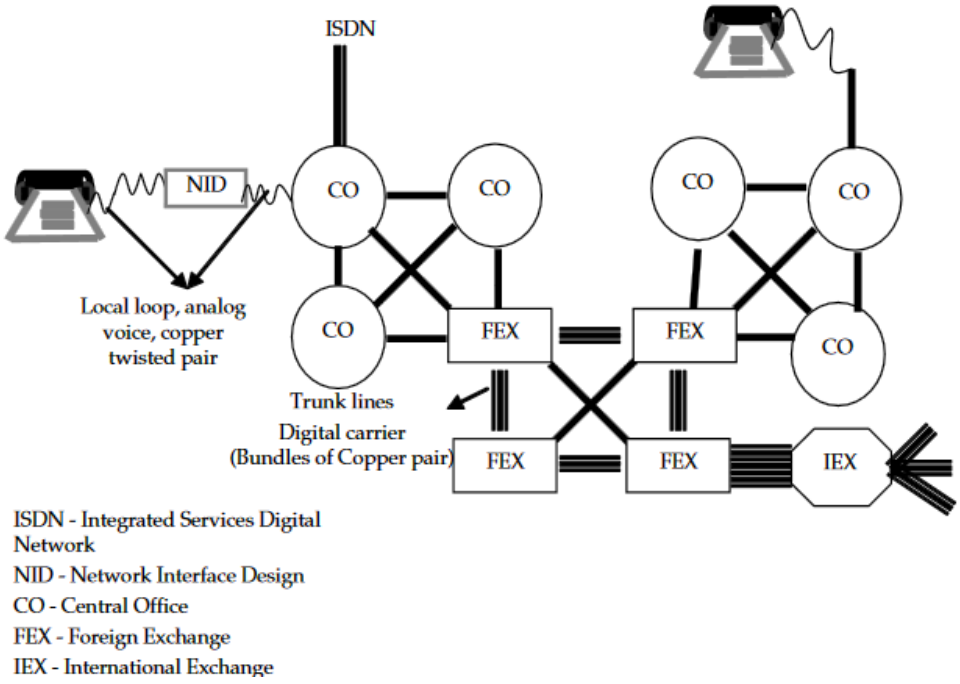
- **Bandwidth**: Satelit dapat mendukung banyak transponder dan, oleh karena itu, bandwidth yang besar, dengan masing-masing transponder umumnya memberikan peningkatan bandwidth.
- **Kinerja Kesalahan**: Transmisi satelit rentan terhadap gangguan lingkungan, khususnya pada frekuensi di atas 20 GHz. Bintik matahari dan jenis interferensi elektromagnetik lainnya mempengaruhi transmisi satelit dan gelombang mikro. Selain itu, beberapa pita frekuensi satelit, misalnya C-band memerlukan manajemen frekuensi yang cermat. Akibat dari faktor-faktor ini, transmisi satelit seringkali memerlukan kemampuan deteksi dan koreksi kesalahan yang ekstensif.
- **Jarak:** Satelit tidak dianggap memiliki batasan jarak karena sebagian besar sinyal bergerak melalui ruang hampa. Selanjutnya setiap sinyal menempuh jarak sekitar 36.000 km di setiap arah.
- **Penundaan Propagasi**: Satelit geostasioner, karena ketinggian orbitnya yang tinggi, menyebabkan penundaan propagasi yang cukup signifikan pada sinyalnya. Oleh karena itu, aplikasi suara, data, dan video yang sangat interaktif tidak didukung secara efektif melalui komunikasi satelit dua arah.
- **Keamanan**: Seperti halnya dengan semua sistem gelombang mikro dan radio lainnya, transmisi satelit pada dasarnya tidak aman. Transmisi satelit sangat rentan terhadap intersepsi, karena sinyalnya disiarkan ke seluruh area tapak. Oleh karena itu, pengguna yang tidak berwenang hanya boleh mengetahui satelit dan rentang frekuensi terkait yang digunakan. Keamanan harus diberlakukan melalui enkripsi (pengacakan) sinyal.
- **Biaya**: Biaya akuisisi, penyebaran, dan penataan ulang sistem satelit segmen ruang angkasa bisa sangat tinggi, hingga beberapa juta rupee. Namun, satelit dapat digunakan bersama oleh sejumlah besar pengguna, dan setiap pengguna mungkin menghubungkan sejumlah besar situs. Akibatnya, jaringan satelit sering dibandingkan dengan sistem kabel atau sistem gelombang mikro untuk banyak aplikasi point-to-multipoint.
- **Aplikasi**: Aplikasi satelit jumlahnya banyak dan meningkat pesat seiring dengan bertambahnya layanan suara dan data tradisional. Layanan suara dan data internasional tradisional telah banyak digantikan oleh sistem kabel serat optik bawah laut.

Secara tradisional, aplikasinya mencakup suara dan data internasional, suara dan data jarak jauh, siaran televisi dan radio, navigasi maritim, konferensi video, manajemen dan pengendalian inventaris melalui VSAT, pemulihan bencana, dan paging. Aplikasi yang lebih baru dan baru mencakup navigasi udara, Sistem Pemosisian Global (GPS), suara dan data seluler karena Satelit Orbit Bumi Rendah (LEO), Sistem Manajemen Lalu Lintas Tingkat Lanjut (ATMS), TV Satelit Siaran Langsung (DBS), Jaringan Layanan Digital Terpadu. (ISDN), televisi interaktif, dan multimedia interaktif.

## 4.3 JARINGAN TELEPON UMUM

Umumnya sistem telepon yang terdapat di rumah dan kantor merupakan bagian dari Public Switched Telephone Network (PSTN). Hal ini diakses melalui telepon, saluran pertukaran cabang swasta dan pengaturan data. Oleh karena itu, PSTN dapat disebut sebagai sistem komunikasi publik yang menyediakan layanan telepon lokal, lokal lanjutan, dan jarak jauh kepada pelanggan. PSTN menggunakan telepon Circuit-Switched yang hampir mirip dengan jaringan packet-switched berbasis IP untuk Internet. PSTN tersedia untuk umum melalui sekelompok operator komunikasi umum yang telah sepakat untuk bertukar panggilan dan koneksi atas nama pelanggan mereka sesuai dengan hukum internasional dan hukum negara tempat beroperasinya.

PSTN mengikuti standar teknis yang dikembangkan oleh ITU-T. Nomor teleponnya didasarkan pada alamat E.163/E.164. PSTN memiliki beberapa sentral telepon yang terhubung bersama untuk membentuk sistem komunikasi telepon nasional dan seluruh dunia. Semua telepon di PSTN memiliki jaringan sedemikian rupa sehingga telepon mana pun dapat melakukan panggilan ke telepon lain di dalam negeri atau di luar negeri sesuai dengan hukum internasional yang ditentukan oleh ITU.




**Gambar 4.1 Struktur PSTN**

Telepon atau perangkat telepon bertindak sebagai perangkat antarmuka untuk menyediakan antarmuka ke PSTN. Ini memungkinkan pelanggan untuk menghubungi nomor telepon untuk melakukan panggilan. Tata letak sederhana PSTN seperti yang ditunjukkan pada Gambar 4.4 terdiri dari komponen-komponen berikut:

(a) **Perangkat Telepon**: Perangkat telepon menyediakan fungsi panggilan dan mengubah suara menjadi sinyal listrik sehingga dapat melintasi kabel tembaga dan sirkuit terkait lainnya untuk mencapai tujuan. Telepon yang dipasang di tujuan mengubah sinyal listrik pada saluran kembali menjadi suara pihak yang menelepon. Perangkat telepon

telah melewati berbagai tahap perkembangan dari sistem magneto sederhana, sistem elektromekanis, hingga sistem digital.

(b) **Loop Lokal**: Koneksi mil terakhir atau loop lokal (kabel drop dari telepon rumah ke kotak sambungan tiang telegraf lokal atau kabel di jalan) adalah kabel fisik untuk menghubungkan pelanggan telepon ke PSTN. Jalur ini mungkin membawa sinyal suara atau data atau keduanya. Pengkabelan fisik untuk loop lokal terdiri dari sepasang kabel tembaga yang dipilin dari kantor pusat penyedia layanan telekomunikasi (CO) ke tempat pelanggan dan sepasang kabel tembaga yang dipilin dari tempat pelanggan ke CO, sehingga membuat satu lingkaran. Sambungan telepon pelanggan menuju ke kotak sambungan di luar rumah yang juga mengumpulkan kabel drop dari rumah lain di area yang sama. Kotak koneksi ini disebut Network Interface Device (NID).

(c) **NID**: NID menyediakan koneksi dupleks antara kabel rumah ke kabel loop lokal ke CO yang melaluinya sinyal listrik analog dilewatkan. Sinyal suara yang dihasilkan oleh mikrofon pada perangkat telepon pelanggan diubah menjadi serangkaian pulsa listrik untuk membentuk sinyal analog. Pengkabelan rumah memungkinkan sinyal analog ini mencapai NID sehingga dapat diteruskan ke RCU (Remote Concentrator Unit) CO melalui kabel loop lokal.

(d) **CO**: Pada CO, ribuan pasang kabel tembaga bergabung membentuk kumpulan bundel yang terdiri dari 26 pasang kabel yang dipecah menjadi pasangan-pasangan individual dan kemudian dilubangi menjadi blok pelubang yang dipasang pada sisi pelanggan atau loop dalam kerangka distribusi. Sisi lain dari kerangka distribusi disambungkan ke sakelar sambungan silang digital untuk menghubungkan panggilan telepon ke belahan dunia lain. Perangkat multipleks pembagian waktu disediakan dalam sakelar sambungan silang untuk melipatgandakan beberapa saluran ke dalam satu sirkuit berkecepatan lebih tinggi. Beberapa contohnya adalah 24 rangkaian DS0 diubah menjadi rangkaian T1.

Pertukaran telepon dianggap sebagai satu set satu atau lebih saklar penghubung silang di satu atau lebih kantor pusat untuk merespons satu kode tiga digit. Kode tiga digit pertama menentukan pertukaran pelanggan yang mereka miliki. Kantor pusat dapat melayani lebih dari satu bursa. Valuta asing adalah pertukaran apa pun di luar pertukaran area panggilan pelanggan atau pertukaran lokal dan terhubung ke pertukaran lokal melalui jalur utama berkecepatan tinggi, sebaiknya T3 atau lebih baik. Devisa tersebut dirujuk ke area panggilan lokal yang diperluas.

Valuta asing dianggap sebagai pertukaran apa pun dalam sistem telepon berbasis sirkuit di luar area panggilan pertukaran lokal pelanggan. Pertukaran lokal lainnya, pertukaran nasional dan pertukaran internasional adalah contoh pertukaran asing. Ketika pelanggan memanggil nomor telepon di luar sentral lokal, panggilan pelanggan diselesaikan dengan membuka koneksi ke sentral lain melalui jalur utama. Pertukaran eksternal yang memfasilitasi penyelesaian panggilan disebut sebagai pertukaran asing.

Pertukaran nasional menyediakan koneksi dari penyedia telepon regional ke penyedia telepon jarak jauh. Pertukaran ini mendefinisikan kode area. Pertukaran internasional adalah

titik di mana penyedia sambungan jarak jauh terhubung ke penyedia sambungan jarak jauh lainnya di luar negeri. Pertukaran internasional menyediakan kode negara. Contoh nomor panggilan untuk Johannesburg, Afrika Selatan dari AS akan terlihat seperti berikut:

| Kode negara | Kode area | Kode Pertukaran | Nomor |
|---|---|---|---|
| 27 | 11 | xx | xxxxxxx |

**Saluran Digital**

Jaringan telepon asli didasarkan pada koneksi suara analog melalui switchboard manual. Secara bertahap, teknologi saklar digital digunakan untuk menghubungkan sirkuit digital antara pertukaran dengan sirkuit dua kabel analog untuk menghubungkan ke sebagian besar telepon. Rangkaian digital dasar menggunakan Sinyal Digital 0 (DS0) yaitu saluran 64 kilobit per detik untuk meneruskan panggilan telepon biasa dari pihak pemanggil ke pihak yang dipanggil. Ia menggunakan Modulasi Kode Pulsa (PCM) 8-bit dengan laju sampel 8 kHz untuk mendigitalkan suara audio mulai dari 30 Hz hingga 3300 Hz. Selain itu, pita pelindung 70 Hz digunakan untuk menjaga suara tetap bersih dan jernih. Jadi, suara audio berkisar antara 0 Hz hingga 4.000 Hz. Menurut teorema pengambilan sampel, diperlukan pengambilan sampel dua kali sinyal audio untuk mereproduksi suara. Sinyal suara diambil sampelnya dengan kecepatan 8000 kali per detik.

**Garis Batang**

Jalur utama telekomunikasi yang selalu bersifat digital menyediakan koneksi berkecepatan tinggi antar kantor pusat dalam sistem PSTN. Kabel twisted pair antara kantor pusat rentan terhadap crosstalk dan kebisingan. Twisted pair juga mahal untuk dipasang dari CO ke CO. Perkembangan bertahap di bidang telekomunikasi mengarah pada pengembangan teknik TDM untuk membawa data melalui jalur tembaga yang ada dan selanjutnya melalui kabel serat optik. Kabel serat menggunakan multiplexing pembagian waktu statistik, hierarki digital sinkron, multiplexing pembagian gelombang kasar atau padat, dan peralihan optik untuk lebih meningkatkan kecepatan transmisi. Oleh karena itu, jalur utama berisi ribuan panggilan simultan yang telah digabungkan menggunakan TDM untuk meneruskannya dari satu CO ke CO lainnya. Protokol pensinyalan SS7 digunakan untuk mengirimkan panggilan dari satu sentral telepon ke sentral telepon lainnya. Di CO, mereka dide-multipleks dan dialihkan melalui saklar penghubung silang akses digital untuk mencapai pertukaran yang tepat dan nomor telepon lokal. Beberapa contoh jalur trunk adalah T1, T3, DS1, DS3, Tie line, Tie trunk, dll.

- **T1**: T1 yang dianggap sebagai sirkuit khusus tersedia sebagai T1 penuh, T1 tersalurkan, dan T1 pecahan. Sirkuit T1 terdiri dari loop lokal dari penyedia layanan lokal dan sirkuit pembawa yang disediakan oleh perusahaan yang sama atau penyedia layanan berbeda. Layanan T1 lengkap yang sering disebut sebagai jalur utama digital biasanya tersedia sebagai rangkaian lengkap dengan kecepatan total hingga 1,544Mbps baik sebagai data atau suara, tetapi tidak keduanya. T1 yang disalurkan seperti namanya berisi 24 saluran individual yang mampu membawa suara atau data. Kumpulan saluran

lengkap memberikan kecepatan yang sama dengan T1 penuh. Saluran individual dapat dibagi menjadi jalur suara untuk layanan telepon atau jalur data untuk layanan Internet menggunakan perangkat yang disebut Unit Layanan Saluran/Unit Layanan Data atau CSU/DSU. T1 pecahan tersedia kurang dari bandwidth T1 penuh di mana satu atau lebih saluran digabungkan menjadi satu. Mirip dengan T1 yang disalurkan, saluran individual dapat berupa suara atau data dan CSU/DSU digunakan untuk membagi saluran. Sirkuit T1 selalu aktif dan oleh karena itu disebut sebagai jalur pribadi atau jalur data khusus.

- **DS1**: Digital Signaling Level 1 (DS1) berisi 24 TDM suara ke dalam frame 192-bit melalui koneksi fisik tunggal yang menyediakan throughput data 1,544 Mbps melalui koneksi suara digital Lapisan Fisik T1.
- **DS3**: Mengacu pada sirkuit telekomunikasi yang membawa banyak panggilan dari satu kantor pusat ke kantor pusat lainnya dan juga disebut sebagai tie trunks atau tie line. DS3 berisi setara dengan 28 sirkuit T1/DS1 dengan mengurangi waktu yang dialokasikan untuk setiap sampel data dan mengalikan T1 bersama-sama untuk membentuk aliran data DS3 akhir.

## 4.4 SISTEM TELEPON SELULER

Perkembangan sistem telepon seluler atau telepon seluler merupakan perkembangan terkini. Ini juga dikenal sebagai ponsel dan sesuai dengan namanya, ponsel ini dirancang untuk pengguna ponsel yang perlu melakukan panggilan telepon dari lokasi berbeda ketika mereka biasanya jauh dari rumah atau kantor.

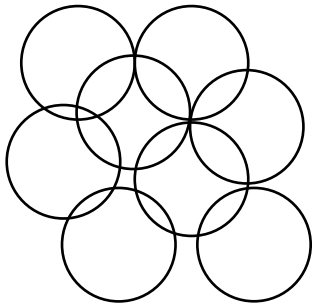

**Gambar 4.5 SmartPhone**

Pesatnya perkembangan teknologi perangkat keras membantu dalam merancang perangkat telepon portabel seperti yang ditunjukkan pada Gambar 4.5 sehingga pengguna dapat membawanya di dalam tas kantor atau saku saat bergerak. Telepon seluler

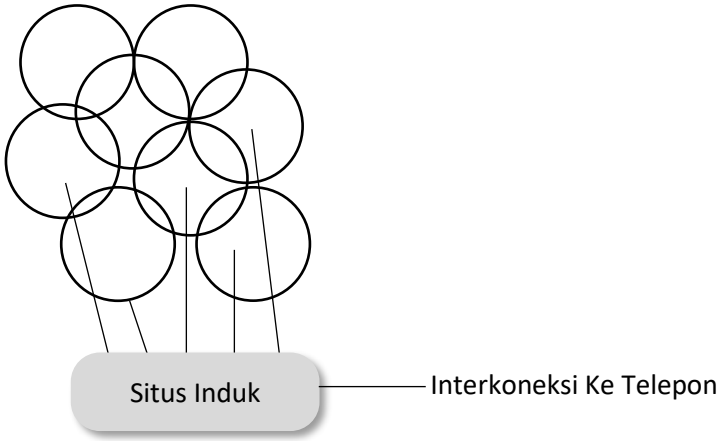
menggunakan frekuensi radio untuk berbicara dengan situs seluler terdekat. Situs seluler bertindak sebagai titik akses untuk panggilan seluler dan telepon seluler secara teratur berkomunikasi dengan situs seluler terdekat untuk memberi tahu jaringan bahwa situs tersebut terhubung.

**Situs Sel**

Ini dapat didefinisikan sebagai wilayah geografis melingkar yang menangani telepon seluler dalam batas fisik yang ditentukan. Jaringan seluler seperti yang ditunjukkan pada Gambar 4.5 dianggap terdiri dari sel-sel yang tumpang tindih sehingga dapat disediakan area yang lebih luas dengan kemungkinan putusnya panggilan yang rendah. Struktur yang tumpang tindih ini membantu menjaga panggilan tetap utuh saat pengguna berpindah lokasi dari satu situs sel ke situs sel lainnya. Dalam hal ini, panggilan ditransfer ke situs sel terdekat yang bertanggung jawab atas area fisik tersebut.



**Gambar 4.6: Jaringan Seluler yang Terdiri dari Sel-sel Individual**




**Gambar 4.7 Koneksi Jaringan Selular ke Pertukaran Telepon**

Telepon seluler cocok untuk wilayah geografis yang lebih luas termasuk lokasi terpencil. Ini menghemat biaya kawat tembaga dan upaya pemasangannya di daerah padat penduduk.

Setiap situs sel yang ditunjukkan pada Gambar 4.6 terhubung ke situs master, yang bertindak sebagai titik akses untuk jaringan seluler tertentu. Situs induk menyediakan interkoneksi ke jaringan telepon biasa. Panggilan yang ditangani oleh masing-masing situs sel diteruskan kembali ke situs sel master, yang kemudian meneruskannya ke jaringan telepon seperti yang ditunjukkan pada Gambar 4.7

Sel depan dapat menggunakan kembali frekuensi yang digunakan pada sel sebelumnya. Ini membantu dalam berbagi pita frekuensi yang sama. Banyak panggilan dapat ditangani oleh satu frekuensi terutama bila telepon digital digunakan.

## 4.5 TELEVISI KABEL

Televisi kabel atau TV Kabel menggunakan kabel koaksial sebagai media transmisi untuk mentransmisikan program televisi ke televisi di rumah atau kantor. Televisi konvensional menggunakan siaran sinyal melalui udara menggunakan gelombang radio untuk mengirimkan program televisi ke penerima televisi. Sistem ini memerlukan antena televisi. Di sisi lain, sistem televisi kabel menggunakan sinyal frekuensi radio melalui serat optik tetap atau kabel koaksial untuk mengirimkan program televisi ke konsumen. Aplikasi lain dari televisi kabel adalah program radio FM, Internet berkecepatan tinggi, telepon, dll.

Tahukah kamu? Penggunaan kabel koaksial memberikan beberapa keuntungan karena bandwidthnya yang besar; transmisi sinyal dua arah dan data dalam jumlah besar dimungkinkan. Sinyal televisi kabel memerlukan bandwidth saluran koaksial yang kecil. Oleh karena itu, sisa bandwidth dapat digunakan untuk layanan digital lainnya seperti Internet broadband dan telepon kabel.

- **Internet Broadband melalui Kabel Koaksial:** Hal ini dimungkinkan karena modem kabel yang mengubah data internet menjadi sinyal digital yang dapat ditransfer melalui kabel koaksial.
- **Layanan Telepon Kabel**: Antarmuka telepon khusus dipasang di tempat pelanggan untuk mengubah sinyal analog dari kabel di rumah pelanggan menjadi sinyal digital. Sinyal analog kemudian dikirim pada loop lokal ke pusat switching. Keuntungannya meliputi kebutuhan bandwidth yang lebih sedikit, kualitas suara yang lebih baik dan integrasi ke jaringan VoIP.

**Modem kabel**

Modem kabel bekerja berdasarkan prinsip modem dan menyediakan akses ke sinyal data yang dikirim melalui infrastruktur televisi kabel. Modem kabel memberikan akses Internet broadband dalam bentuk Internet kabel, memanfaatkan bandwidth yang tidak terpakai pada jaringan televisi kabel menggunakan kabel koaksial atau kabel serat optik. Modem kabel berfungsi seperti jembatan sesuai dengan IEEE 802.1D untuk jaringan Ethernet. Modem kabel meneruskan frame Ethernet antara LAN pelanggan dan jaringan kabel koaksial.

**Ringkasan**

- Ada beberapa macam media transmisi. Teknologi media mulai dari kabel tembaga hingga nirkabel dan serat optik telah berkembang begitu pesat dan menggantikan teknologi lainnya dengan sangat cepat di era informasi ini. Dapat dilihat bahwa Public Telephone Switched Network (PSTN) telah berevolusi dari penggunaan awal kabel koaksial hingga menghubungkan pusat-pusat utama. Secara bertahap, hal ini digantikan dengan penggunaan stasiun gelombang mikro karena biaya tembaga dan infrastruktur terkait.

- Komunikasi jarak jauh dapat dibuat terjangkau, layak dan dapat diandalkan dengan menggunakan menara gelombang mikro tinggi yang digabungkan dengan stasiun repeater pada jarak tertentu. Hal ini memerlukan lebih sedikit perawatan dan peningkatan keandalan karena antarmuka udara dibandingkan jalur fisik dalam bentuk kabel koaksial. Komunikasi jarak jauh ini diperkuat dengan tersedianya satelit yang ada dimana-mana dalam jumlah yang memadai. Komunikasi satelit mempunyai masalah penundaan yang besar.
- Saat ini kabel serat optik digunakan sebagai sarana pilihan untuk menghubungkan pusat-pusat utama secara bersamaan. Hal ini tidak berarti bahwa media baru seperti serat optik dan satelit sudah ketinggalan jaman dari media konvensional. Faktanya, di era informasi ini, setiap media memiliki tujuan yang berbeda-beda dan mempunyai tempatnya masing-masing.
- Komunikasi seluler juga dapat dilihat dalam perspektif yang sama, karena layanan ini harus tersedia kapan saja dan di mana saja.

**Latihan Soal**

Cocokkan yang berikut ini:

| Kolom A | Kolom B |
|---|---|
| C–band | 14GHz/11GHz |
| Gelombang radio | 30GHz/20GHz |
| Ku-band | Komunikasi Satelit |
| Sistem Pemosisian Global (GPS) | $3 \times 10^8$ meter per detik. |
| Ka-band | 6GHz/4GHz |

Isilah bagian yang kosong:

1. Kecepatan perpindahan energi di ruang bebas adalah .....
2. ..... merupakan masalah serius dalam sistem komunikasi gelombang mikro.
3. Sistem satelit mengirimkan sinyal jauh di atas bumi dari .....
4. Frekuensi uplink dan frekuensi down dijaga agar berbeda dalam sistem komunikasi satelit untuk .....
5. .....adalah saluran transmisi yang lebih besar yang membawa data yang dikumpulkan dari saluran-saluran yang lebih kecil yang saling berhubungan dengannya.
6. ..... wilayah geografis melingkar yang menangani telepon seluler dalam batas fisik yang ditentukan.
7. Rentang frekuensi gelombang mikro 10-12 GHz akan memiliki pemisahan antena maksimum pada kisaran ..... untuk transmisi digital.
8. Operator kabel biasanya mengambil sinyal TV dari ..... sebelum mendistribusikannya ke pelanggannya.

**Uraian**

1. Jelaskan perbedaan komunikasi satelit dengan siaran radio?

2. Tuliskan dua keuntungan dan kerugian menggunakan komunikasi satelit.
3. Bagaimana sel dalam komunikasi seluler memastikan rendahnya kemungkinan terputusnya panggilan?
4. Bagaimana sinyal gelombang mikro diperkuat hingga nilai maksimalnya untuk meningkatkan jarak transmisi pada tingkat yang dapat diterima?

# BAB 5
# PERANGKAT JARINGAN

**Pendahuluan**

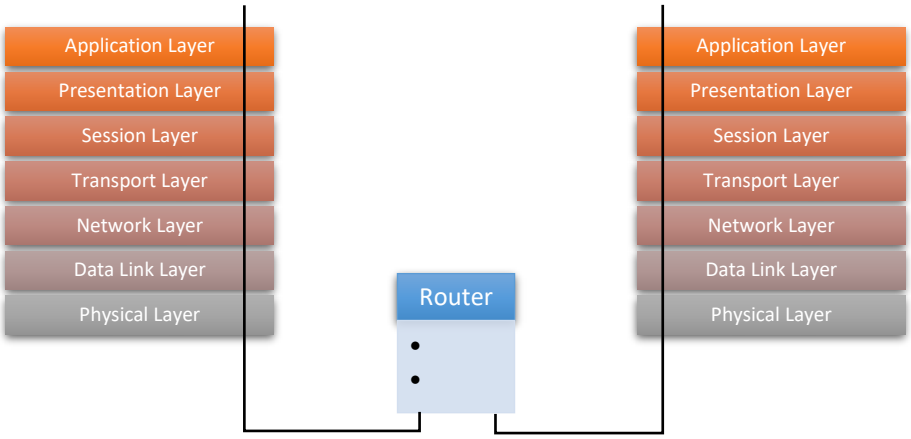
Perangkat jaringan adalah komponen yang digunakan untuk menghubungkan komputer atau perangkat elektronik lainnya sehingga dapat berbagi file atau sumber daya seperti printer atau mesin faks. Perangkat yang digunakan untuk setup Local Area Network (LAN) merupakan jenis perangkat jaringan yang paling umum digunakan oleh masyarakat. LAN memerlukan hub, router, teknologi kabel atau radio, kartu jaringan, dan jika akses online diinginkan, modem berkecepatan tinggi.

## 5.1 ROUTER

Router digunakan untuk menghubungkan LAN serupa dan berbeda, seperti yang ditunjukkan pada Gambar 5.1. Router beroperasi pada lapisan jaringan model OSI menggunakan lapisan fisik, lapisan data link dan lapisan jaringan untuk menyediakan konektivitas, pengalamatan dan peralihan seperti yang ditunjukkan pada Gambar 5.2. Ini adalah perangkat yang sangat cerdas. Dalam kasus jaringan TCP/IP, Protokol Internet (IP) digunakan sebagai alamat jaringan; ini adalah router yang menafsirkan alamat IP dan mengirimkan paket dengan andal. Sekarang kita dapat mengatakan bahwa router mentransmisikan data lapisan jaringan dan oleh karena itu menyediakan transmisi data antar LAN yang menggunakan protokol data link berbeda tetapi menggunakan protokol lapisan jaringan yang sama. Karena itu Ethernet dapat dihubungkan dengan jaringan token ring menggunakan router. Selain itu, router menyediakan konektivitas ke MAN (SMDS) dan WAN (X.25, Frame Relay dan ATM). Router sensitif terhadap protokol, biasanya mendukung banyak protokol dan ukuran paket yang besar dan bervariasi seperti yang mungkin terlibat dalam mendukung Ethernet dan Token Ring.

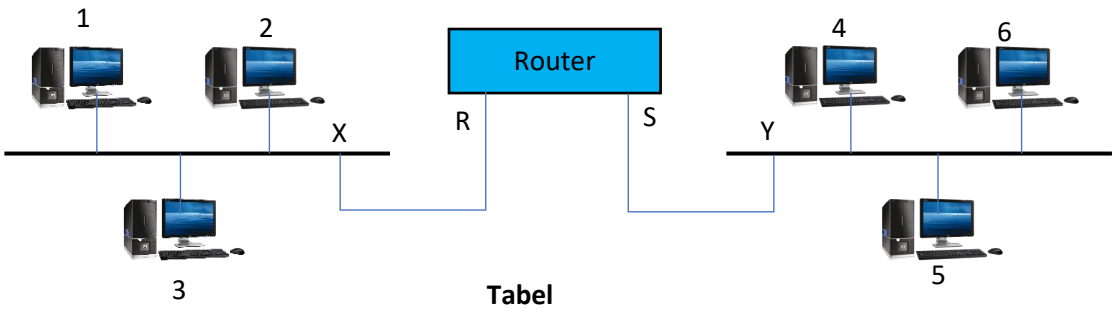
Jaringan yang terdiri dari router dapat memiliki banyak jalur, tidak seperti jembatan. Biasanya jalur terpendek dalam jaringan digunakan untuk mentransfer paket.


**Gambar 5.1 jaringan router**




**Gambar 5.2 Korespondensi OSI Pada Router**

Perhatikan kasus transmisi data dari Komputer 1 ke Komputer 5 pada jaringan yang ditunjukkan pada Gambar 5.3. Ketika Komputer 1 mulai mengirimkan data, ia membandingkan alamat IP-nya dengan Komputer 5 yaitu alamat komputer tujuan untuk mengetahui apakah Komputer 5 terletak di jaringannya sendiri atau tidak. Ketika Komputer 1 menemukan bahwa ia tidak berada dalam jaringannya, ia mengirimkan paket data yang berisi alamat MAC R router dalam hal ini. Ketika router menerima paket ini, ia menetapkan alamat MAC Komputer 5 dan mengirimkan paket ke port yang memiliki alamat tujuan IP yang sama seperti yang diberikan dalam paket data. Dengan cara ini Komputer 5 menerima paket data.


**Tabel**

| Network Address | Port |
|---|---|
| 240.0.0.0 | X |
| 241.0.0.0 | Y |

**Gambar 5.3 Komunikasi melalui Router**

**Karakteristik Router**

1. Router adalah perangkat multiport dengan tulang punggung berkecepatan tinggi.
2. Router juga mendukung pemfilteran dan enkapsulasi seperti jembatan.

3. Seperti bridge, router juga belajar mandiri, karena mereka dapat mengkomunikasikan keberadaannya ke perangkat lain dan dapat mempelajari keberadaan router, node, dan segmen LAN baru.
4. Router merutekan lalu lintas dengan mempertimbangkan jaringan secara keseluruhan. Hal ini menunjukkan bahwa mereka menggunakan tingkat kecerdasan yang tinggi untuk menyelesaikan tugas ini. Karakteristik ini membuat mereka lebih unggul dibandingkan hub dan bridge karena mereka hanya melihat jaringan berdasarkan link-by-link.
5. Paket yang ditangani oleh router dapat mencakup alamat tujuan, tingkat prioritas paket, rute berbiaya paling rendah, penundaan rute minimum, jarak rute minimum, dan tingkat kemacetan rute.
6. Router senantiasa memantau kondisi jaringan, secara keseluruhan untuk beradaptasi secara dinamis terhadap perubahan kondisi jaringan.
7. Mereka biasanya memberikan tingkat redundansi tertentu agar mereka tidak terlalu rentan terhadap kegagalan yang sangat besar.

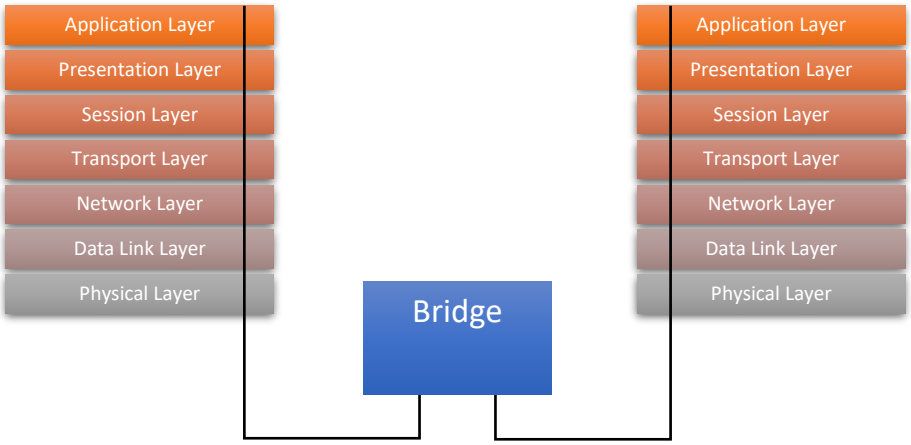
**Protokol Router**

Protokol router terdiri dari protokol bridging dan routing seperti yang tercantum di bawah ini:

1. Protokol Antar-router: Ini adalah protokol router-ke-router yang dapat beroperasi melalui jaringan yang berbeda. Protokol ini merutekan informasi dan menyimpan paket data selama periode tidak aktif.
2. Protokol Jalur Serial: Protokol ini banyak digunakan melalui koneksi serial atau dialup, tidak seperti router. Contohnya termasuk HDLC, SLIP (Serial Line Interface Protocol), dan PPP (Point-to-Point Protocol).
3. Protokol Stack Routing dan Bridging Protocols: Ini memberi saran pada router mengenai paket mana yang harus dirutekan dan mana yang harus dijembatani.

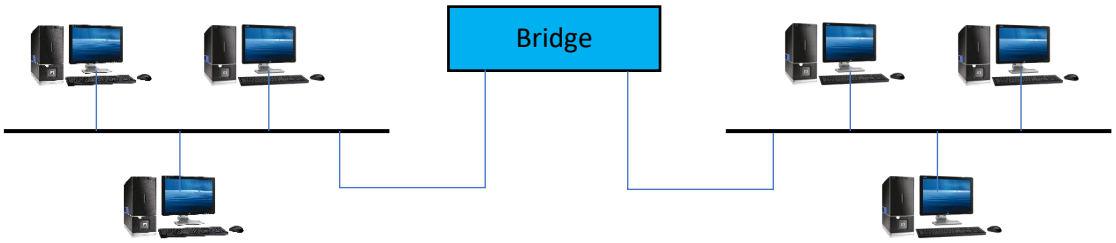
## 5.2 (BRIDGE) JEMBATAN

Seperti repeater, bridge digunakan untuk menghubungkan LAN serupa secara bersamaan, misalnya Ethernet-ke-Ethernet dan beroperasi pada dua lapisan terbawah model OSI yaitu lapisan fisik dan lapisan data link seperti yang ditunjukkan pada Gambar 5.4. Karena beroperasi pada lapisan kedua model OSI, maka ia hanya meneruskan data yang diperlukan ke sinyal lain. Alamat MAC (alamat fisik) digunakan untuk menentukan apakah data diperlukan untuk dikirim ke segmen LAN lain atau tidak. Ia meneruskan informasi dari satu segmen LAN ke segmen LAN lainnya berdasarkan alamat tujuan paket. Dengan kata lain, ketika sebuah jembatan menerima data melalui salah satu portnya, ia memeriksa data tersebut untuk alamat MAC. Jika alamat ini cocok dengan node yang terhubung ke port lain, bridge mengirimkan data ini melalui port ini. Tindakan ini disebut penerusan. Jika alamatnya tidak cocok dengan node mana pun yang terhubung ke port lain, bridge akan membuangnya. Tindakan ini disebut pemfilteran. Hal ini ditunjukkan pada Gambar 5.5. Tidak seperti repeater, bridge mempunyai buffer untuk menyimpan dan meneruskan paket jika link tujuan padat dengan lalu lintas.




**Gambar 5.4 Korespondensi Model Referensi Bridge dan OSI**

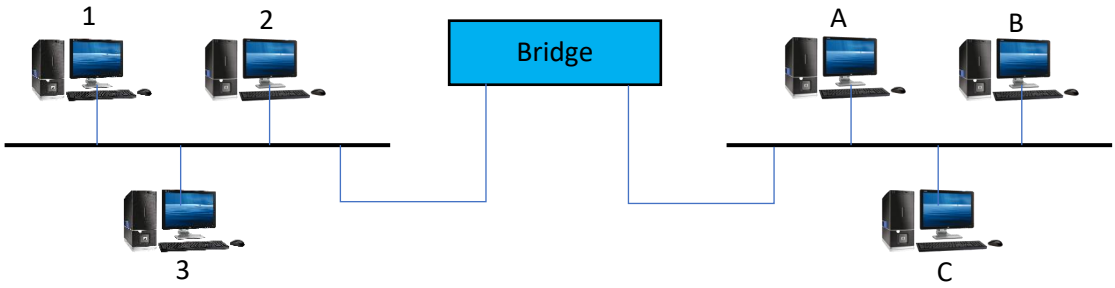
Keuntungan utama dari bridge over repeater adalah ia memiliki tindakan penyaringan. Jika ada noise pada Ethernet yang terjadi karena tabrakan atau gangguan pada sinyal listrik, bridge akan menganggapnya sebagai frame yang bentuknya salah dan tidak akan meneruskan ke segmen yang terhubung ke port lain di bridge. Seperti yang Anda ketahui bahwa maksimal empat repeater dapat digunakan untuk menghubungkan beberapa segmen Ethernet. Namun, jika jembatan disediakan antara repeater, batas empat ini akan ditingkatkan. Jumlah maksimal jembatan tidak dibatasi secara khusus.




**Gambar 5.5 Jaringan LAN bridge**

Dari sudut pandang arsitektur, jembatan adalah perangkat yang tidak bergantung pada protokol dan sangat sederhana. Mereka tidak melakukan proses rumit pada paket data yang melewatinya seperti evaluasi jaringan secara keseluruhan untuk membuat keputusan perutean ujung ke ujung. Mereka cukup membaca alamat tujuan paket data yang masuk dan meneruskannya ke link berikutnya. Oleh karena itu, jembatan tidak mahal dan cepat. Ada jembatan yang disebut jembatan cascading yang digunakan untuk mendukung banyak LAN yang dihubungkan oleh banyak media.

LAN yang berbeda seperti Ethernet-to-token ring juga dapat dihubungkan dengan bantuan jembatan yang dikenal sebagai jembatan enkapsulasi. Fungsi jembatan enkapsulasi juga sangat sederhana. Ini merangkum data LAN asal bersama dengan informasi kontrol LAN pengguna akhir. Bridge dengan fungsi routing antar LAN juga tersedia.




**Gambar 5.6 pemfilteran dan penerusan pada jaringan bridge**

Komputer 1 pada Gambar 5.6 ingin berbicara dengan Komputer 3 di jaringan yang sama. Paket yang dikirim oleh Komputer 1 akan berisi alamat fisik Komputer 3 yang juga akan diterima oleh perangkat jembatan yang menghubungkan kedua segmen LAN. Bridge akan membaca alamat fisik yang terdapat dalam paket dan mengamati bahwa alamat ini milik komputer di segmen LAN yang sama. Oleh karena itu bridge akan memfilter paket ini dan tidak mengizinkannya dikirim melalui sisi lain jaringan. Jika Komputer 1 ingin berbicara dengan Komputer C di segmen lain, bridge akan mengetahui dari tabel alamatnya bahwa alamat ini milik komputer yang terhubung ke segmen lain dalam jaringan. Dalam hal ini, ini akan diteruskan ke segmen LAN lainnya. Bridge mempelajari lokasi komputer yang terhubung ke jaringan dengan mengamati frame. Hal ini akan dijelaskan kemudian pada pembahasan selanjutnya. Perhatikan bahwa dalam kasus paket siaran dan multicast, bridge meneruskan paket ini ke semua komputer yang terhubung ke segmen di kedua sisi.

**Jembatan Kontrol Akses Media (MAC).**

Ini digunakan untuk menghubungkan LAN yang berbeda seperti Ethernet-to-token ring menggunakan enkapsulasi atau terjemahan. Jembatan ini menerjemahkan format paket asli dari segmen LAN yang meminta dengan merangkum atau membungkus data kontrol khusus untuk protokol segmen LAN tujuan.

**Tabel Alamat**

Seperti dijelaskan di atas, setiap jembatan harus memiliki tabel alamat yang menunjukkan lokasi komputer atau node yang berbeda pada segmen LAN. Lebih khusus lagi, ini menunjukkan hubungan antara node dan port. Saat jembatan di-boot pertama kali, tabel ini ternyata kosong. Sekarang muncul pertanyaan bagaimana tabel ini diisi dengan alamat yang sesuai dari berbagai node yang terpasang pada port. Sebagian besar jembatan disebut jembatan adaptif atau jembatan mandiri karena jembatan tersebut mempelajari sendiri lokasi node dan port terkait serta membuat daftar node yang dilampirkan pada setiap segmen.

Ketika sebuah bridge menerima paket data dari komputer, pertama-tama bridge akan menyalin alamat fisik komputer yang terdapat dalam paket tersebut ke dalam daftarnya. Setelah itu, bridge menentukan apakah paket ini harus diteruskan atau tidak. Dengan kata lain, bridge mempelajari lokasi komputer di jaringan segera setelah komputer di jaringan mengirimkan beberapa paket.

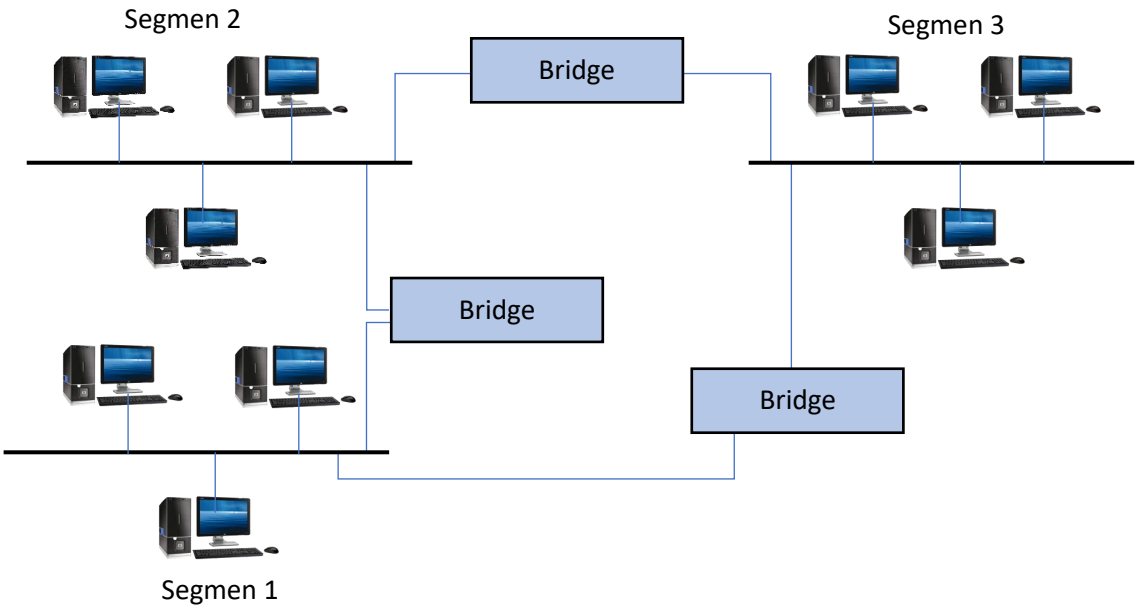
Jika komputer tidak mengirimkan paket, bridge tidak akan pernah dapat menentukan posisinya dan tidak perlu meneruskan paket tersebut ke jaringan. Untungnya, hal ini tidak

dapat terjadi karena komputer dengan perangkat lunak jaringan yang terpasang pada jaringan mengirimkan setidaknya satu frame saat sistem pertama kali melakukan booting. Selain itu, komunikasi komputer bersifat dua arah, selalu ada pengakuan untuk setiap paket yang diterima.

**Protokol Bridge**

Protokol bridge mencakup pohon rentang, protokol perutean sumber, dan perutean sumber transparan.

- **Jembatan Spanning Tree Protocol** (STP): Ini juga dikenal sebagai jembatan adaptif atau pembelajaran mandiri dan didefinisikan dalam standar IEEE 802.1. Sudah dijelaskan pada bagian di atas. Idealnya, dalam jaringan yang dijembatani, pohon jaringan dari jembatan hanya menyediakan satu rentang (link) untuk setiap koneksi LAN-ke-LAN dan oleh karena itu tidak ada jaringan dengan jembatan yang dapat membentuk satu lingkaran. Terkadang perulangan bisa terjadi. Hal ini dapat dijelaskan dengan bantuan Gambar 5.7.




**Gambar 5.7 perputaran pada jaringan bridge**

Paket data siaran yang dikirim oleh komputer yang terpasang pada segmen 1 dapat menjangkau seluruh komputer yang terpasang pada segmen 2 dan 3 tanpa adanya sambungan antara segmen 1 dan 3 seperti terlihat pada Gambar 5.7. Terkadang, koneksi jembatan antara segmen 1 dan 3 atau sejenisnya disediakan untuk memberikan lebih banyak redundansi pada jaringan. Sekarang dalam hal ini paket siaran yang sama yang dikirim oleh segmen 1 akan mencapai segmen 3 melalui dua rute yaitu dari segmen 1 ke 2 ke 3 dan rute lainnya melalui segmen 1 ke 3. Dengan cara ini komputer di segmen 3 akan menerima paket duplikat. Dalam kasus jaringan besar, beberapa segmen mungkin menerima banyak paket dan menyebabkan perulangan.

Oleh karena itu, sebuah loop dapat menyebabkan paket siaran atau paket dengan tujuan yang tidak diketahui beredar melaluinya, sehingga membuat jaringan tidak dapat beroperasi. Kondisi ini dihindari dengan membuat beberapa jembatan yang tidak meneruskan rangka. Algoritme yang dikenal sebagai Distributed Spanning Tree (DST) menyelesaikan tugas ini. Algoritma ini memutuskan jembatan mana yang harus meneruskan paket-paket dalam jaringan. Di bawah skema ini jembatan bertukar pesan kontrol yang dikenal sebagai pesan hello untuk memilih satu rute transmisi. Jembatan yang tersisa mempertahankan posisi siaga dan menyediakan jalur alternatif jika terjadi kegagalan beberapa jembatan pada jalur transmisi yang dipilih. Pada Gambar 5.8 jembatan yang menghubungkan segmen 1 dan 3 akan aktif hanya jika jembatan yang menghubungkan segmen 2 dan 3 gagal, sebaliknya jembatan tersebut bertindak sebagai jembatan siaga untuk jaringan. Dengan kata lain, jembatan yang mendukung algoritma spanning tree mempunyai kemampuan untuk secara otomatis mengkonfigurasi ulang dirinya sendiri untuk jalur alternatif jika suatu segmen jaringan gagal, sehingga meningkatkan keandalan secara keseluruhan.

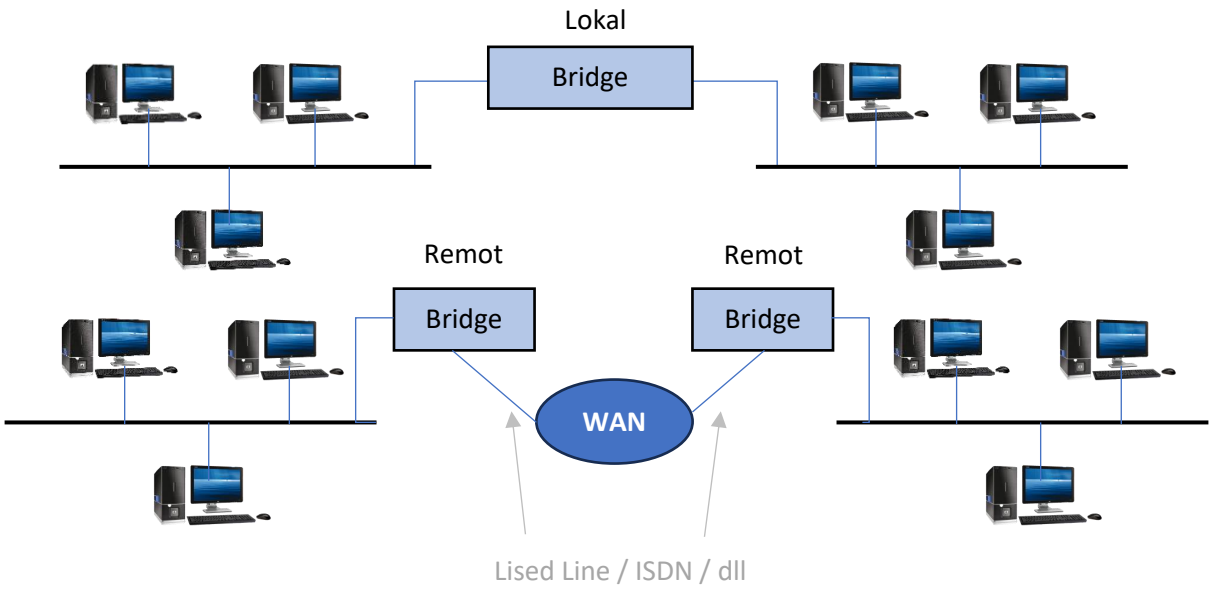
- **IBM Source Routing Protocol (SRP) Bridge**: Ini diprogram dengan rute spesifik untuk setiap paket berdasarkan pertimbangan seperti lokasi fisik node, dan jumlah jembatan yang terlibat.
- **Source Routing Transparent (SRT)**: Ini didefinisikan dalam standar IEEE 802.1. Ini secara efektif merupakan kombinasi STP dan SRP. Router SRT dapat menghubungkan LAN dengan metode apa pun, sesuai program.

**Klasifikasi Bridge**

Ini diklasifikasikan menjadi jembatan lokal dan jarak jauh:

- Pengantin lokal adalah jembatan biasa
- Jembatan jarak jauh digunakan untuk menghubungkan jaringan yang berjauhan satu sama lain. WAN umumnya disediakan antara dua jembatan.

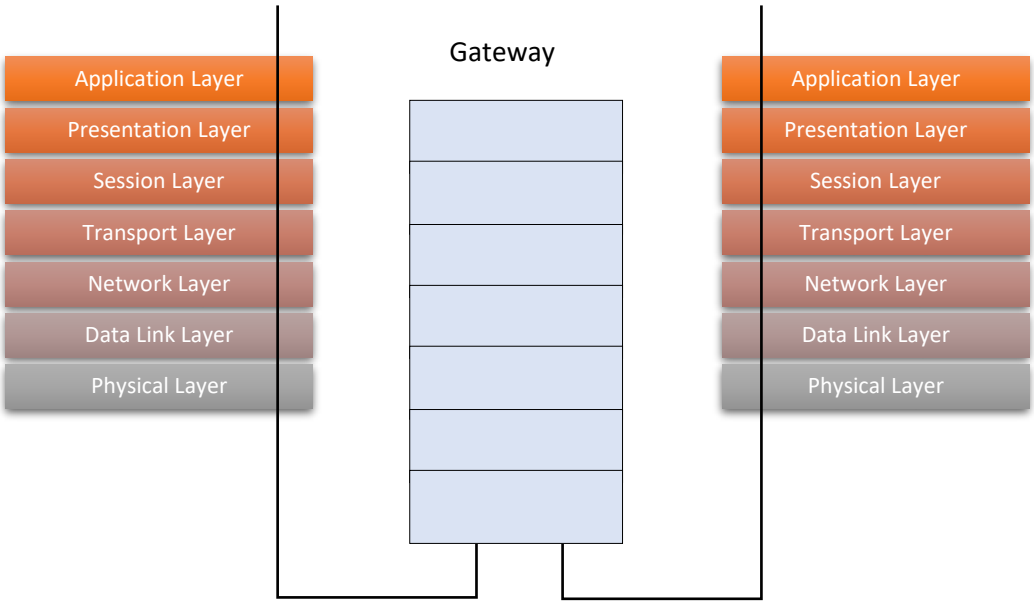
Gambar 5.8 menunjukkan koneksi jembatan lokal dan jarak jauh.



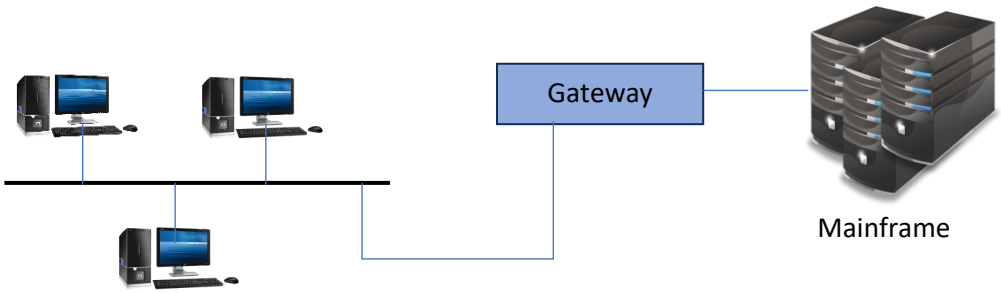

**Gambar 5.8 Lokal dan remote bridge**

## 5.3 GATEWAY

Router gateway digunakan untuk menghubungkan LAN yang berbeda dan menjalankan semua fungsi bridge dan router. Ini beroperasi di ketujuh lapisan Model Referensi OSI seperti yang ditunjukkan pada Gambar 5.9. Ini sebenarnya adalah pendahulu dari router saat ini dan secara teknologi lebih mahal dan sangat fungsional. Mereka pada umumnya terdiri dari perangkat lunak, yang berada di komputer host, seperti midrange atau mainframe seperti ditunjukkan pada Gambar 5.9.




**Gambar 5.9 Korespondensi OSI dari Gateway**




**Gambar 5.10 Interkoneksi antara Ethernet dan Mainframe menggunakan Gateway**

**Karakteristik Gateway**

1. Gateway menyediakan konversi protokol penuh dari satu teknologi LAN eksklusif ke teknologi lainnya, misalnya ethernet ke token ring atau FDDI atau standar atau protokol lain apa pun selain enkapsulasi.
2. Ia menggunakan lapisan model OSI yang lebih tinggi, mungkin melalui lapisan 7, lapisan aplikasi. IBM SNA, DECnet, Internet TCP/IP dan protokol lainnya dapat dikonversi dari jaringan ke jaringan.

3. Tidak seperti bridge dan router, gateway beroperasi lambat karena konversi protokol. Akibatnya, hal ini dapat menimbulkan kemacetan selama periode puncak penggunaan.

## 5.4 SWITCH

Switch adalah perangkat yang menggabungkan fungsi jembatan serta 'koneksi khusus' point-to-point. Mereka menghubungkan perangkat atau jaringan, menyaring, meneruskan dan membanjiri frame berdasarkan alamat tujuan MAC dari setiap frame. Switch beroperasi pada lapisan datalink model OSI. Secara teknis mereka disebut jembatan. Mereka memindahkan data tanpa perselisihan. Sakelar Ethernet menyediakan kombinasi koneksi bersama/khusus 10/100/1000 Mbps. Beberapa switch E-net mendukung cut-through switching: frame diteruskan segera ke tujuan tanpa menunggu perakitan seluruh frame di switch buffer. Mereka secara signifikan meningkatkan throughput. Mereka menyediakan jalur ekspres untuk lalu lintas.

Perbandingan Switch dan Hub

| Hub | Switch |
|---|---|
| Domain Tabrakan | Domain Siaran |
| Semua bagian pada hub adalah bagian dari Ethernet yang sama | Setiap bagian pada switch dapat dianggap sebagai Ethernet terpisah (tetapi semuanya merupakan bagian dari jaringan area lokal yang sama) |
| Semua bagian di hub berbagi bandwidth 10Mb (100 Mb) yang sama | Setiap bagian pada switch mempunyai bandwidth 10Mb (100 Mb) sendiri |
| Setiap frame yang muncul pada satu port hub diulangi ke semua port lain di hub | Frame terarah yang muncul pada satu bagian switch hanya diteruskan ke port tujuan. |
| Sniffer pada port hub mana pun dapat melihat semua lalu lintas di jaringan | Jaringan yang dialihkan sulit untuk diendus |
| Hub akan mengulangi frame yang rusak | |

## 5.5 HUB

Jika beberapa koneksi masuk perlu dihubungkan dengan beberapa koneksi keluar, maka diperlukan hub. Dalam komunikasi data, hub adalah tempat konvergensi dimana data datang dari satu atau lebih arah dan diteruskan ke satu atau lebih arah lainnya. Hub adalah repeater multi-port, dan karena itu mereka mematuhi aturan yang sama seperti rep eater. Mereka beroperasi pada Lapisan Fisik Model OSI. Hub digunakan untuk menyediakan Topologi Bintang Fisik. Di pusat bintang terdapat hub, dengan node jaringan terletak di ujung bintang.

**Topologi Bintang**

Hub dipasang di lemari kabel pusat, dengan semua kabel memanjang ke node jaringan. Keuntungan memiliki lokasi pengkabelan terpusat adalah lebih mudah untuk memelihara dan memecahkan masalah jaringan besar. Semua kabel jaringan datang ke hub pusat. Dengan cara

ini, sangat mudah untuk mendeteksi dan memperbaiki masalah kabel. Anda dapat dengan mudah memindahkan stasiun kerja ke dalam - topologi bintang - dengan mengubah koneksi ke hub di lemari kabel pusat.

Kerugian dari topologi star diberikan di bawah ini:

1. Kegagalan Hub dapat menonaktifkan sebagian besar jaringan.
2. Topologi Star memerlukan lebih banyak kabel dibandingkan topologi ring atau bus karena semua stasiun harus terhubung ke hub, bukan ke stasiun berikutnya.

**Karakteristik Segmen-ke-Segmen Hub**

Untuk memahami karakteristik segmen-ke-segmen Ethernet dari sebuah hub, pertama-tama mari kita tentukan cara kerja Hub Ethernet. Logikanya, mereka muncul sebagai Topologi Bus, dan secara fisik sebagai Topologi Star. Melihat ke dalam Hub Ethernet, kita dapat melihat bahwa itu terdiri dari papan sirkuit cetak elektronik. Memahami bahwa di dalam Hub hanya terdapat lebih banyak repeater, kita dapat menarik kesimpulan bahwa semua koneksi yang terpasang pada Hub berada pada Segmen yang sama (dan memiliki Nomor Segmen yang sama). Repeater tunggal dikatakan ada dari port mana pun ke port mana pun, meskipun diindikasikan sebagai jalur 2 repeater.

**Jaringan Hub Berjenjang**

Menghubungkan Hub bersama-sama melalui port menciptakan Cascading Hubs. Satu Hub Master (Level 1) terhubung ke banyak Hub Level 2 (Budak), yang merupakan master ke Hub Level 3 (Budak) dalam pohon hierarki (atau bintang berkelompok). Jumlah maksimum stasiun dalam Jaringan Cascaded Hub dibatasi hingga 128.

**Jaringan Tulang Punggung**

Di Jaringan Backbone, tidak ada Master Hub. Hub Level 1 terhubung melalui port AUI ke Coax Backbone. Untuk Thin Coax, hingga 30 Hub dapat dihubungkan secara bersamaan. Untuk Thick Coax, hingga 100 Hub dapat dihubungkan ke backbone. Tulang Punggung dianggap sebagai segmen berpenduduk.

Hub Level 2 diperbolehkan untuk dihubungkan ke 10 port BaseT Hub Level 1. Koneksi antara 2 Hub ini dianggap sebagai segmen tak berpenghuni, atau segmen tautan. Hingga 1024 stasiun (atau node) dapat dipasang ke 10 port BaseT Hub Level 2. Semua stasiun dan segmen akan muncul sebagai satu segmen logis, dengan satu Nomor jaringan. Perhatian Di dunia nyata, 1024 stasiun tidak pernah terhubung ke satu segmen; karena lalu lintas yang dihasilkan akan memperlambat perayapan jaringan.

**Pengalamatan Hub**

Karena Hub hanyalah sekumpulan repeater dalam kotak yang sama, lalu lintas jaringan antar node terdengar melalui seluruh jaringan. Sejauh menyangkut stasiun-stasiun, mereka terhubung pada satu bus logis (kabel) yang panjang.

**Hub Ethernet Setengah Dupleks dan Dupleks Penuh**

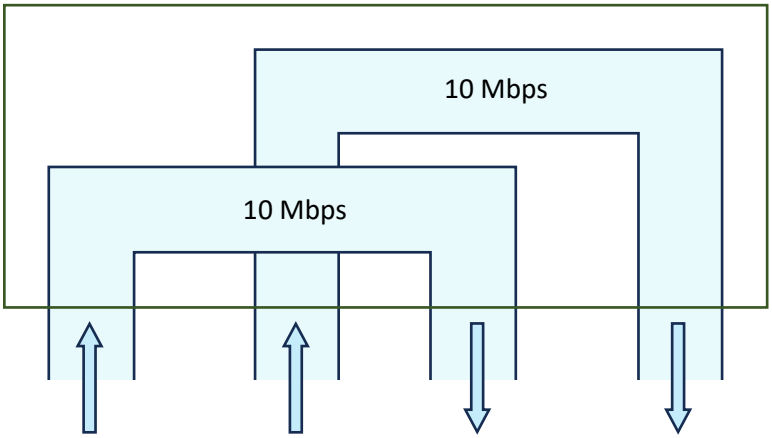
Operasi Ethernet normal adalah Half-Duplex: hanya 1 stasiun atau node yang berbicara pada satu waktu. Stasiun-stasiun bergiliran berbicara di dalam bus (CSMA/CD -arbitrase bus). Hub Ethernet Full-Duplex adalah Hub yang memungkinkan komunikasi dua arah, sehingga

menggandakan bandwidth yang tersedia dari 10 Mbps menjadi 20 Mbps. Hub dupleks penuh adalah produk eksklusif, dan biasanya hanya berfungsi dalam lini pabrikannya sendiri.

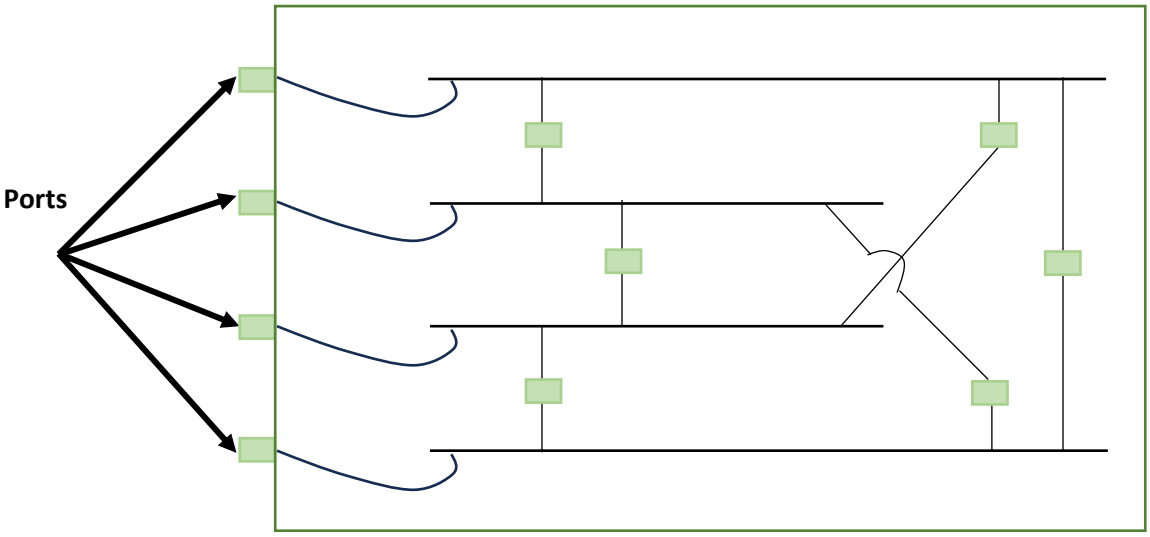
Misalnya, jika A ingin berbicara dengan C, jalur langsung 10 Mbps akan dihubungkan melalui 2 hub switching. Secara bersamaan, jika D ingin berbicara dengan B, jalur langsung 10 Mbps lainnya (dalam arah berlawanan) akan dihubungkan melalui dua Hub switching (menggandakan bandwidth yang tersedia menjadi 20 Mbps). Tidak ada standar resmi untuk Full-Duplex Ethernet meskipun standar kepemilikannya memang ada.

**Peralihan Hub**

Sebuah saklar yang menyerupai hub dikenal sebagai hub switching. Namun ada perbedaan mencolok antara hub dan switching hub atau switch. Hub bertindak sebagai konsentrator dan repeater LAN.




**Gambar 5.11 Switching Hub dengan Multiple Bus**




**Gambar 5.12 Konfigurasi Switch**

Ini terdiri dari satu kotak dengan banyak port. Setiap port terhubung dengan komputer terpisah. Sinyal yang dikirimkan oleh komputer berjalan ke semua port seperti topologi bus. Dengan evolusi teknologi jembatan, paket data yang dimasukkan ke satu port terlebih dahulu

diperiksa tujuannya dan dikeluarkan sesuai dengan port masing-masing. Dengan cara ini beberapa port dapat berkomunikasi secara bersamaan satu sama lain menggunakan switch. Dengan kata lain, dapat dikatakan bahwa hub switching memiliki banyak bus untuk beberapa LAN seperti yang ditunjukkan pada Gambar 5.11. Konfigurasi saklar ditunjukkan pada Gambar 5.12.

Hub switching mengartikan alamat MAC komputer tujuan yang terdapat dalam paket data dan mengirimkan paket data tersebut ke komputer tujuan yang sesuai menggunakan port yang sesuai ketika hub menggunakan teknik repeater dalam melakukannya. Oleh karena itu, switching hub diperlakukan sebagai jembatan.

**Karakteristik Switching Hub**

- Hub switching dapat beroperasi dengan banyak media (kabel koaksial, UTP, dan fiber).
- Ia dapat bekerja dengan teknologi berbeda dengan kecepatan berbeda.
- Ini juga menyediakan kemampuan perutean.
- Ini dapat dikelola melalui SNMP (Simple Network Management Protocol) atau protokol manajemen jaringan lain yang sesuai.
- Switching hub menyediakan bandwidth yang diperluas.

## 5.6 TEKNIK PERALIHAN

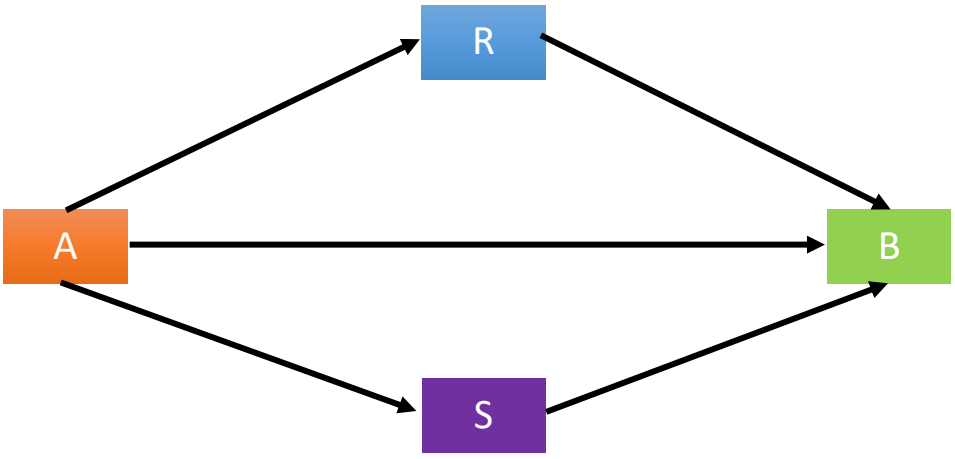
Sebuah Ethernet hanya dapat menghubungkan hingga 1024 host dalam rentang hanya 1500 meter. Oleh karena itu, teknologi LAN tidak cukup untuk membangun jaringan global dan menghubungkan host-host jaringan lain. Dalam pertukaran telepon, saklar menyediakan koneksi antara pihak yang dipanggil dan pihak yang menelepon tanpa menyediakan koneksi saluran-ke-saluran langsung di antara keduanya. Jaringan telepon menggunakan peralihan sirkuit yang menyediakan saluran khusus antara pihak yang dipanggil dan pihak yang menelepon, sedangkan jaringan komputer menggunakan peralihan paket yang tidak menyediakan saluran khusus antara host. Gambar 5.13 mencoba menjelaskan teknik switching dimana setiap komputer dapat bertukar informasi dengan komputer lain. Sakelar digunakan untuk menghubungkan host-host yang berbeda ke beberapa input dan outputnya. Fungsi switch adalah menyimpan dan meneruskan, routing dan kontrol kemacetan yang diperlukan untuk mencapai interkoneksi. Teknik switching memungkinkan kita membangun MAN atau WAN atau Internet.

Bayangkan bagaimana jadinya jika Anda hanya dapat menggunakan telepon untuk berbicara dengan satu orang saja! Anda tidak akan menjadi sangat produktif. Jadi, ada persyaratan untuk berpindah sistem untuk mengarahkan panggilan Anda ke seluruh dunia.
Ada beberapa cara untuk melakukan peralihan:

- Peralihan Sirkuit
- Peralihan Paket
- Peralihan Pesan
- Peralihan Sel

**Peralihan Sirkuit**

Teknik peralihan sirkuit menyediakan jalur komunikasi fisik khusus dari terminal sumber ke terminal tujuan dalam jaringan. Oleh karena itu, bandwidth khusus dibuat, dipelihara, dan diakhiri untuk setiap sesi komunikasi. Sesi peralihan sirkuit, dengan demikian, terdiri dari 3 fase seperti pembentukan sirkuit, transfer data, dan pemutusan sirkuit. Sebelum transfer data, koneksi khusus dibuat untuk transfer data. Di akhir transfer data, koneksi terputus. Dengan cara ini, peralihan sirkuit menyediakan saluran kecepatan data tetap untuk perangkat sumber dan tujuan. Teknik switching sirkuit mempunyai kelemahan dibandingkan teknik packet switching karena pemborosan bandwidth ketika tidak ada data untuk transmisi pada suatu saat. Selain itu, pengaturan koneksi juga membutuhkan waktu. Peralihan sirkuit melibatkan transmisi datagram dan aliran data. Transmisi datagram memiliki frame yang ditangani secara individual. Transmisi aliran data tidak memiliki bingkai. Mereka memiliki aliran data yang pemeriksaan alamatnya hanya dilakukan satu kali. Peruteannya bisa berupa perutean statis atau perutean dinamis. Gambar 5.13 menjelaskan rute khusus alternatif untuk transfer data dari satu host ke host lain.



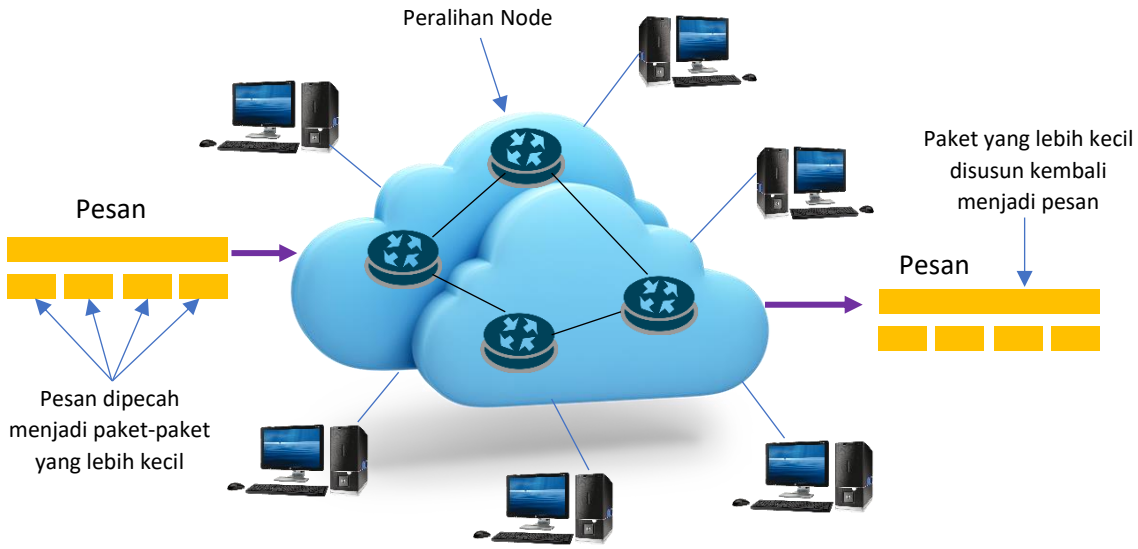

**Gambar 5.13: Rute Khusus Alternatif untuk Sambungan dari A ke B**

Awalnya, peralihan sirkuit dikembangkan untuk lalu lintas suara dan menemukan aplikasi di jaringan telepon untuk menyediakan sirkuit fisik khusus dari awal panggilan hingga akhir panggilan. Integrated Services Digital Network (ISDN) adalah salah satu contoh teknologi WAN berbasis sirkuit.

**Peralihan Paket**

Jaringan data packet-switched membagi data menjadi satu atau lebih unit pesan, yang disebut paket di host sumber sebelum mengirimkannya ke host tujuan. Paket-paket tersebut memiliki panjang yang bervariasi dan mencakup alamat sumber dan tujuan serta informasi kontrol yang diperlukan. Dalam jaringan switch, node switching menerima paket dan menyimpannya sebentar sebelum meneruskannya ke node berikutnya. Node switching memeriksa alamat tujuan yang terdapat dalam paket yang sampai di sana. Setiap node switching memelihara direktori routing dalam bentuk tabel untuk menentukan link keluar berdasarkan alamat tujuan paket yang diterima. Paket-paket tersebut akhirnya sampai ke node tujuan dan diteruskan ke perangkat tujuan. Perangkat tujuan mengumpulkan semua

paket data yang sama yang sampai ke sana dari rute berbeda dan mengaturnya secara berurutan sesuai dengan nomor urut yang terdapat dalam setiap paket.




**Gambar 5.14 Jaringan packet Switched**

Berbeda dengan peralihan sirkuit, peralihan paket tidak melibatkan saluran khusus untuk transfer informasi sehingga rentan terhadap kesalahan dan paket rusak atau hilang dalam rute dari perangkat sumber ke perangkat tujuan. Oleh karena itu, prosedur pengendalian kesalahan dan aliran diterapkan pada setiap link oleh node switching. Keuntungan dari packet switching adalah efisiensi saluran, tidak ada kondisi sibuk dan prioritas pengiriman data. Jaringan packet-switched membuat penggunaan kapasitas yang tersedia menjadi lebih efisien karena beberapa pengguna dapat berbagi bandwidth yang tersedia. Datagram perpindahan paket memperlakukan setiap paket secara independen dan paket mengambil rute apa pun untuk mencapai tujuan terlepas dari nomor urutnya. Perangkat tujuan merakit kembali paket-paket untuk mereproduksi pesan dan memulihkan paket-paket yang hilang. Peralihan paket memungkinkan untuk mengirimkan informasi yang sama ke lebih dari satu penerima pada waktu yang sama. Peralihan paket juga memungkinkan komunikasi antar terminal yang memiliki kecepatan transfer berbeda dan jenis antarmuka berbeda. Paket-paket tersebut ditangani menggunakan metode datagram dan sirkuit virtual serta sirkuit virtual permanen.

- **Datagram**: Ini mengacu pada paket data mandiri yang membawa informasi yang cukup untuk merutekannya secara andal dari perangkat sumber ke perangkat tujuan mengikuti rute apa pun. Perangkat tujuan mengumpulkan dan menyusun kembali paket-paket untuk merekonstruksi informasi. Kemungkinannya adalah beberapa paket mungkin hilang. Perangkat penerima kemudian meminta paket yang hilang.

**Sirkuit Virtual dan Sirkuit Virtual Permanen**

Ini mengacu pada pembuatan koneksi virtual antara perangkat sumber dan tujuan. Hal ini berbeda dengan peralihan sirkuit yang menciptakan koneksi fisik khusus. Koneksi virtual yang dibuat mungkin berorientasi koneksi atau tanpa koneksi. Datagram adalah contoh

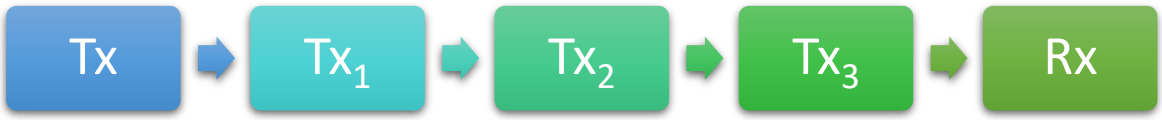
komunikasi tanpa koneksi. Peralihan paket menggunakan dua jenis koneksi virtual. Mereka adalah Switched Virtual Circuit (SVC) atau Virtual Circuit (VC) dan Permanent Virtual Circuit (PVC).

(a) **Koneksi Sirkuit Virtual** (VC): Seperti peralihan sirkuit, perangkat sumber memilih tautan atau rute yang akan digunakan untuk mengirim data ke perangkat tujuan sebelum komunikasi. Tautan terputus segera setelah paket ditransfer.

(b) **Sirkuit Virtual Permanen** (PVC): Seperti saluran sewaan, PVC adalah sirkuit virtual yang digunakan untuk membangun koneksi jangka panjang antara ujung pengirim dan penerima untuk tipe pengguna permanen yang selalu ingin terhubung ke saluran logis. Ini menghilangkan kebutuhan untuk pengaturan dan penghentian koneksi berulang kali. Hal ini disediakan oleh node switching yang menyimpan informasi secara permanen untuk transfer paket antara dua perangkat atau lebih.

**Peralihan Pesan**

Dalam peralihan pesan, tidak perlu ada koneksi yang dibuat dari sumber ke tujuan. Gambar 5.15 menunjukkan komunikasi antara Tx (perangkat pengirim atau pengirim) dan Rx (perangkat penerima) melalui sejumlah tautan seperti Tx ke $Tx_1$, $Tx_1$ ke $Tx_2$,$Tx_2$ ke $Tx_3$, $Tx_3$ ke Rx.




**Gambar 5.15: Koneksi antara Dua Sistem Tx dan Rx melalui 3 Link**

Node-node switching seperti $Tx_1$, $Tx_2$ dan seterusnya menerima pesan, menyimpannya dan meneruskan pesan ke node switching pesan yang berdekatan setelah membuat koneksi dengan switch pesan yang berdekatan. Peralihan pesan juga dikenal sebagai peralihan simpan dan teruskan karena pesan disimpan di node perantara dalam perjalanan ke tujuannya. Perbedaan antara perpindahan paket dan perpindahan pesan dapat dipahami dari ukuran paketnya. Pada kasus packet switching, ukuran paket sangat pendek dibandingkan dengan ukuran pesan pada message switching.

Paket berukuran pendek membutuhkan waktu lebih sedikit untuk mencapai tujuan dan oleh karena itu penyusunan kembali paket yang rusak tidak memerlukan koneksi khusus. Dengan demikian perpindahan paket memungkinkan paket-paket milik pesan lain dikirim di antara paket-paket lain. Peralihan paket menggunakan pipelining untuk membuat aliran paket yang berkelanjutan dari perangkat sumber ke perangkat tujuan melalui node peralihan perantara. Oleh karena itu, tautan dari perangkat sumber ke perangkat tujuan dan node perantara digunakan untuk mengirimkan paket secara bersamaan. Hal ini meningkatkan efisiensi saluran dan mengurangi total penundaan transmisi melalui jaringan paket dibandingkan dengan perpindahan pesan.

**Peralihan Sel**

Peralihan sel, terkait dengan Mode Transmisi Asinkron (ATM) dianggap sebagai teknologi peralihan kecepatan tinggi untuk mengatasi masalah kecepatan untuk aplikasi waktu nyata. Peralihan sel menggunakan jaringan packet-switched yang berorientasi koneksi. Dalam peralihan sel, koneksi dikenal sebagai pensinyalan. Peralihan sel menggunakan paket dengan panjang tetap 53 byte dimana 5 byte dicadangkan untuk header. Teknik packet switching menggunakan panjang paket yang bervariasi. Seperti halnya packet switching, teknik cell switching juga membagi pesan menjadi paket-paket yang lebih kecil namun panjangnya tetap. Keunggulannya adalah performa tinggi, arsitektur LAN/WAN yang umum, dukungan multimedia, bandwidth dinamis, dan skalabilitas. Performa tinggi dicapai karena penggunaan sakelar perangkat keras. Peralihan sel juga memiliki fitur layanan berorientasi koneksi dari peralihan sirkuit. Sirkuit virtual berorientasi koneksi untuk setiap fase mengalokasikan sumber daya tertentu untuk aliran lalu lintas yang berbeda.

**Perbedaan antara Circuit Switching dan Packet Switching**

Konsep dan ide pengalihan data (ke dalam jaringan switching sirkuit) ke dalam blok atau paket kecil sesuai dengan ukuran, konten atau strukturnya pertama kali diwakili oleh “Paul Baran” pada awal tahun 1960-an. Di sisi lain, Peralihan paket yang juga dikenal sebagai peralihan virtual juga ada dalam konten fitur jaringan.

Peralihan Sirkuit Vs. Peralihan paket sebenarnya mendefinisikan perbedaan antara dua metode peralihan yang berbeda. Sirkuit Vs. Packet Switching merupakan perbandingan mutlak antara kedua switching tersebut. Sirkuit Vs. Peralihan paket terjadi berdasarkan fitur yang berbeda dari dua jenis peralihan yang berbeda. Perbedaan penggunaan teknologi lama dan baru juga menjadi ciri pembanding utama antara keduanya yang mendukung Circuit switching Vs. Peralihan Paket.

Packet Switching merupakan teknologi switching yang lebih modern dan baru serta merupakan metode switching yang cocok dan terjangkau, sedangkan Circuit Switching adalah metode switching yang lama dan mahal, yang membuat garis perbedaan yang menonjol antara keduanya dan mendukung topik Circuit Vs. Peralihan paket. Sirkuit lainnya Vs. Fitur peralihan paket adalah pertentangan antara keandalan dan metode peralihan yang tidak dapat diandalkan.

Rangkaian catu daya switching adalah catu daya elektronik (PSU adalah unitnya) yang secara otomatis mengubah karakteristik volt dan arus ke yang lain. Rangkaian catu daya switching juga dilengkapi dengan regulator switching agar sangat efisien. Keuntungan utama dari rangkaian catu daya switching adalah mendapatkan bekal efisiensi yang besar karena transistor switching hanya membuang sedikit daya dan energi ketika berada di luar jangkauan wilayah sebenarnya. Jadi, rangkaian catu daya switching memiliki kepentingan tersendiri dan efisiensinya tetap sama jika situasi yang menantang dari Circuit switching Vs. Peralihan paket juga terjadi.

*Tugas* Berikan satu contoh masing-masing hal berikut:

(a) Peralihan sirkuit

(b) Peralihan paket

(c) Peralihan pesan
(d) Peralihan Sel

**Ringkasan**

- Pada unit ini Anda telah mempelajari berbagai jenis perangkat penghubung seperti hub, bridge, switch, router dan gateway.
- Bridge digunakan untuk menghubungkan beberapa LAN dua perangkat pada lapisan data link model OSI. Sakelar digunakan untuk menjalankan fungsi jembatan serta koneksi khusus point-to-point.
- Hub digunakan untuk menghubungkan berbagai koneksi masuk dengan koneksi keluar yang berbeda pada lapisan Fisik model OSI.
- Router digunakan untuk menghubungkan dua perangkat pada lapisan jaringan Model OSI. Router digunakan untuk menghubungkan LAN yang serupa dan berbeda dan mengoperasikan lapisan 3. Protokol router terdiri dari protokol penghubung dan perutean seperti antar-router, protokol jalur serial dan protokol perutean tumpukan dan protokol penghubung.
- Gateway digunakan untuk menghubungkan jaringan yang benar-benar berbeda karena mereka dapat melakukan konversi protokol untuk ketujuh lapisan Model OSI. Router gateway digunakan untuk menghubungkan LAN yang berbeda dan menjalankan semua fungsi bridge dan router. Ini beroperasi di ketujuh lapisan Model Referensi OSI. Sebuah hub switching dapat beroperasi dengan banyak media (kabel koaksial, UTP, dan fiber).
- Ada beberapa cara untuk melakukan switching seperti Circuit Switching, Packet Switching, Message Switching dan Cell Switching.

**Latihan Soal**

Beri nama berikut ini:

1. Tempat konvergensi dimana data datang dari satu atau lebih arah dan diteruskan ke satu atau lebih arah lainnya.
2. Perangkat yang memungkinkan administrator jaringan untuk melakukan segmentasi jaringan mereka secara transparan.
3. Perangkat yang menggabungkan fungsi jembatan serta 'koneksi khusus' titik-ke-titik. Mereka menghubungkan perangkat atau jaringan, menyaring, meneruskan dan membanjiri frame berdasarkan alamat tujuan MAC dari setiap frame.
4. Perangkat yang digunakan untuk menghubungkan dua perangkat pada lapisan jaringan Model OSI.
5. Perangkat yang digunakan untuk menghubungkan jaringan yang sama sekali berbeda karena mereka dapat melakukan konversi protokol untuk ketujuh lapisan Model OSI.

Isilah bagian yang kosong:

1. Kemampuan klasik “meneruskan pesan suara” di beberapa sistem pesan suara adalah contoh dari …….. Beralih

2. SEBUAH…….. rangkaian catu daya adalah catu daya elektronik (PSU adalah unitnya) yang secara otomatis mengubah karakteristik volt dan arus ke yang lain.
3. Peralihan rangkaian adalah……. dapat diandalkan daripada perpindahan paket.
4. Peralihan paket yang juga dikenal sebagai……. beralih.
5. ……sangat ideal untuk lingkungan terintegrasi dan ditemukan dalam jaringan berbasis seluler seperti ATM.

**Uraian**

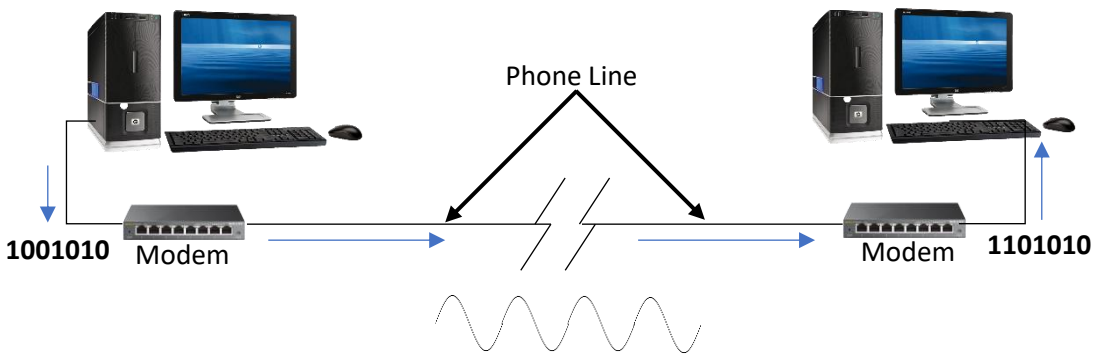
1. Apa tujuan utama penggunaan router dalam suatu jaringan?
2. Mengapa hub termasuk dalam kategori topologi bus sedangkan secara fisik termasuk dalam tipe topologi star?
3. Apa perbedaan jembatan dengan hub?
4. Jelaskan salah satu keuntungan dari routing statis dan dinamis mengapa mereka digunakan.
5. Router, bridge, dan repeater digunakan untuk menghubungkan jaringan yang berbeda. Dalam keadaan apa masing-masing teknologi ini akan digunakan?
6. Apa perbedaan jembatan dengan saklar?
7. Apa yang terjadi jika Anda mengganti hub dengan switch?
8. Apa yang dimaksud dengan peralihan? Jelaskan empat jenis peralihan.

# BAB 6
# MULTIPLEKSING

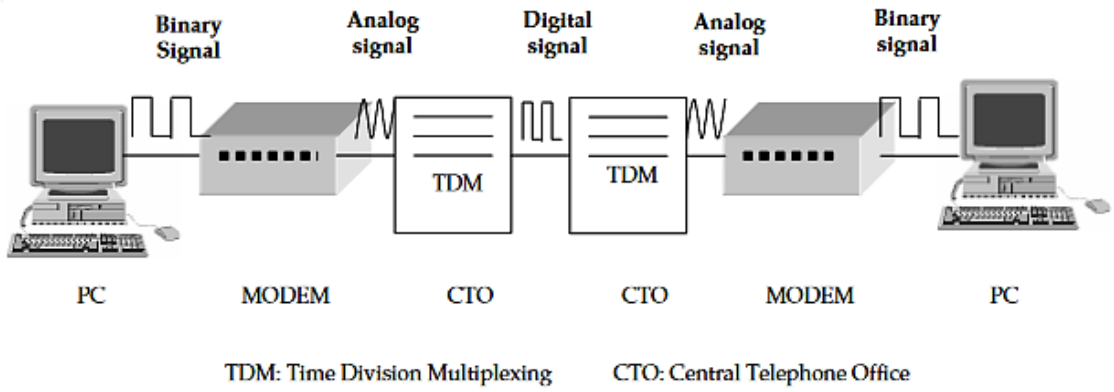
**Pendahuluan**

Dalam sistem komunikasi data, komunikasi digital dan analog secara bersama-sama memegang peranan yang sangat penting dan terintegrasi terlepas dari banyak kelebihan komunikasi digital dibandingkan analog. Gambar 6.1 menunjukkan peran integrasi komunikasi digital dan analog untuk melengkapi sistem komunikasi data.

Gambar 6.1 menunjukkan bahwa hubungan antar modem merupakan modulasi sinyal analog yang dihasilkan oleh modem. Demikian pula kita dapat mempertimbangkan Gambar 6.2 dimana sistem komunikasi data disajikan dalam arti yang lebih luas. Komunikasi dari PC ke modem terdiri dari sinyal biner sedangkan komunikasi antara Central Telephone Office (CTO) dan modem berlangsung dalam sinyal analog termodulasi. Komunikasi antara CTO dengan CTO lainnya dilakukan melalui sinyal digital dengan menggunakan time Division Multiplexer. Setelah itu CTO memasukkan sinyal analog termodulasi ke modem dan modem mengubahnya menjadi sinyal biner untuk PC. Sekarang kita dapat mengatakan bahwa berbagai jenis sinyal muncul pada tautan komunikasi dan mencapai CTO dalam perjalanan melintasi kota. Ini dapat dimultipleks untuk berbagi tautan komunikasi yang sama untuk transmisi ke tujuan.




**Gambar 6.1 Sistem Komunikasi data**




**Gambar 6.2 Komunikasi Data dalam Pengertian yang lebih luas**

Transmisi analog mengacu pada penyampaian informasi suara, data, gambar, sinyal atau video menggunakan sinyal kontinu yang bervariasi dalam amplitudo, fase, atau properti lain sebanding dengan variabel. Informasi dapat disampaikan menggunakan media kabel atau nirkabel seperti kabel twisted-pair atau coax, kabel serat optik, udara, air, dll. Modulasi amplitudo dan modulasi frekuensi adalah dua tipe dasar metode transmisi analog. Mereka didasarkan pada bagaimana mereka memodulasi data untuk menggabungkan sinyal masukan sidengan sinyal pembawa. Sampai saat ini, komunikasi telepon dan suara bersifat analog seperti halnya transmisi televisi dan radio. Transmisi analog masih digunakan untuk jarak pendek karena biayanya jauh lebih rendah. Transmisi digital mencari peralatan multiplexing dan pengaturan waktu yang kompleks yang tidak diperlukan untuk transmisi analog.

## 6.1 SIRKUIT, SALURAN DAN MULTISALURAN

Rangkaian adalah jalur antara dua titik atau lebih yang dilalui arus listrik. Dalam komunikasi data, rangkaian dianggap sebagai jalur spesifik antara dua titik atau lebih di mana sinyal dibawa. Sinyalnya mungkin analog, biner atau digital. Hal ini ditunjukkan pada Gambar 6.1 dan 6.2. Pada Gambar 6.1 dan Gambar 6.2 hubungan antara PC dan modem, modem, hubungan antara modem dan CTO dan seterusnya merupakan suatu rangkaian. Sirkuit mungkin berupa jalur fisik yang terdiri dari kabel atau mungkin nirkabel. Suatu jaringan, baik kabel maupun nirkabel, melibatkan sejumlah sirkuit yang terdiri dari sejumlah sakelar perantara. Suatu rangkaian diklasifikasikan berdasarkan kegunaannya seperti sambungan dial up, jalur sewaan, dll. Sambungan antara dua titik atau lebih juga dibuat secara virtual, tidak seperti sambungan yang dibuat melalui dial up dan jalur sewaan yang bersifat fisik. Sirkuit tersebut didefinisikan sebagai Sirkuit Virtual (VC) berdasarkan jenis dan sifat koneksi. Sirkuit virtual adalah jalur logis yang dipilih dari banyak kemungkinan jalur fisik yang tersedia antara dua titik atau lebih. Namun, koneksi dalam sirkuit virtual tidak dijamin.

Sirkuit virtual yang memastikan koneksi permanen antara dua titik disebut Sirkuit Virtual Permanen (PVC). PVC memberikan jaminan koneksi antara dua titik atau lebih bila diperlukan tanpa harus memesan jalur fisik tertentu terlebih dahulu. Switched Virtual Circuit (SVC) mirip dengan sirkuit virtual permanen dan memungkinkan pengguna untuk terhubung ke jaringan sirkuit virtual. Suatu rangkaian mungkin berisi banyak saluran secara bersamaan. Jaringan Digital Pelayanan Terpadu (ISDN) mendukung 2 saluran layanan Basic Rate Interface (BRI) dan 1 saluran persinyalan. Sirkuit Sinyal Digital 1 (DS1) mendukung 24 saluran 64-Kb/s, sedangkan sirkuit DS3 mendukung 612 saluran 64-Kb/s. Jumlah saluran dalam satu rangkaian ini dimungkinkan karena teknik multiplexing.

## 6.2 MULTIPLEKSING

Multiplexing adalah proses di mana beberapa saluran digabungkan untuk transmisi melalui jalur transmisi yang sama. Ada beberapa teknik berbeda untuk multiplexing:

- Multiplexing Pembagian Frekuensi (FDM)
- Multiplexing Pembagian Waktu (TDM)
- Multiplexing Divisi Kode (CDM)

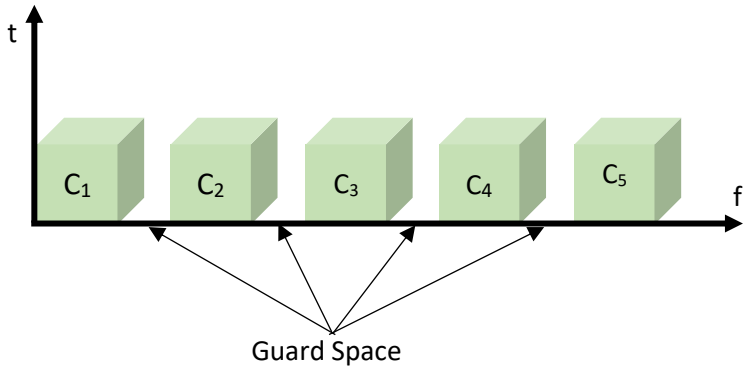
- Multiplexing Divisi Panjang Gelombang (WDM)

**Multiplexing Pembagian Frekuensi (FDM)**

Beberapa saluran digabungkan bersama untuk transmisi melalui satu saluran. Saluran dipisahkan berdasarkan frekuensinya. Dijelaskan pada Gambar 6.3 dimana suatu dimensi frekuensi dibagi menjadi beberapa pita frekuensi yang tidak tumpang tindih. Setiap saluran ci diberikan pita frekuensinya sendiri seperti yang digambarkan pada Gambar 6.3.

Selalu ada beberapa ruang frekuensi yang tidak terpakai antar saluran. Mereka dikenal sebagai band penjaga dan juga ditunjukkan pada Gambar 6.3. Mereka digunakan untuk mengurangi efek tumpang tindih antar saluran yang berdekatan. Tumpang tindih saluran yang berdekatan cenderung menghasilkan crosstalk.

FDM adalah skema multiplexing pertama yang banyak digunakan dalam penyebaran jaringan. Mereka masih digunakan sampai sekarang dan digunakan dengan transmisi analog. Namun, Time Division Multiplexing lebih disukai daripada FDM. Kerugian utama dari FDM adalah pemborosan sumber daya frekuensi karena didedikasikan untuk saluran tertentu sepanjang waktu. Ini juga membatasi jumlah saluran.



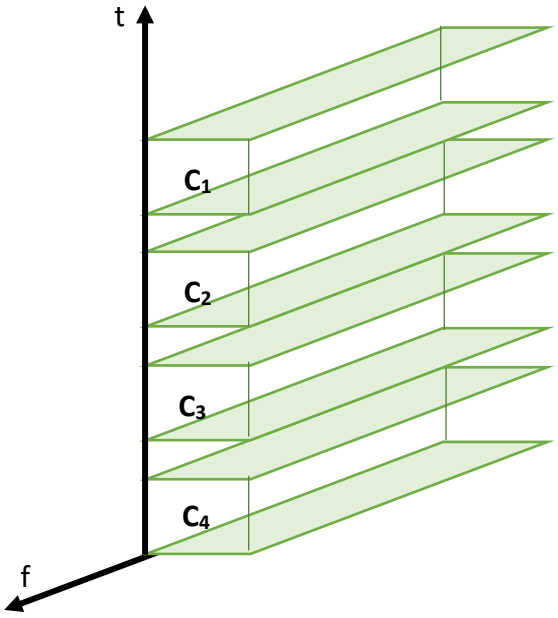

**Gambar 6.3 Frequency Division Multiplexing**

**Multiplexing Pembagian Waktu (TDM)**

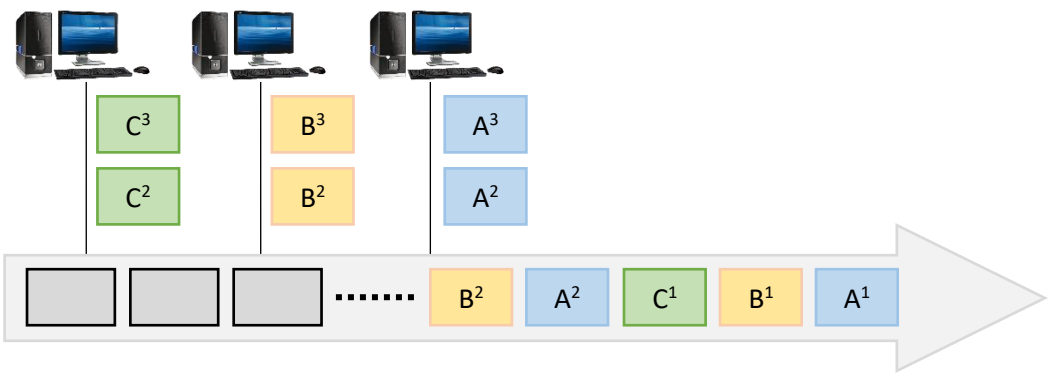
Dalam transmisi digital, Time Division Multiplexing (TDM) dan Code Division Multiplexing (CDM) banyak digunakan. TDM adalah proses menggabungkan data dari beberapa sumber ke dalam satu saluran untuk komunikasi melalui media transmisi seperti saluran telepon, sistem gelombang mikro, atau sistem satelit. TDM diimplementasikan dalam dua cara. Mereka adalah TDM sinkron dan TDM asinkron. TDM asinkron dikenal sebagai TDM Statistik (STDM). Teknik TDM sinkron membagi satu saluran ke dalam slot waktu dan masing-masing perangkat transmisi diberikan setidaknya satu slot waktu untuk transmisinya seperti yang ditunjukkan pada Gambar 6.4. Slot waktu ditetapkan sedemikian rupa sehingga setiap perangkat transmisi mendapatkan bagian yang diperlukan dari bandwidth yang tersedia. Karena teknik multiplexing bandwidth-waktu ini, TDM tidak sensitif terhadap protokol dan mampu menggabungkan berbagai protokol ke dalam satu tautan transmisi berkecepatan tinggi.

Dengan kata lain kita dapat mengatakan bahwa multiplekser mengalokasikan slot waktu yang sama persis ke setiap perangkat setiap saat, baik perangkat tersebut aktif atau menganggur. Beberapa perangkat, seperti sistem suara dan video mungkin memerlukan lebih banyak slot untuk memastikan bahwa data sampai pada link-end yang jauh tanpa terdistorsi karena kecepatan data yang lebih lambat. Slot waktu yang berbeda ini dikelompokkan ke dalam bingkai. Sebuah frame terdiri dari satu siklus slot waktu yang lengkap. Sebagai alternatif, Gambar 6.4 menjelaskan lebih jelas konsep TDM dalam lingkungan komunikasi data di mana tiga PC berbagi sirkuit yang sama. Paket-paket yang dihasilkan oleh masing-masing PC dimultipleks pada jalur umum sebagai A1, B1, C1 dan seterusnya.

Ini lebih fleksibel daripada FDM. Berbeda dengan FDM, seluruh bandwidth untuk jangka waktu tertentu diberikan kepada pengguna. Semua pengguna menggunakan frekuensi yang sama tetapi pada waktu yang berbeda. Alokasi waktu ini dapat bervariasi sesuai kebutuhan dan prioritas layanan pengguna. Pada Gambar 6.4 ditunjukkan ruang antara slot waktu yang berbeda, yang dikenal sebagai ruang penjaga dalam dimensi waktu. Ini digunakan untuk menghilangkan interferensi saluran bersama.




**Gambar 6.4 Time Division Multiplexing**




**Gambar 6.5 Time Slot dalam TDM**

Kerugian utama dari skema ini adalah diperlukannya sinkronisasi yang tepat antara pengirim yang berbeda untuk menghindari interferensi saluran bersama.

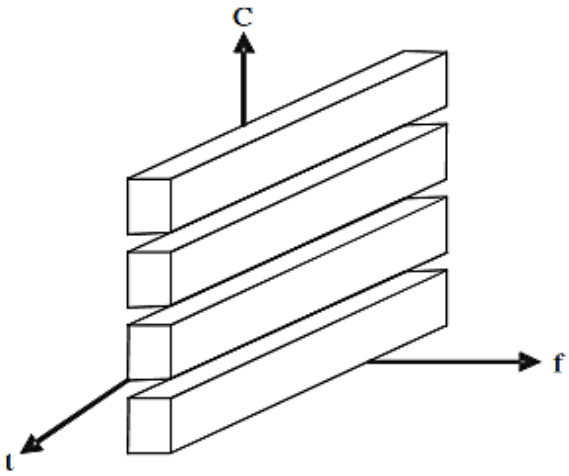
**Multiplexing Pembagian Waktu Statistik (STDM)**

Dalam kasus TDM, slot waktu dialokasikan ke saluran, meskipun saluran tersebut tidak memiliki informasi untuk dikirimkan. Ini hanyalah pemborosan bandwidth dan untuk mengatasi ketidakefisienan TDM standar ini, diterapkan teknik yang disebut STDM yang mana waktu dialokasikan ke saluran hanya berdasarkan permintaan. Hal ini dicapai dengan penggunaan perangkat cerdas yang mampu mengidentifikasi kapan terminal menganggur dan secara statistik mengkompensasi waktu menganggur normal sehingga lebih banyak saluran dapat dihubungkan ke media transmisi. Selama periode lalu lintas puncak, memori buffer menyimpan data untuk sementara sehingga waktu saluran berkecepatan tinggi dapat dimanfaatkan secara efektif dengan saluran aktif. Ini mengadopsi metodologi di mana setiap transmisi memiliki informasi identifikasi (pengidentifikasi saluran). Hal ini meningkatkan overhead, yang ditangani dengan mengelompokkan sejumlah karakter untuk setiap saluran untuk transmisi. Ini juga disebut sebagai TDM “Cerdas”.

Dalam hal ini, kapasitas kecepatan data jauh di bawah jumlah kapasitas terhubung masing-masing saluran karena saluran tersebut memanfaatkan waktu idle dengan sangat efektif. Ini hanya bersifat digital dan memerlukan pembingkaian data yang lebih kompleks. Ini banyak digunakan untuk komunikasi jarak jauh dengan banyak terminal. Layanan tambahan seperti kompresi data, prioritas jalur, jalur kecepatan campuran, berbagi port host, kontrol port jaringan, deteksi kecepatan otomatis, dll tersedia dengan teknik STDM.

**Code Division Multiplexing (CDM)/Spread Spectrum**

CDM banyak digunakan dalam komunikasi nirkabel 3G generasi kedua (2G) dan generasi ketiga. Teknologi ini digunakan dalam sistem telepon seluler frekuensi ultra tinggi (UHF) pada pita 800 MHz dan 1,9 GHz. Ini adalah kombinasi konversi analog-ke-digital dan teknologi spektrum tersebar. CDM dapat didefinisikan sebagai bentuk multiplexing dimana pemancar mengkodekan sinyal menggunakan urutan acak semu. CDM melibatkan sinyal digital asli dengan kode penyebaran. Hal ini mempunyai efek menyebarkan spektrum sinyal secara besar-besaran dan mengurangi kekuatan pada salah satu bagian spektrum. Di sisi lain, penerima mengetahui kode yang dihasilkan dan dikirimkan oleh pemancar dan oleh karena itu dapat memecahkan kode sinyal yang diterima. Setiap urutan acak yang berbeda berhubungan dengan saluran komunikasi yang berbeda dari beberapa stasiun.




**Gambar 6.6 Code Division Multiplexing (CDM)**

Code Division Multiplexing memberikan kodenya sendiri pada setiap saluran untuk memisahkannya satu sama lain. Kode-kode dasar yang unik ini, yang ketika didekodekan akan mengembalikan sinyal asli yang diinginkan sekaligus menghilangkan sepenuhnya efek saluran berkode lainnya. Ruang penjaga diwujudkan dengan menggunakan kode dengan kode ortogonal. Dalam kasus TDM dan FDM, saluran diisolasi berdasarkan slot waktu atau frekuensi terpisah, yang ditempati oleh semua pengguna. Gambar 6.6 menjelaskan bagaimana semua saluran Ci menggunakan frekuensi yang sama pada waktu yang sama untuk transmisi.

Satu bit dapat ditransmisikan dengan memodulasi serangkaian elemen sinyal pada frekuensi berbeda dalam urutan tertentu. Jumlah frekuensi berbeda per bit ini disebut sebagai kecepatan chip. Jika satu atau lebih bit ditransmisikan pada frekuensi yang sama, hal ini disebut dengan frekuensi hopping. Hal ini akan terjadi hanya jika kecepatan chip kurang dari satu karena kecepatan chip adalah rasio frekuensi dan bit. Di sisi penerima, penerima menerjemahkan bit 0 atau 1 dengan memeriksa frekuensi-frekuensi ini dalam urutan yang benar.

Kerugian dari CDM adalah bandwidth yang dikirimkan setiap pengguna lebih besar daripada kecepatan data digital sumbernya. Hasilnya adalah bandwidth yang terisi kira-kira sama dengan kecepatan yang dikodekan. Oleh karena itu CDM dan spread spektrum digunakan secara bergantian. Pemancar dan penerima memerlukan sirkuit elektronik yang kompleks. Keunggulan utama CDM adalah perlindungan dari gangguan dan penyadapan karena hanya pengirim dan penerima yang mengetahui kode penyebarannya.

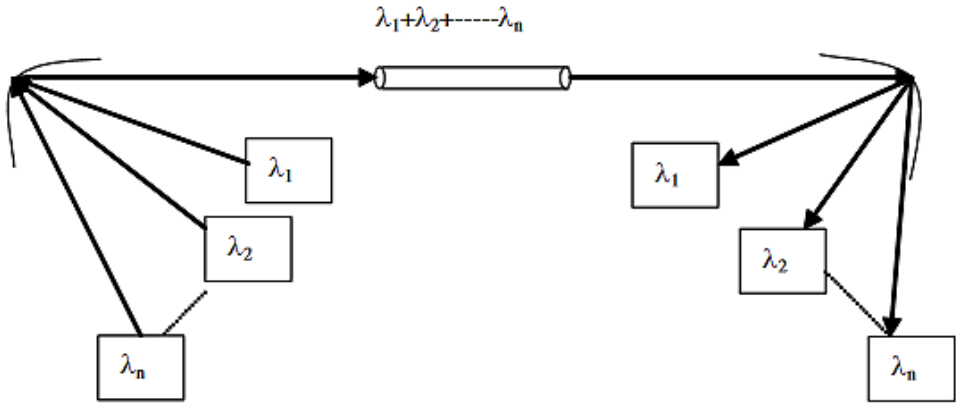
**Multiplexing Divisi Panjang Gelombang (WDM)**

Teknologi serat optik dianggap dapat memenuhi permintaan bandwidth yang terus meningkat untuk pertukaran informasi dan WDM memberikan solusi atas permintaan bandwidth yang terus meningkat melalui jaringan optik. Dalam komunikasi optik, analog FDM disebut sebagai distance-division multiplexing (WDM).

WDM dapat didefinisikan sebagai teknik transmisi serat optik yang menggunakan dua atau lebih sinyal optik yang memiliki panjang gelombang berbeda untuk mengirimkan data secara bersamaan dalam arah yang sama melalui satu serat, dan kemudian dipisahkan

berdasarkan panjang gelombang pada ujung yang jauh. WDM memungkinkan transmisi sinyal analog atau digital hingga beberapa GHz atau Gbits/s pada frekuensi operator yang sangat tinggi sekitar 190 THz (inframerah). Faktanya, menggunakan beberapa gelombang pembawa yang merambat tanpa interaksi signifikan pada kabel yang sama dapat meningkatkan bit rate lebih lanjut. Gelombang pembawa ini sesuai dengan panjang gelombang yang berbeda. Inilah alasan mengapa disebut Wavelength Division Multiplexing (WDM). Hubungan antara frekuensi dan panjang gelombang diberikan sebagai berikut: l = c/f dimana c dan f adalah kecepatan dan frekuensi sinyal dalam medium.

Dalam WDM beberapa sumber memancarkan pada panjang gelombang yang berbeda misalnya $\lambda_1$, $\lambda_2$, $\lambda_3$ dan seterusnya digabungkan ke dalam serat optik yang sama dan ini dipisahkan setelah transmisi pada serat menuju detektor yang berbeda pada ujung serat. Gambar 6.7 menjelaskan teknik WDM.




**Gambar 6.7: Multiplexing Pembagian Panjang Gelombang yang menunjukkan Panjang Gelombang berbeda yang dimultiplekskan Masuk dan Keluar dari Serat**

## 6.3 TEKNIK MODULASI MODEM

Sampai saat ini, komunikasi telepon dan suara sebagian besar bersifat analog dan saluran komunikasi seperti saluran telepon merupakan media transmisi analog. Media analog dianggap sebagai saluran dengan bandwidth terbatas. Bandwidth saluran telepon yang dapat digunakan berada pada kisaran 300 Hz hingga 3300 Hz. Sinyal digital yang berbentuk nilai diskrit tidak dapat ditransmisikan melalui media analog. Oleh karena itu, sinyal digital diubah menjadi sinyal analog sehingga saluran komunikasi dapat membawa informasi dari satu tempat ke tempat lain. Teknik yang memungkinkan konversi ini disebut modulasi. Pada dasarnya ada jenis modulasi berikut yang digunakan dalam modem. Ini adalah sebagai berikut:

- ASK – Penguncian Pergeseran Amplitudo
- FSK – Penguncian Pergeseran Frekuensi
- PSK – Penguncian Pergeseran Fase
- QPSK – Penguncian Bergeser Fase Kuadratur
- DPSK – Penguncian Pergeseran Fase Diferensial
- QAM – Modulasi Amplitudo Kuadratur

Modem menggunakan kombinasi teknik modulasi dan kompresi di atas untuk mencapai kecepatan transfer data yang tinggi.

## 6.4 MODULASI SINYAL DIGITAL

Transmisi digital menggunakan saluran low pass dengan bandwidth tinggi. Demikian pula, transmisi analog juga dimungkinkan pada saluran band pass yang memerlukan konversi data biner atau sinyal analog low pass menjadi sinyal analog band pass. Teknik ini disebut modulasi. Dengan demikian, modulasi data biner atau modulasi digital ke analog dilakukan dengan mengubah salah satu karakteristik sinyal analog sesuai dengan informasi pada sinyal digital. Informasi pada sinyal digital selalu berupa 0 dan 1. Ciri-ciri sinyal analog yang diubah adalah amplitudo, frekuensi dan fasa bentuk gelombang analog. Berdasarkan perubahan salah satu karakteristiknya, modulasi digital ke analog dapat berupa jenis penguncian pergeseran amplitudo (ASK), penguncian pergeseran frekuensi (FSK), dan penguncian pergeseran fasa (PSK). Modulasi amplitudo kuadratur adalah kategori keempat yang menggabungkan perubahan amplitudo dan fase untuk memberikan efisiensi yang lebih baik.

**Kecepatan Data**

Kecepatan bit adalah jumlah bit (0 atau 1) yang ditransmisikan selama 1 detik. Jumlah perubahan sinyal per satuan waktu untuk mewakili bit disebut kecepatan data modem. Tingkat tersebut biasanya dinyatakan dalam satuan yang dikenal sebagai baud. Unit sinyal mungkin memiliki 1 atau lebih dari 1 bit. Oleh karena itu, baud adalah berapa kali per detik kondisi saluran dapat beralih dari “1” ke “0”. Kecepatan baud dan kecepatan bit, yang dinyatakan dalam bit per detik, biasanya tidak sama, karena beberapa bit dapat ditransmisikan melalui saluran oleh modem pada setiap perubahan sinyal (beberapa bit dapat ditransmisikan sebagai satu simbol). Hubungan antara bit rate dan baud dinyatakan bahwa bit rate sama dengan baud rate dikalikan jumlah bit yang diwakili oleh setiap unit sinyal. Kecepatan bit selalu lebih besar atau sama dengan kecepatan baud. Alasan baud rate adalah menentukan bandwidth yang dibutuhkan untuk mengirimkan sinyal. Sinyalnya bisa berbentuk potongan atau blok yang mungkin berisi bit. Diperlukan bandwidth yang lebih sedikit untuk memindahkan unit sinyal ini dengan bit besar untuk sistem yang efisien. Untuk memahami hubungan antara bit dan baud rate, kami mempertimbangkan analogi mobil, penumpang, dan jalan raya dengan unit sinyal, bit, dan bandwidth masing-masing.

Sebuah mobil mempunyai kapasitas mengangkut maksimal 5 penumpang sekaligus. Misalkan sebuah jalan raya hanya dapat menampung 1000 mobil per satuan waktu tanpa kemacetan. Apabila setiap mobil di jalan raya mengangkut 5 penumpang, maka jalan raya tersebut dianggap mampu memberikan pelayanan tanpa kemacetan. Dengan demikian layanan jalan raya diperlakukan secara efisien. Pertimbangkan kasus lain, ketika 5000 penumpang ini ingin berangkat dengan mobil terpisah, mereka memerlukan 5000 mobil dan jalan raya hanya dapat mendukung 1000 mobil dalam satu waktu. Pelayanan yang diberikan semakin menurun karena kapasitas jalan raya hanya mampu menampung 1000 mobil. Tidak peduli apakah 1000 mobil ini mengangkut 1000 penumpang atau 5000 penumpang atau lebih.

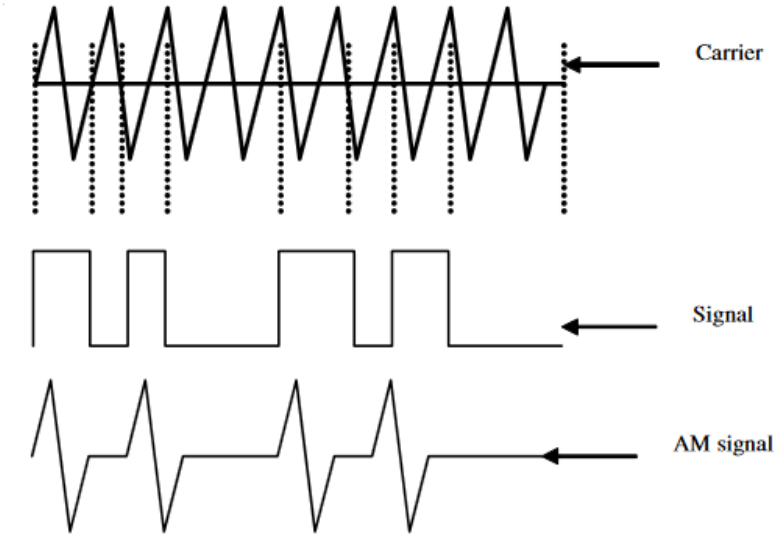
Untuk mendukung lebih banyak mobil, jalan raya perlu diperlebar. Demikian pula, jumlah baud menentukan bandwidth.

**Sinyal Pembawa**

Sinyal pembawa yaitu sinyal frekuensi tinggi memainkan peran penting dalam modulasi dan transmisi data. Ini adalah sinyal dasar yang dihasilkan oleh perangkat pengirim yang salah satu karakteristiknya diubah sesuai dengan sinyal digital yang akan dimodulasi. Sinyal modulasi atau sinyal digital yang melewati sinyal pembawa ditransmisikan ke perangkat penerima. Perangkat penerima disetel ke frekuensi sinyal pembawa. Keuntungan lain dari sinyal pembawa adalah menyediakan transmisi yang efisien antara perangkat pengirim dan perangkat penerima dan memerlukan ukuran antena yang lebih kecil karena frekuensi transmisi yang lebih tinggi.

**Penguncian Pergeseran Amplitudo (ASK)**

ASK menjelaskan teknik bagaimana gelombang pembawa dikalikan dengan sinyal digital f (t) sehingga kekuatan gelombang pembawa divariasikan untuk mewakili biner 0 dan 1. Dalam ASK, frekuensi dan fase gelombang analog dijaga seragam sedangkan amplitudo diubah sesuai dengan sinyal digital.



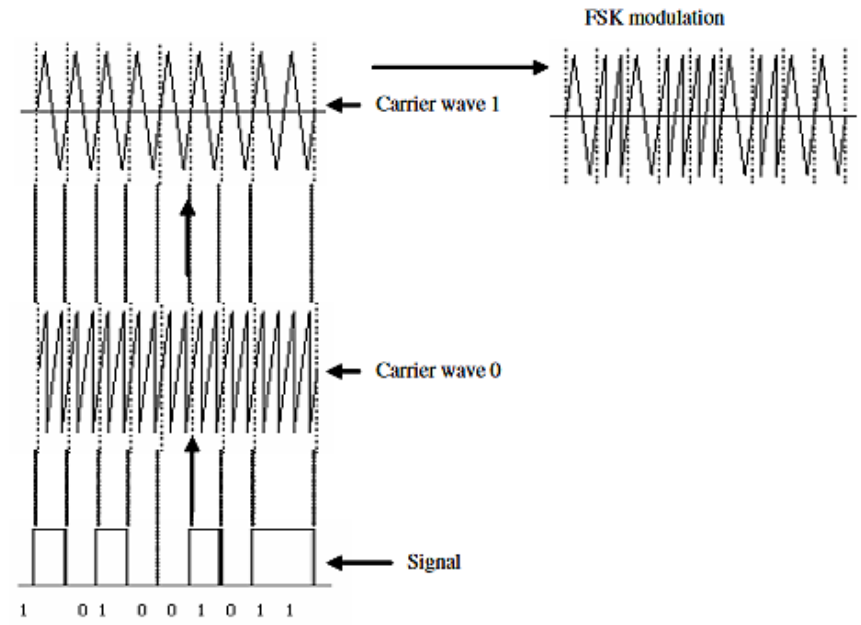

**Gambar 6.8 Menunjukkan teknik modulasi amplitudo.**

Keuntungan utama ASK adalah mudah untuk diproduksi dan dideteksi. Kekurangan ASK adalah sangat rentan terhadap interferensi noise yang mengubah amplitudo sinyal. Angka 0 dapat diubah menjadi 1 dan sebaliknya. Kelemahan lainnya adalah kecepatan perubahan amplitudo dibatasi oleh bandwidth saluran dan perubahan amplitudo yang kecil menyebabkan deteksi yang tidak dapat diandalkan. Saluran telepon membatasi perubahan amplitudo sekitar 3000 perubahan per detik. Kekurangan dari modulasi amplitudo menyebabkan teknik ini tidak lagi digunakan oleh modem, namun digunakan bersamaan dengan teknik lain.

**Penguncian Pergeseran Frekuensi**

FSK menjelaskan modulasi pembawa (atau dua pembawa) dengan menggunakan frekuensi berbeda untuk 1 atau 0. Dalam teknik ini frekuensi sinyal pembawa diubah sesuai data dengan tetap menjaga amplitudo dan fase konstan. Pemancar mengirimkan frekuensi yang berbeda untuk 1 dibandingkan 0 seperti yang ditunjukkan pada Gambar 6.9. Sinyal termodulasi yang dihasilkan dapat dianggap sebagai jumlah dari dua sinyal termodulasi amplitudo dari frekuensi pembawa yang berbeda.

Secara matematis, gelombang termodulasi y(t) dapat ditampilkan sebagai y(t) = f1(t) sin(2pfc1t + j) + f2(t) sin(2pfc2t + j) dengan fc1 dan fc2 adalah frekuensi pembawa berbeda dari dua gelombang berbeda. sinyal. FSK diklasifikasikan sebagai pita lebar jika pemisahan antara dua frekuensi pembawa lebih besar daripada bandwidth spektrumnya. FSK pita sempit adalah istilah yang digunakan untuk menggambarkan sinyal FSK yang frekuensi pembawanya dipisahkan kurang dari lebar spektrum dibandingkan ASK untuk modulasi yang sama.




**Gambar 6.9 Frequency Shift Keying**

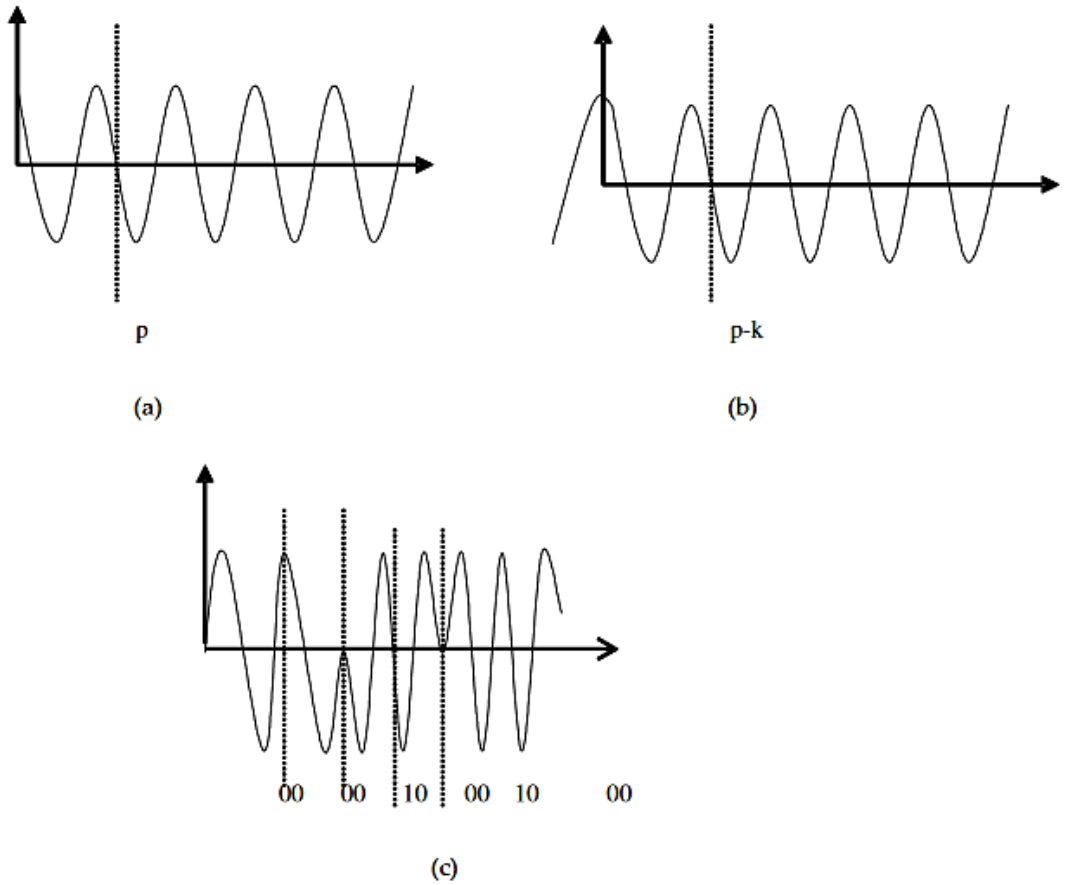
Keuntungan FSK adalah memberikan kekebalan yang lebih baik dari kebisingan karena perangkat penerima mencari perubahan frekuensi tertentu selama beberapa periode tertentu dan frekuensi hampir tidak terpengaruh oleh kebisingan. Kerugian dari teknik ini adalah sama seperti modulasi amplitudo. Laju perubahan frekuensi dibatasi oleh bandwidth saluran, dan distorsi yang disebabkan oleh saluran membuat pendeteksian menjadi lebih sulit daripada modulasi amplitudo. Saat ini teknik ini digunakan pada modem asinkron berkecepatan rendah hingga 1200 baud saja. Bandwidth untuk sinyal FSK adalah jumlah dari baud rate sinyal dan pergeseran frekuensi. Pergeseran frekuensi adalah perbedaan antara dua frekuensi pembawa.

**Penguncian Pergeseran Fase (PSK)**

Dalam metode modulasi ini gelombang sinus ditransmisikan dan fase gelombang sinus membawa data digital atau fase gelombang sinus divariasikan untuk mewakili biner 1 atau 0 dan amplitudo dan frekuensi bentuk gelombang analog dijaga konstan. Untuk 0, gelombang sinus fase 0 derajat ditransmisikan. Untuk 1, gelombang sinus 180 derajat ditransmisikan. Karena metode ini melibatkan dua keadaan perubahan fasa, maka disebut PSK biner atau 2-PSK. Teknik ini, untuk mendeteksi fasa setiap simbol, memerlukan sinkronisasi fasa antara fasa penerima dan pemancar.

Hal ini mempersulit desain receiver. Kelebihan PSK adalah kebal terhadap noise dan tidak dibatasi band.

- **Modulasi Fase Diferensial**: Sub metode modulasi fase adalah modulasi fase diferensial. Dalam metode ini, modem menggeser fase setiap sinyal berikutnya dalam sejumlah derajat tertentu, misalnya 0 untuk 90 derajat dan 1 untuk 270 derajat seperti diilustrasikan pada Gambar 6.10.




**Gambar 6.10 Phase Shift Keying**

PSK merupakan suatu teknik yang menggeser periode suatu gelombang. Gelombang pada Gambar 6.10 (a) mempunyai periode p yang dimulai dari 0. Gelombang pada Gambar 6.10 (b) merupakan gelombang yang sama seperti pada Gambar 6.10 (a), namun fasanya telah bergeser. Perhatikan bahwa periode dimulai pada titik tertinggi gelombang 1 pada sumbu vertikal. Kebetulan kita telah menggeser gelombang ini sebanyak seperempat periode penuh

gelombang tersebut. Kita dapat menggesernya seperempat lagi, jika kita mau, sehingga gelombang aslinya akan bergeser setengah periodenya. Dan kita bisa melakukannya sekali lagi, sehingga bergeser tiga perempat dari periode aslinya.

Ini berarti terdapat 4 gelombang terpisah dan oleh karena itu setiap gelombang disediakan untuk beberapa nilai biner. Karena ada 4, 2 bit disediakan untuk setiap gelombang yang direpresentasikan di bawah ini:

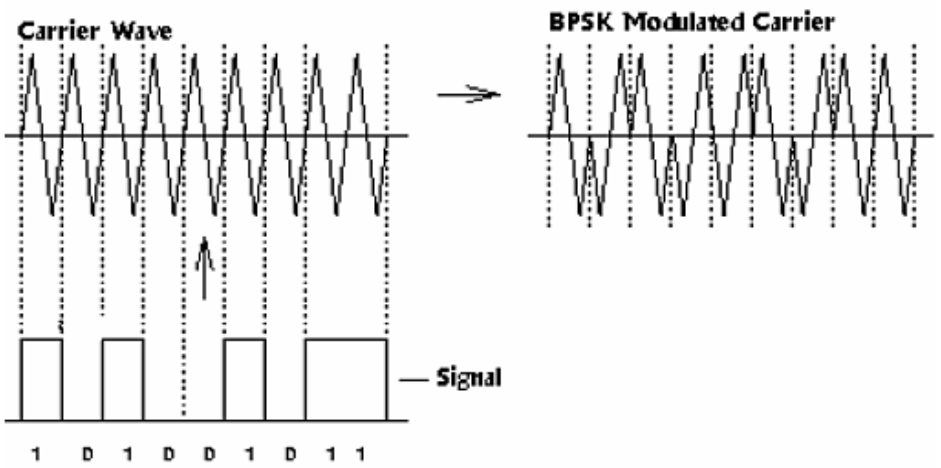
| Nilai sedikit | Jumlah Pergeseran |
|---|---|
| 00 | Tidak ada |
| 01 | ¼ |
| 10 | ½ |
| 11 | ¾ |

Teknik yang membiarkan setiap pergeseran gelombang mewakili beberapa nilai bit adalah penguncian pergeseran fasa. Namun kunci sebenarnya adalah menggeser setiap gelombang relatif terhadap gelombang sebelumnya. PSK menjelaskan teknik modulasi yang mengubah fase pembawa. Secara matematis dapat direpresentasikan sebagai y(t) = f(t) sin(2pfct + j(t)) dengan jc adalah pergeseran fasa. Cara ini lebih mudah dideteksi dibandingkan cara sebelumnya. Penerima harus mendeteksi pergeseran fasa antar simbol dan bukan fasa absolut.

Penguncian Pergeseran Fasa Biner (BPSK): Dalam kasus dua kemungkinan pergeseran fasa, modulasinya akan disebut BPSK - biner PSK. Dalam kasus 4 kemungkinan pergeseran fasa yang berbeda untuk setiap simbol yang berarti bahwa setiap simbol mewakili 2 bit maka modulasinya disebut quadrature PSK (QPSK), dan dalam kasus 8 pergeseran fasa yang berbeda maka teknik modulasinya disebut 8-PSK.

Saluran data tunggal memodulasi operator. Transisi bit tunggal, 1 ke 0 atau 0 ke 1, menyebabkan pergeseran fasa 180 derajat pada pembawa. Dengan demikian, pembawa dikatakan termodulasi oleh data. Karena ini hanya memiliki dua fase, 0 dan 1. Oleh karena itu, ini adalah jenis ASK dengan nilai -1 atau 1 dan bandwidthnya sama dengan ASK. Penguncian pergeseran fasa menawarkan cara sederhana untuk meningkatkan jumlah level dalam transmisi tanpa menambah bandwidth dengan memperkenalkan pergeseran fasa yang lebih kecil. Penguncian pergeseran fase kuadratur (QPSK) memiliki empat fase seperti 0, p/2, p, 3p/2. Akibatnya, M-ary PSK mempunyai tahapan M yang diberikan pada pukul 14.00/M; m = 0,1…M-1. Untuk kecepatan bit tertentu, QPSK memerlukan setengah bandwidth PSK dan banyak digunakan karena alasan ini.

Tahukah kamu? Berapa kali parameter sinyal (amplitudo, frekuensi, dan fase) diubah per detik disebut laju sinyal. Itu diukur dalam baud. 1 baud = 1 perubahan per detik. Dengan modulasi biner seperti ASK, FSK dan BPSK, laju pensinyalan sama dengan laju bit. Dengan QPSK dan M-ary PSK, kecepatan bit mungkin melebihi kecepatan baud.



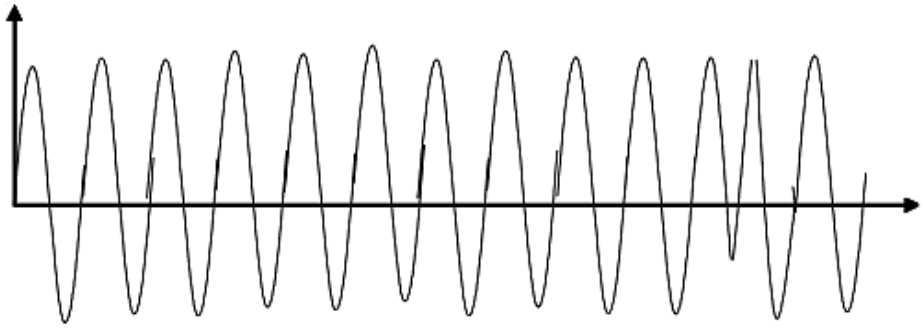

**Gambar 6.11 Binary Phase Shift Keying**

**Penguncian Pergeseran Fase Kuadratur (QPSK)**

Dua saluran data memodulasi operator. Transisi dalam data menyebabkan pembawa bergeser 90 atau 180 derajat. Hal ini memungkinkan transmisi dua aliran data terpisah, yang diidentifikasi sebagai data saluran I (Dalam fase) dan saluran Q (Kuadrat). Dalam metode ini empat sudut fase yang berbeda digunakan.

**Penguncian Pergeseran Fase Diferensial (DPSK)**

DPSK mengubah fase gelombang pembawa, bukan frekuensi. Ini digunakan untuk transmisi digital di mana fase pembawa divariasikan secara diskret sehubungan dengan fase elemen sinyal yang mendahuluinya dan sesuai dengan data yang ditransmisikan. Pergeseran fase terjadi dari fase sekarang dan bukan dari standar absolut oleh karena itu teknik ini disebut DPSK. Kerugian dari DPSK adalah BER vs. SNR yang lebih tinggi dibandingkan BPSK (sekitar 1 dB).



**Gambar 6.12 menunjukkan DPSK menggunakan dua perubahan fasa yaitu 0 adalah pergeseran fasa 00 dan 1 adalah perubahan fasa 1800.**

**QAM (Modulasi Amplitudo Kuadratur)**

Teknik ini didasarkan pada modulasi amplitudo dan modulasi fasa untuk meningkatkan kinerja modulasi amplitudo. Secara teoritis, sejumlah perubahan amplitudo dapat dikaitkan dengan sejumlah perubahan fase. Misalnya, dua sinyal pembawa ditransmisikan secara bersamaan pada frekuensi yang sama dengan pergeseran fasa 90 derajat. QAM bermaksud untuk menggabungkan manfaat modulasi penguncian amplitudo dan pergeseran fasa. Ini

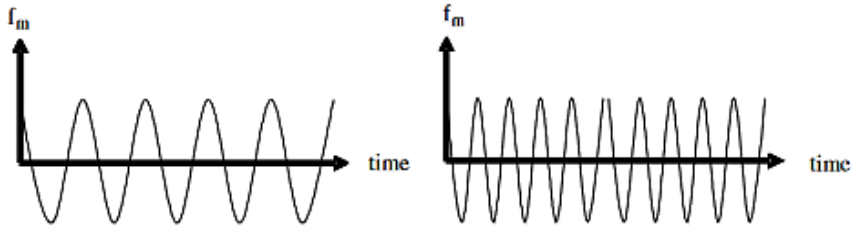
melibatkan lebih sedikit jumlah pergeseran amplitudo daripada pergeseran fasa karena modulasi amplitudo rentan terhadap kebisingan. Bandwidth minimum yang diperlukan untuk QAM setara dengan bandwidth minimum yang diperlukan untuk ASK dan PSK.

## 6.5 MODULASI SINYAL ANALOG

Modulasi adalah tindakan menerjemahkan beberapa frekuensi rendah (sinyal pita dasar) seperti suara, data, dll ke frekuensi yang lebih tinggi. Modulasi/demodulasi adalah proses nonlinier di mana dua sinusoid berbeda dikalikan. Dalam proses modulasi, beberapa karakteristik pembawa sinusoidal frekuensi tinggi $f_c$ seperti yang ditunjukkan pada Gambar diubah berbanding lurus dengan amplitudo sesaat sinyal pita dasar sebagai $f_m$ pada Gambar 6.13. Mari kita asumsikan dua sinusoida seperti yang ditunjukkan pada Gambar 6.13 sebagai $f_m$ dan $f_c$ masing-masing sebagai sinyal pita dasar dan pembawa dan direpresentasikan sebagai:

$$f_m = A \sin \omega_m t + \emptyset_1 \qquad (6.1)$$
$$f_c = B \sin \omega_c t + \emptyset_2 \qquad (6.2)$$

Dalam persamaan 2, baik amplitudo B atau frekuensi sudut wc dapat divariasikan sesuai dengan persamaan 1 dan dengan demikian menghasilkan masing-masing modulasi amplitudo atau modulasi frekuensi atau modulasi fasa. Frekuensi sudut didefinisikan sebagai 2p kali frekuensi sinyal pembawa.




**Gambar 6.13 Dua Perbedaan Sinusioda**

Dengan kata lain, modulasi digunakan untuk menempatkan pesan (suara, gambar, data, dll.) ke gelombang pembawa untuk transmisi. Frekuensi yang menyusun pesan (pita dasar) diterjemahkan ke rentang frekuensi yang lebih tinggi. Frekuensi yang terkandung dalam pesan dipertahankan, yaitu setiap frekuensi dalam pesan tersebut diskalakan dengan nilai konstan seperti dijelaskan di atas. Modulasi diperlukan untuk komunikasi data karena beberapa alasan. Hal ini memungkinkan transmisi simultan dari dua atau lebih sinyal pita dasar dengan menerjemahkannya ke frekuensi yang berbeda. Ini juga mengurangi ukuran antena untuk frekuensi yang lebih tinggi dengan efisiensi yang lebih besar.

**Antar Modulasi**

Intermodulasi adalah kasus khusus dimana dua (atau lebih) sinusoid saling mempengaruhi untuk menghasilkan produk yang tidak diinginkan, yaitu frekuensi yang tidak diinginkan (noise). Sekali lagi, hal ini hanya dapat terjadi jika kedua gelombang menggunakan perangkat non-linier yang sama. Ketidaklinieran menghasilkan beberapa harmonik genap atau

ganjil. Harmonisa adalah kelipatan frekuensi dasar, yaitu frekuensi pesan. Indeks modulasi adalah rasio puncak sinyal modulasi dengan puncak sinyal pembawa jika terjadi modulasi amplitudo. Dalam modulasi sudut, rasio deviasi frekuensi sinyal termodulasi dengan frekuensi sinyal modulasi sinusoidal.

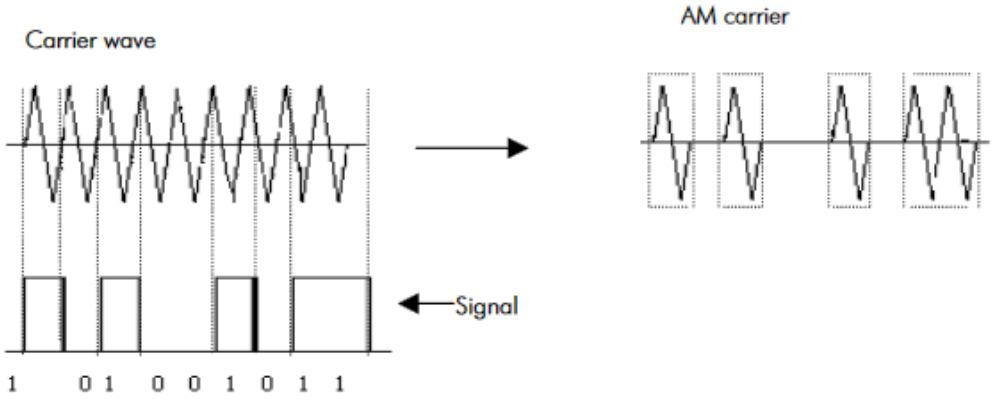
**Modulasi Amplitudo**

Ini menjelaskan teknik di mana gelombang pembawa dikalikan dengan sinyal digital f(t). Secara matematis, sinyal pembawa termodulasi y(t) adalah: y(t) = f(t) sin(2p¦ct+j) dengan fc adalah frekuensi pembawa dan t adalah waktu sesaat. Gambar 6.14 menunjukkan teknik modulasi amplitudo.

Keuntungan utama dari teknik ini adalah mudahnya menghasilkan sinyal tersebut dan juga mendeteksinya. Teknik ini memiliki dua kelemahan utama. Yang pertama adalah kecepatan perubahan amplitudo dibatasi oleh bandwidth saluran. Kedua, perubahan amplitudo yang kecil menyebabkan deteksi yang tidak dapat diandalkan. Saluran telepon membatasi perubahan amplitudo sekitar 3000 perubahan per detik. Kekurangan dari modulasi amplitudo menyebabkan teknik ini tidak lagi digunakan oleh modem, namun digunakan bersamaan dengan teknik lain.

**QAM (Modulasi Amplitudo Kuadratur)**

Teknik ini didasarkan pada modulasi amplitudo dasar. Teknik ini meningkatkan kinerja modulasi amplitudo dasar. Dalam teknik ini dua sinyal pembawa ditransmisikan secara bersamaan. Kedua sinyal pembawa berada pada frekuensi yang sama dengan pergeseran fasa 90 derajat.




**Gambar 6.14 Modulasi Amplitudo**

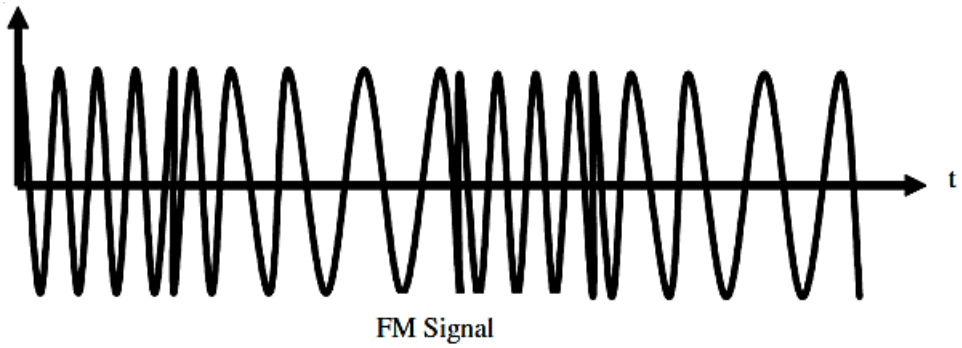
**Modulasi Frekuensi**

Modulasi Frekuensi melibatkan modulasi frekuensi gelombang sinus analog di mana frekuensi sesaat pembawa menyimpang sebanding dengan deviasi pembawa termodulasi terhadap frekuensi amplitudo sesaat dari sinyal modulasi. Secara sederhana dapat dikatakan bahwa ini terjadi ketika frekuensi pembawa diubah berdasarkan amplitudo sinyal masukan. Berbeda dengan AM, amplitudo sinyal pembawa tidak berubah. Hal ini membuat modulasi FM lebih kebal terhadap kebisingan dibandingkan AM dan meningkatkan rasio signal-to-noise secara keseluruhan pada sistem komunikasi. Keluaran dayanya juga konstan, berbeda dengan keluaran daya AM yang bervariasi. Jumlah bandwidth analog yang diperlukan untuk

mentransmisikan sinyal FM lebih besar daripada jumlah yang diperlukan untuk AM, sehingga menjadi batasan bagi beberapa sistem. Indeks modulasi untuk FM diberikan seperti di bawah ini:

$\beta = f_p/f_m$, dimana

$\beta$ = Indeks modulasi, $f_m$ = frekuensi sinyal modulasi dan $f_p$ = deviasi frekuensi puncak




**Gambar 6.15 Modulasi Frekuensi**

Dari Gambar 6.15, disimpulkan bahwa amplitudo sinyal termodulasi selalu konstan, terlepas dari frekuensi dan amplitudo sinyal modulasi. Ini berarti bahwa sinyal modulasi tidak menambahkan daya ke pembawa dalam modulasi frekuensi, tidak seperti modulasi amplitudo. FM menghasilkan pita samping dalam jumlah tak terhingga yang diberi jarak oleh frekuensi modulasi, sedangkan fm tidak berlaku untuk AM. Oleh karena itu, AM dianggap sebagai proses linier sedangkan FM dianggap sebagai proses nonlinier. Penting untuk mentransmisikan semua pita samping untuk mereproduksi sinyal bebas distorsi. Idealnya, bandwidth dari sinyal termodulasi dalam kasus ini tidak terbatas. Secara umum penentuan kandungan frekuensi bentuk gelombang FM rumit, tetapi jika b kecil, bandwidth sinyal FM adalah 2fm. Sebaliknya, jika b besar, bandwidth ditentukan (secara empiris) sebesar 2 fm (1 + b).

**Modulasi Fase**

Modulasi Fase (PM) mirip dengan modulasi frekuensi. Alih-alih frekuensi gelombang pembawa berubah, fase gelombang pembawa pun berubah. Dalam PM, fase pembawa dibuat sebanding dengan amplitudo sesaat dari sinyal modulasi. Indeks modulasi untuk PM diberikan sebagai b = Dj, dimana Dj adalah deviasi fase puncak dalam radian. Seperti dalam kasus modulasi sudut, argumen sinusoidal bervariasi dan oleh karena itu kita akan memiliki sifat sinyal resultan yang sama untuk modulasi frekuensi dan fase. Perbedaan dalam hal ini hanya dapat dibuat dengan perbandingan langsung antara sinyal dengan gelombang sinyal modulasi, seperti yang ditunjukkan pada Gambar 6.16.


**Gambar 6.16 Modulasi Fase (PM)**

Perhatian Modulasi fase dan modulasi frekuensi dapat dipertukarkan dengan memilih respons frekuensi modulator sehingga tegangan keluarannya akan sebanding dengan integrasi sinyal modulasi dan diferensiasi sinyal modulasi. Masalah bandwidth dan daya sama dengan masalah modulasi frekuensi.

**Perbandingan FM dan AM**

Keuntungan utama FM dibandingkan AM adalah:

1. Peningkatan rasio sinyal terhadap kebisingan (sekitar 25dB) w.r.t. terhadap campur tangan buatan manusia.
2. Interferensi geografis yang lebih kecil antar stasiun tetangga.
3. Daya pancarannya lebih sedikit.
4. Area layanan yang ditentukan dengan baik untuk daya pemancar tertentu. Kekurangan FM adalah:
   ※ Bandwidth Lebih Banyak (sebanyak 20 kali lipat).
   ※ Penerima dan pemancar yang lebih rumit.

**Ringkasan**

- Sirkuit adalah jalur antara dua titik atau lebih yang dilalui sinyal. Sirkuit mungkin berupa jalur fisik yang terdiri dari kabel atau mungkin nirkabel. Suatu jaringan, baik kabel maupun nirkabel, melibatkan sejumlah sirkuit yang terdiri dari sejumlah sakelar perantara.
- Sirkuit virtual adalah jalur logis yang dipilih dari banyak kemungkinan jalur fisik yang tersedia antara dua titik atau lebih.
- Multiplexing adalah proses di mana beberapa saluran digabungkan untuk transmisi melalui jalur transmisi yang sama.
- Dalam FDM, beberapa saluran digabungkan untuk transmisi melalui satu saluran.
- TDM adalah proses menggabungkan data dari beberapa sumber ke dalam satu saluran untuk komunikasi melalui media transmisi seperti saluran telepon, sistem gelombang mikro, atau sistem satelit. TDM asinkron dikenal sebagai TDM Statistik (STDM). Teknik TDM sinkron membagi satu saluran ke dalam slot waktu dan masing-masing perangkat transmisi diberikan setidaknya satu slot waktu untuk transmisinya.
- CDM didefinisikan sebagai suatu bentuk multiplexing dimana pemancar mengkodekan sinyal menggunakan urutan acak semu.

- WDM didefinisikan sebagai teknik transmisi serat optik yang menggunakan dua atau lebih sinyal optik yang mempunyai panjang gelombang berbeda untuk mengirimkan data secara bersamaan dalam arah yang sama melalui satu serat, dan kemudian dipisahkan berdasarkan panjang gelombang pada ujung yang jauh.
- SDMA adalah teknologi akses paling populer untuk komunikasi satelit dimana antena parabola sering dan banyak digunakan.
- FDMA membagi pita frekuensi menjadi berbagai saluran berdasarkan teknik FDM. Masing-masing dapat melakukan percakapan suara atau, dengan layanan digital, membawa data digital.
- TDMA adalah teknologi transmisi digital yang memungkinkan sejumlah saluran mengakses satu saluran frekuensi radio (RF) tanpa gangguan dengan mengalokasikan slot waktu unik untuk setiap saluran.
- Transmisi digital memerlukan saluran low pass dengan bandwidth tinggi. Transmisi analog dapat dilakukan pada saluran band pass. Berbagai metode yang mengubah data biner atau sinyal analog low pass menjadi sinyal analog band pass disebut modulasi.
- Konversi digital ke analog meliputi ASK (Amplitude Shift Keying), FSK (Frequency Shift Keying), PSK (Phase Shift Keying), QPSK (Quadrature Phase Shift Keying), QAM (Quadrature Amplitude Modulation) dan telah dijelaskan pada bagian Modem Teknik Modulasi.
- Konversi sinyal analog ke analog melibatkan teknik modulasi amplitudo, modulasi frekuensi, dan modulasi fasa.

**Latihan Soal**

Isilah bagian yang kosong:

1. CDM banyak digunakan dalam komunikasi yang disebut generasi kedua (2G) dan 3G generasi ketiga ……..
2. Dalam komunikasi optik, analog FDM disebut ……..
3. TDM adalah proses menggabungkan data dari beberapa sumber ke dalam satu saluran untuk komunikasi melalui ……..
4. …….. adalah jalur logis yang dipilih dari banyak kemungkinan jalur fisik yang tersedia antara dua titik atau lebih.
5. …….. dianggap sebagai jalur tertentu antara dua titik atau lebih di mana sinyal dibawa.

Nyatakan apakah pernyataan berikut ini benar atau salah:

1) Modulasi adalah tindakan menerjemahkan beberapa frekuensi tinggi (sinyal pita dasar) seperti suara, data, dll ke frekuensi yang lebih rendah.
2) Modulasi Amplitudo (AM) melibatkan modulasi amplitudo pembawa sebagai gelombang sinus analog.
3) FM dianggap sebagai proses linier sedangkan AM sebagai proses nonlinier.
4) Dalam PM, fase pembawa dibuat sebanding dengan amplitudo sesaat dari sinyal modulasi.

5) Konversi sinyal analog ke analog hanya melibatkan teknik modulasi amplitudo dan modulasi frekuensi.

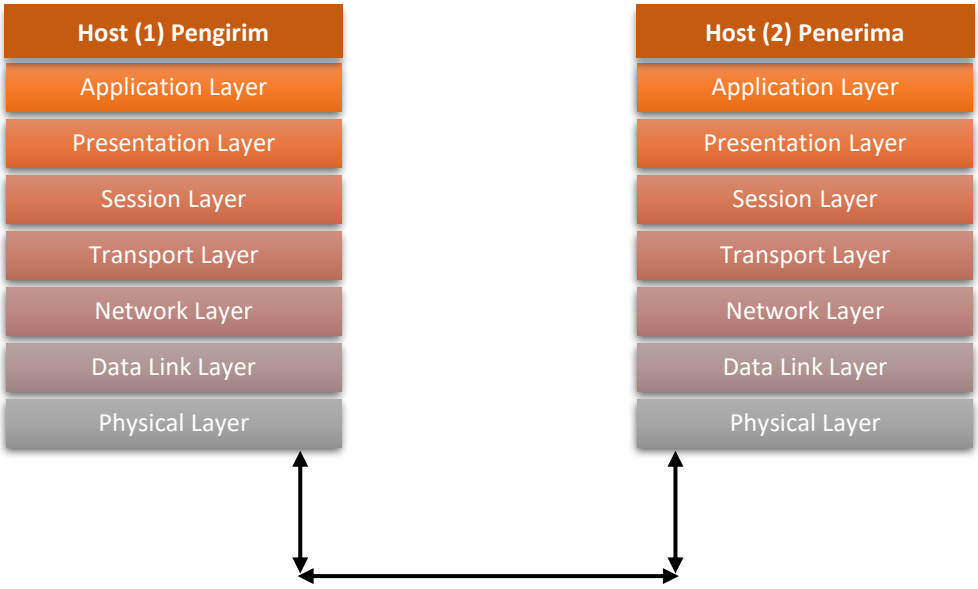
**Uraian**

1. Kapan suatu saluran disebut rangkaian?
2. Bagaimana multi-channeling membantu transmisi broadband?
3. Bagaimana satu transmisi dapat dibagi di antara sinyal-sinyal yang berbeda? Jelaskan dua metode apa pun.
4. Mengapa metode TDM dan FDM digunakan untuk digunakan dalam sistem telepon, namun tidak untuk jaringan komputasi?
5. Apa tujuan dari guard band di FDM?
6. Bagaimana satu transmisi dapat dibagi di antara sinyal-sinyal yang berbeda? Jelaskan dua metode apa pun.
7. Mengapa metode TDM dan FDM digunakan untuk digunakan dalam sistem telepon, namun tidak untuk jaringan komputasi?
8. Mengapa kita biasanya menggunakan gelombang sinusoidal sebagai gelombang pembawa untuk mengirimkan informasi?
9. Bagaimana output yang dihasilkan komputer dapat dikirimkan melalui jaringan komputer yang dihubungkan melalui saluran telepon?
10. Apa itu modulasi? Bagaimana modulasi membantu mengurangi ukuran antena untuk transmisi?

# BAB 7
# LAPISAN DATA LINK

**Pendahuluan**

Lapisan data link adalah lapisan kedua setelah lapisan fisik dalam model referensi OSI. Ini menjelaskan teknik untuk mengakses saluran komunikasi bersama dan transmisi bingkai data yang andal dalam lingkungan komunikasi komputer. Ia menerima aliran bit mentah untuk lapisan fisik di mesin pengirim. Aliran data mentah dibuat menggunakan teknologi berbeda seperti kabel, DSL, nirkabel, serat optik, dll. Lapisan tautan data mengubah data bebas dari kesalahan transmisi yang tidak terdeteksi ke lapisan jaringan. Lapisan data link menyelesaikan tugas ini dengan menggunakan bingkai pengakuan dan algoritma deteksi kesalahan. Dengan kata lain, tugas lapisan data link adalah mengirimkan bit ke mesin tujuan. Lapisan data link dari mesin tujuan kemudian menyerahkan data yang diterima ke lapisan jaringan untuk diproses. Komunikasi antara dua host yang terhubung secara fisik melalui suatu saluran dapat ditunjukkan pada Gambar 7.1.




**Gambar 7.1 Channel Komunikasi antara 2 Host**

Secara singkat, lapisan data-link menyediakan transfer datagram melalui saluran komunikasi antara dua mesin yang berdekatan. Tugas utamanya, yang akan dijelaskan dalam unit ini, adalah pembingkaian, checksum, deteksi dan koreksi kesalahan, pengakuan, kontrol aliran, antarmuka layanan andal yang terdefinisi dengan baik ke lapisan jaringan, merangkum paket dari lapisan jaringan ke bingkai, dan lain-lain. banyak jenis teknologi tingkat tautan yang dapat digunakan untuk menghubungkan dua node atau mesin. Contoh protokol lapisan tautan adalah Ethernet, token ring, FDDI, dan PPP.

## 7.1 MASALAH DESAIN LAPISAN DATA LINK

**Layanan yang Disediakan pada Lapisan Jaringan**

Lapisan data link menyediakan antarmuka yang terdefinisi dengan baik ke lapisan jaringan, menangani kesalahan transmisi, mengatur aliran data dan menjaga keselarasan pengirim dan penerima dengan menawarkan fungsionalitas berikut:

Untuk menyediakan antarmuka layanan yang terdefinisi dengan baik dan andal ke lapisan 3 atau lapisan jaringan yang juga akan bergantung pada efisiensi dan tingkat kesalahan lapisan fisik yang mendasarinya. Lapisan data link menyelesaikan aktivitas ini dengan cara berikut:

(a) Layanan connectionless yang tidak diakui: Ini melibatkan frame independen dari host sumber ke host tujuan tanpa mekanisme pengakuan apa pun. Itu tidak termasuk pengaturan atau pelepasan koneksi apa pun. Itu tidak menangani pemulihan bingkai karena gangguan saluran.

(b) Layanan tanpa koneksi yang diakui: Saluran komunikasi lebih rawan kesalahan. Hal ini memerlukan layanan pengakuan untuk setiap frame yang dikirim antara dua host untuk memastikan bahwa frame telah tiba dengan benar. Namun, lapisan transport juga mengirimkan pesan pengakuan.

(c) Layanan berorientasi koneksi yang diakui: Lapisan data link menyediakan layanan ini ke lapisan jaringan dengan membuat koneksi antara host sumber dan tujuan sebelum transfer data terjadi. Urutan setiap frame dijaga dan dijamin penerimaan frame oleh host penerima. Komunikasi antara host sumber dan tujuan selesai dalam tiga fase. Yaitu pengaturan koneksi, transmisi frame aktual, dan pelepasan koneksi.

**Pembingkaian**

Lapisan data link menerima aliran bit mentah dari lapisan fisik yang mungkin tidak bebas kesalahan. Untuk menyediakan transfer aliran bit yang andal ke lapisan jaringan, lapisan data link memecah aliran bit menjadi beberapa bingkai. Kemudian menghitung checksum untuk setiap frame, yang ditransmisikan bersama frame tersebut. Host tujuan menerima sebuah frame dan menghitung checksum lain dari datanya untuk dibandingkan dengan frame yang dikirimkan. Hal ini memastikan lapisan data link penerima mendeteksi dan mengoreksi frame. Namun, beberapa metode checksum tidak memberikan koreksi.

**Pengendalian Kesalahan**

Ini juga melibatkan pengurutan frame dan pengiriman frame kontrol untuk pengakuan. Saluran yang berisik dapat menyebabkan bit terbalik, kehilangan bit dari bingkai, memasukkan bit baru ke dalam bingkai, hilangnya bingkai sepenuhnya, dll selama komunikasi. Untuk komunikasi yang andal, host tujuan mengirimkan pengakuan positif atau negatif ke host sumber dalam batas waktu yang ditentukan. Host sumber memiliki batas waktu untuk mengirim ulang frame jika tidak menerima pengakuan dalam jangka waktu tertentu dari host tujuan. Selain itu, setiap frame keluar diberi nomor urut untuk mencegah lapisan data link host tujuan meneruskan frame yang sama lebih dari satu kali ke lapisan jaringan. Keseluruhan urusan ini merupakan bagian integral dari desain lapisan data link.

**Kontrol Aliran**

Masalah penting lainnya dalam desain data link adalah mengendalikan laju transmisi data antara dua host sumber dan tujuan. Jika ada ketidaksesuaian antara kecepatan pengiriman dan penerimaan data host sumber dan host tujuan, hal itu akan menyebabkan hilangnya paket di ujung penerima. Hal ini lebih lanjut menyebabkan pengirim kehabisan waktu pada paket pengakuan, menyebabkan transmisi ulang. Sehingga membuat jaringan menjadi kurang efisien.

## 7.2 DETEKSI DAN KOREKSI KESALAHAN

Ini adalah kumpulan metode yang melibatkan pengkodean untuk mendeteksi kesalahan dalam data yang dikirimkan atau disimpan dan memperbaikinya. Kita pasti telah mempelajari sebelumnya beberapa bentuk deteksi kesalahan yang paling sederhana di mana kita menambahkan bit paritas atau melakukan pemeriksaan redundansi siklik. Jika menggunakan beberapa bit paritas, kita tidak hanya dapat mendeteksi kesalahannya, tetapi juga bit mana yang telah dibalik, dan oleh karena itu harus dibalik kembali untuk mengembalikan data asli. Semakin banyak bit tambahan yang ditambahkan, semakin besar kemungkinan beberapa kesalahan dapat dideteksi dan diperbaiki. Ada beberapa metode berbeda tergantung pada koreksi kesalahan tunggal, deteksi kesalahan ganda (SECDEC).

**Kode Deteksi Kesalahan**

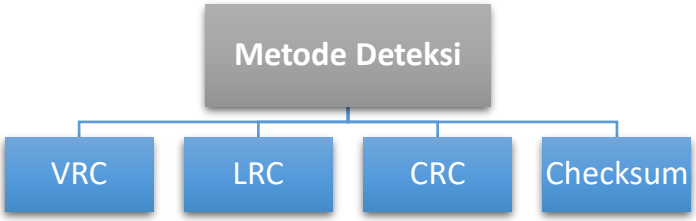
**Redundansi**

Salah satu mekanisme deteksi kesalahan yang akan memenuhi persyaratan ini adalah dengan mengirimkan setiap unit data dua kali. Perangkat penerima kemudian dapat melakukan perbandingan sedikit demi sedikit antara kedua versi data tersebut. Perbedaan apa pun akan menunjukkan adanya kesalahan, dan mekanisme koreksi yang tepat dapat diterapkan. Sistem ini akan benar-benar akurat (kemungkinan terjadinya kesalahan pada bit yang sama persis di kedua kumpulan data sangatlah kecil), namun sistem ini juga akan sangat lambat. Tidak hanya waktu transmisi yang akan berlipat ganda, tetapi waktu yang diperlukan untuk membandingkan setiap unit sedikit demi sedikit harus ditambah.

Konsep memasukkan informasi tambahan dalam transmisi semata-mata untuk tujuan perbandingan adalah ide yang bagus. Namun alih-alih mengulangi seluruh aliran data, kelompok bit yang lebih pendek dapat ditambahkan ke akhir setiap unit. Teknik ini disebut redundansi karena bit tambahan tersebut bersifat mubazir terhadap informasi: bit tersebut dibuang segera setelah keakuratan transmisi ditentukan.

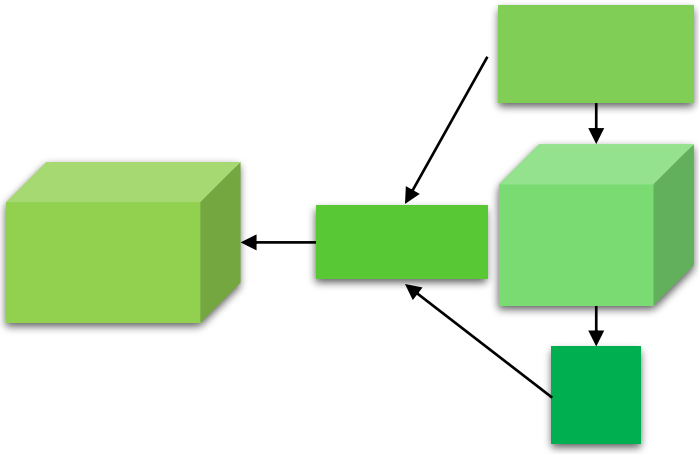
Gambar menunjukkan proses penggunaan bit-bit berlebihan untuk memeriksa keakuratan unit data. Setelah aliran data dihasilkan, aliran data melewati perangkat yang menganalisisnya dan menambahkan pemeriksaan redundansi yang diberi kode yang sesuai: Unit data, yang sekarang diperbesar beberapa bit, bergerak melalui tautan ke penerima. Penerima menempatkan seluruh aliran melalui fungsi pemeriksaan. Jika aliran bit yang diterima melewati kriteria pemeriksaan, bagian data dari unit data diterima dan bit yang berlebihan dibuang.

Empat jenis pemeriksaan redundansi yang digunakan dalam komunikasi data: pemeriksaan redundansi vertikal (VRC) (juga disebut pemeriksaan paritas), pemeriksaan redundansi longitudinal (LRC), pemeriksaan redundansi siklik (CRC), dan checksum. Tiga yang pertama, VRC, LRC dan CRC biasanya diimplementasikan pada lapisan fisik untuk digunakan pada lapisan data link. Yang keempat, checksum, digunakan terutama oleh lapisan atas.




**Gambar 7.2 4 tipe cek redundansi**

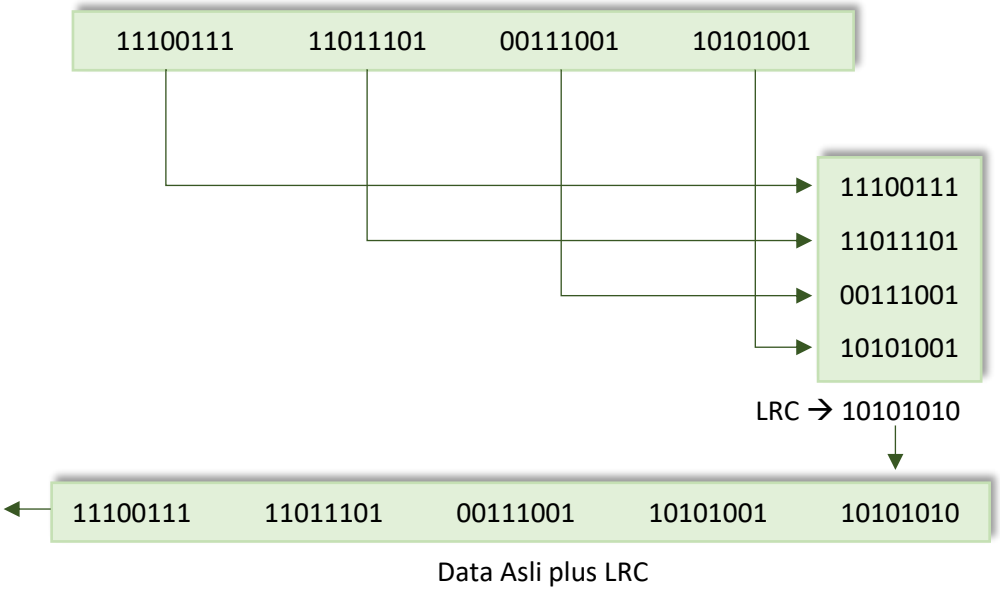
(a) Pemeriksaan Redundansi Vertikal: Mekanisme yang paling umum dan paling murah untuk mendeteksi kesalahan adalah pemeriksaan redundansi vertikal (VCR), sering disebut pemeriksaan paritas. Dalam teknik ini, bit redundan, yang disebut bit paritas, ditambahkan ke setiap unit data sehingga jumlah total bit dalam unit tersebut (termasuk bit paritas) menjadi genap.



**Gambar 7.3 konsep Even Parity VRC**

Misalkan kita ingin mengirimkan unit data biner 1100001. Menjumlahkan angka 1 menghasilkan 3, angka ganjil. Sebelum transmisi, kami melewatkan unit data melalui generator paritas. Generator paritas menghitung bit pertama dan menambahkan bit paritas (dalam kasus ini 1) di akhir. Jumlahnya sekarang menjadi empat, bilangan genap. Bagian tersebut sekarang mentransmisikan seluruh unit yang dikeluarkan melalui tautan jaringan. Ketika mencapai tujuannya, penerima memasukkan kedelapan bit tersebut melalui fungsi pengecekan paritas genap. Jika penerima melihat 11100001, ia dihitung sebagai angka 1, bilangan genap, dan unit data lolos. Namun bagaimana jika unit data rusak dalam perjalanan? Bagaimana jika, bukannya 11100001, penerima melihat 11100101? Penerima mengetahui

bahwa kesalahan telah terjadi pada data di suatu tempat dan karena itu menolak seluruh unit. Perhatikan bahwa demi kesederhanaan, di sini kita membahas pemeriksaan paritas genap, di mana angka 1 haruslah bilangan genap. Beberapa sistem mungkin menggunakan pemeriksaan paritas ganjil, yang mana angka 1 harus ganjil. Prinsipnya sama; perhitungannya berbeda.




**Gambar 7.4 data asli plus LRC**

(b) Pemeriksaan Redundansi Longitudinal: Dalam pemeriksaan redundansi longitudinal (LRC), blok bit disusun dalam sebuah tabel (baris dan kolom). Misalnya, alih-alih mengirimkan blok 32 bit, kami mengaturnya dalam tabel yang terdiri dari empat baris dan delapan kolom, seperti yang ditunjukkan pada gambar. Kami kemudian menghitung bit paritas untuk setiap kolom dan membuat baris baru yang terdiri dari delapan bit, yang merupakan bit paritas untuk keseluruhan blok.

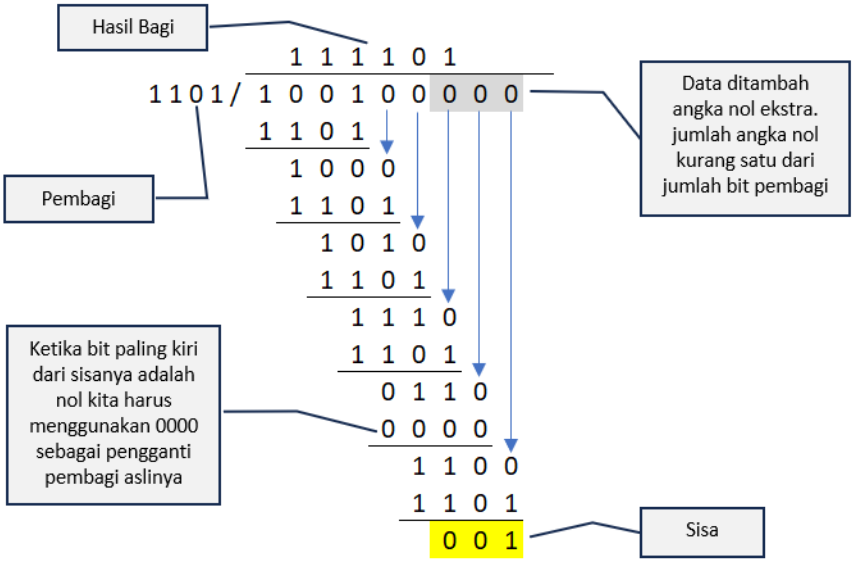
(c) Pemeriksaan Redundansi Siklik: Teknik pemeriksaan redundansi ketiga dan paling kuat adalah pemeriksaan redundansi siklik (CRC). Tidak seperti VRC dan LRC, alih-alih menambahkan bit bersama-sama untuk mencapai paritas yang diinginkan, serangkaian bit redundan, yang disebut sisa CRC dan CRC, ditambahkan ke akhir unit data sehingga unit data yang dihasilkan menjadi habis dibagi satu detik. , bilangan biner yang telah ditentukan. Pada tujuannya, unit data yang masuk dibagi dengan angka yang sama. Jika pada langkah ini tidak ada sisa, maka unit data dianggap utuh dan diterima. Sisanya menunjukkan bahwa unit data telah rusak dalam perjalanan dan oleh karena itu harus ditolak.

Bit redundansi yang digunakan CRC diperoleh dengan membagi unit data dengan pembagi yang telah ditentukan, sisanya adalah CRC. Agar valid, CRC harus mempunyai dua kualitas: ia harus memiliki tepat satu bit lebih kecil dari pembaginya, dan menambahkannya ke akhir string data harus membuat urutan bit yang dihasilkan habis dibagi oleh pembagi. Baik teori maupun penerapan deteksi kesalahan CRC sangatlah mudah. Satu-satunya kerumitan adalah

mendapatkan CRC. Untuk memperjelas proses ini, kita akan mulai dengan gambaran umum dan menambahkan kompleksitas seiring berjalannya waktu. Gambar 7.5 memberikan garis besar tiga langkah dasar.

- ✓ Pertama, serangkaian angka ditambahkan ke unit data. Angka n kurang satu dari jumlah bit pada pembagi yang telah ditentukan, yaitu n + 1 bit.
- ✓ Kedua, unit data yang baru memanjang dibagi dengan pembagi menggunakan proses yang disebut pembagian biner. Sisa hasil pembagian ini adalah CRC.
- ✓ Ketiga, CRC dari n bit yang diperoleh pada langkah 2 menggantikan angka 0 yang ditambahkan pada akhir unit data. Perhatikan bahwa CRC dapat terdiri dari semua angka 0.

Unit data tiba di penerima data terlebih dahulu, baru kemudian CRC. Penerima memperlakukan seluruh string sebagai satu unit dan membaginya dengan pembagi yang sama yang digunakan untuk mencari sisa CRC. Jika string tiba tanpa kesalahan, pemeriksa CRC menghasilkan sisa nol dan unit data lolos. Jika string telah diubah dalam perjalanan, pembagian menghasilkan sisa bukan nol dan unit data tidak lolos.




**Gambar 7.5 Pembagian Bit**

**Pembangkit CRC**

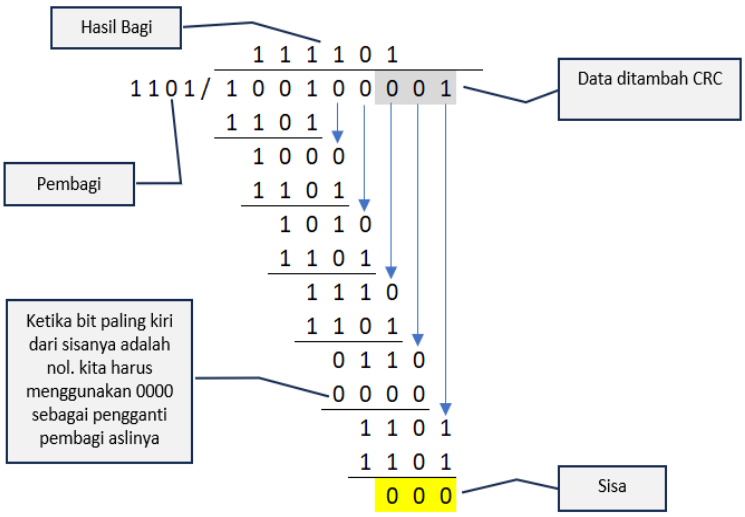
Generator CRC menggunakan divisi modulo-2, Gambar menunjukkan prosesnya. Pada langkah pertama, empat bit pembagi dikurangkan dari empat bit pertama pembagi. Setiap bit pembagi dikurangi dari bit pembagi yang sesuai tanpa mengganggu bit berikutnya yang lebih tinggi. Dalam contoh kita, pembagi, 1101, dikurangkan dari empat bit pertama dari pembagian, 1101. Menghasilkan 1001. Menghasilkan 100 (angka 0 di depan dari sisanya dihilangkan).

Bit berikutnya yang tidak terpakai dari pembagi kemudian ditarik ke bawah untuk membuat jumlah bit sisanya sama dengan jumlah bit dalam pembagi. Oleh karena itu, langkah selanjutnya adalah 1000-1101, yang menghasilkan 101, dan seterusnya. Dalam proses ini,

pembagi selalu diawali dengan 1; pembagi tersebut dikurangkan dari sebagian pembagian/sisa sebelumnya yang sama panjangnya; pembagi hanya dapat dikurangkan dari string 0, yang panjangnya sama dengan pembagi, menggantikan pembagi pada langkah proses tersebut. Untuk string 0, yang panjangnya sama dengan pembagi, menggantikan pembagi pada langkah proses tersebut. Misalnya, jika pembagi panjangnya empat bit, maka diganti dengan empat angka 0. (Ingat, kita berurusan dengan pola bit, bukan nilai kuantitatif; 0000 tidak sama dengan 0). Pembatasan ini berarti bahwa, pada setiap langkah, pengurangan paling kiri akan menjadi 0 – 0 atau 1 – 1, yang keduanya sama dengan 0. Jadi, setelah pengurangan, bit paling kiri dari sisanya. Perhatikan bahwa hanya bit pertama dari sisanya yang dihilangkan – jika bit kedua juga 0. Bit tersebut dipertahankan, dan dividen/sisa untuk langkah berikutnya akan dimulai dengan 0. Proses ini mengulangi satuan dari seluruh dividen yang telah digunakan.

**Pemeriksa CRC**

Pemeriksa CRC berfungsi persis seperti generator. Setelah menerima data yang ditambahkan dengan CRC, ia melakukan modulo yang sama – 2 divisi. Jika sisanya adalah 0, CRC dihilangkan dan data diterima; jika tidak, aliran bit yang diterima akan dibuang dan data dikirim ulang. Gambar menunjukkan proses pembagian yang sama pada penerima. Kami berasumsi tidak ada kesalahan. Oleh karena itu, sisanya semuanya 0 dan data diterima.




**Gambar 7.6 pemeriksaan CRC**

**Kode Koreksi Kesalahan**

Kode koreksi kesalahan (ecc) atau kode koreksi kesalahan penerusan (fec) adalah sistem penambahan data redundan, atau data paritas, ke sebuah pesan, sehingga dapat dipulihkan oleh penerima bahkan ketika sejumlah kesalahan (hingga kemampuan kode yang digunakan) diperkenalkan, baik selama proses transmisi, atau pada penyimpanan. Karena penerima tidak perlu meminta pengirim untuk mengirimkan ulang datanya, saluran belakang tidak diperlukan dalam koreksi kesalahan maju, dan oleh karena itu cocok untuk komunikasi sederhana seperti penyiaran. Kode koreksi kesalahan sering digunakan dalam komunikasi

lapisan bawah, serta untuk penyimpanan yang andal di media seperti CD, DVD, hard disk, dan ram.

Kode koreksi kesalahan biasanya dibedakan antara kode konvolusi dan kode blok:

- Kode konvolusi diproses sedikit demi sedikit. Mereka sangat cocok untuk implementasi di perangkat keras, dan decoder viterbi memungkinkan decoding yang optimal.
- Kode blok diproses berdasarkan blok demi blok. Contoh awal kode blok adalah kode pengulangan, kode hamming, dan kode pemeriksaan paritas multidimensi. Kode-kode tersebut diikuti oleh sejumlah kode yang efisien, kode reed-solomon menjadi yang paling terkenal karena penggunaannya yang luas saat ini. Kode turbo dan kode pemeriksaan paritas kepadatan rendah (ldpc) merupakan konstruksi yang relatif baru yang dapat memberikan efisiensi yang hampir optimal.

Teorema Shannon adalah teorema penting dalam koreksi kesalahan maju, dan menjelaskan kecepatan informasi maksimum yang memungkinkan komunikasi yang andal melalui saluran yang memiliki probabilitas kesalahan atau rasio signal-to-noise (snr) tertentu. Batas atas yang ketat ini dinyatakan dalam kapasitas saluran. Lebih khusus lagi, teorema mengatakan bahwa terdapat kode-kode sedemikian rupa sehingga dengan bertambahnya panjang pengkodean, kemungkinan kesalahan pada saluran memori diskrit yang lebih sedikit dapat dibuat kecil, asalkan kecepatan kode lebih kecil dari kapasitas saluran. Kecepatan kode didefinisikan sebagai pecahan k/n dari k simbol sumber dan n simbol yang dikodekan. Kecepatan kode maksimum sebenarnya yang diperbolehkan bergantung pada kode koreksi kesalahan yang digunakan, dan mungkin lebih rendah. Hal ini karena pembuktian Shannon hanya bersifat eksistensial, dan tidak menunjukkan cara membuat kode yang optimal dan memiliki algoritma pengkodean dan penguraian kode yang efisien.

**Ringkasan**

- Lapisan data link menjelaskan teknik untuk mengakses saluran komunikasi bersama dan transmisi data yang andal. Tugas utamanya adalah pembingkaian, checksum, deteksi dan koreksi kesalahan, pengakuan, kontrol aliran, merangkum paket dari lapisan jaringan ke bingkai, dll.
- Lapisan data link menyediakan layanan tanpa koneksi yang tidak diakui, layanan tanpa koneksi yang diakui, dan layanan berorientasi koneksi yang diakui.
- Pemeriksaan paritas adalah metode deteksi kesalahan yang paling sederhana karena penerima hanya perlu menghitung angka 1 dalam aliran data yang diterima dengan bit paritas tambahan.
- Checksum adalah jenis pemeriksaan redundansi sederhana yang digunakan untuk mendeteksi kesalahan dalam data.
- Cyclic Redundancy Check digunakan secara luas dalam jaringan komputer, merupakan teknik pemberian string data yang ditambahkan ke paket informasi yang dapat digunakan untuk mendeteksi kesalahan pada paket data.

- Protokol Stop dan Wait paling mudah diterapkan dan terbukti paling efisien pada saluran komunikasi bebas kesalahan. Namun, saluran komunikasi bebas kesalahan praktis tidak mungkin dilakukan.

**Latihan Soal**

1. Apa yang dimaksud dengan protokol tautan data?
2. Keuntungan apa yang ditawarkan oleh protokol jendela geser Selective Repeat dibandingkan protokol Go Back N?
3. Apa tujuan pengendalian aliran?
4. Jelaskan bagaimana model mesin negara terbatas melakukan verifikasi protokol?
5. Apa sajakah protokol data link yang tersedia? Mengapa PPP menjadi populer?

# BAB 8
# PROTOKOL DATA LINK

**Pendahuluan**

Lapisan data link adalah lapisan 2 dari model osi tujuh lapisan jaringan komputer. Ini sesuai dengan, atau merupakan bagian dari lapisan tautan model referensi tcp/ip. Lapisan data link adalah lapisan protokol yang mentransfer data antara node jaringan yang berdekatan dalam jaringan area luas atau antar node pada segmen jaringan area lokal yang sama. Lapisan data link menyediakan sarana fungsional dan prosedural untuk mentransfer data antar entitas jaringan dan mungkin menyediakan sarana untuk mendeteksi dan kemungkinan memperbaiki kesalahan yang mungkin terjadi pada lapisan fisik. Contoh protokol data link adalah Ethernet untuk jaringan area lokal (multi-node), Point-to-Point Protocol (PPP), HDLC dan ADCCP untuk koneksi point-to-point (dual-node).

## 8.1 PROTOKOL TAUTAN DATA DASAR

Tujuan dasar komunikasi komputer dalam lingkungan jaringan adalah untuk mengirimkan pesan yang panjangnya tak terhingga dari node sumber ke node tujuan. Untuk menjelaskan bagaimana lapisan data link menyelesaikan komunikasi data ke host tujuan pada lapisan data link, di sini diasumsikan bahwa lapisan 3 atau lapisan jaringan memiliki pesan panjang untuk dikirim ke host tujuan. Pesan yang tersedia di lapisan jaringan dipecah menjadi paket-paket untuk diteruskan ke lapisan data link. Lapisan data link merangkum setiap paket dalam sebuah frame dengan menambahkan header dan trailer. Lapisan data link tidak mengganggu isi paket.

**Simplex Berhenti dan Tunggu**

Saluran komunikasi bebas kesalahan diasumsikan. Node sumber mengambil paket dari lapisan jaringan dan merangkumnya ke dalam bingkai untuk dikirim. Setelah transmisi, node sumber menunggu pengakuan dari node tujuan. Setelah menerima pengakuan, perulangan dimulai lagi. Di node tujuan, mesin menunggu frame dari sumber tujuan. Setelah menerima frame, ia meneruskan frame tersebut ke lapisan jaringan dan mengirimkan pengakuan untuk frame tersebut ke node sumber. Kemudian loop kembali menunggu frame berikutnya dan proses berlanjut hingga frame Akhir File tercapai.

Protokol stop dan wait hanya melibatkan satu frame yang beredar pada satu waktu sehingga tidak diperlukan nomor urut. Pengakuan yang dikirim kembali oleh node tujuan ke mesin sumber adalah bingkai kosong. Protokol Stop dan Wait mudah diterapkan dan tidak menimbulkan kemacetan karena hanya ada satu frame yang beredar pada suatu waktu. Hilangnya frame juga tidak mungkin terjadi karena kemacetan. Host tujuan juga tidak akan kebanjiran pengirim. Kerugian dari metode ini adalah tidak adanya saluran komunikasi yang bebas kesalahan. Oleh karena itu, frame atau mat pengakuan dapat dengan mudah hilang atau rusak dan situasi deadlock dapat terjadi dimana node sumber dan tujuan tidak dapat bergerak maju.

**Pengakuan Positif dengan Protokol Transmisi Ulang (PAR)**

Ini merupakan peningkatan pada protokol Stop dan Wait. Mesin sumber mengambil paket dari lapisan jaringan, merangkumnya ke dalam bingkai dengan nomor urut untuk dikirim ke node tujuan. Setelah transmisi, mesin sumber mencoba mengambil pengakuan dari lapisan fisik. Setelah pengakuan tiba dengan nomor urut yang benar, paket berikutnya yang dikirim dari lapisan jaringan diambil dan karenanya, nomor urut untuk mengirim paket berikutnya diperbarui. Dengan cara ini, perulangan dimulai dari awal. Jika tidak ada frame yang diambil dari fisik dalam waktu yang ditentukan, lapisan fisik akan habis waktunya atau pengakuan dengan nomor urut yang salah akan diterima. Dalam hal ini, frame terakhir yang dikirim ditransmisikan ulang dan dengan demikian perulangan dimulai kembali.

Di node tujuan, mesin penerima menunggu penerimaan frame dari lapisan fisik. Setelah frame diterima, nomor urutnya diperiksa. Jika ditemukan benar, paket diteruskan ke lapisan berikutnya yaitu lapisan jaringan. Mesin tujuan mengirimkan pengakuan untuk frame tersebut ke mesin sumber untuk nomor urut yang baru saja diterima. Jika frame yang salah atau keluar dari urutan tiba, mesin tujuan meminta transmisi ulang ke node sumber.

PAR hanya melibatkan satu frame yang beredar pada suatu waktu, nomor urut harus digunakan untuk menentukan apakah ada frame yang hilang atau rusak. Skema ini hanya membutuhkan dua nomor urut karena pada suatu waktu hanya akan ada satu frame yang beredar dan nomor urut tidak akan berubah sampai pengakuan positif diterima. Protokol ini hanya menggunakan '1' dan '0' sebagai nomor urut. Protokol PAR mudah diimplementasikan. Nomor urut dan transmisi pengakuan untuk frame yang diterima secara berurutan menjaga host sumber dan tujuan tetap sinkron.

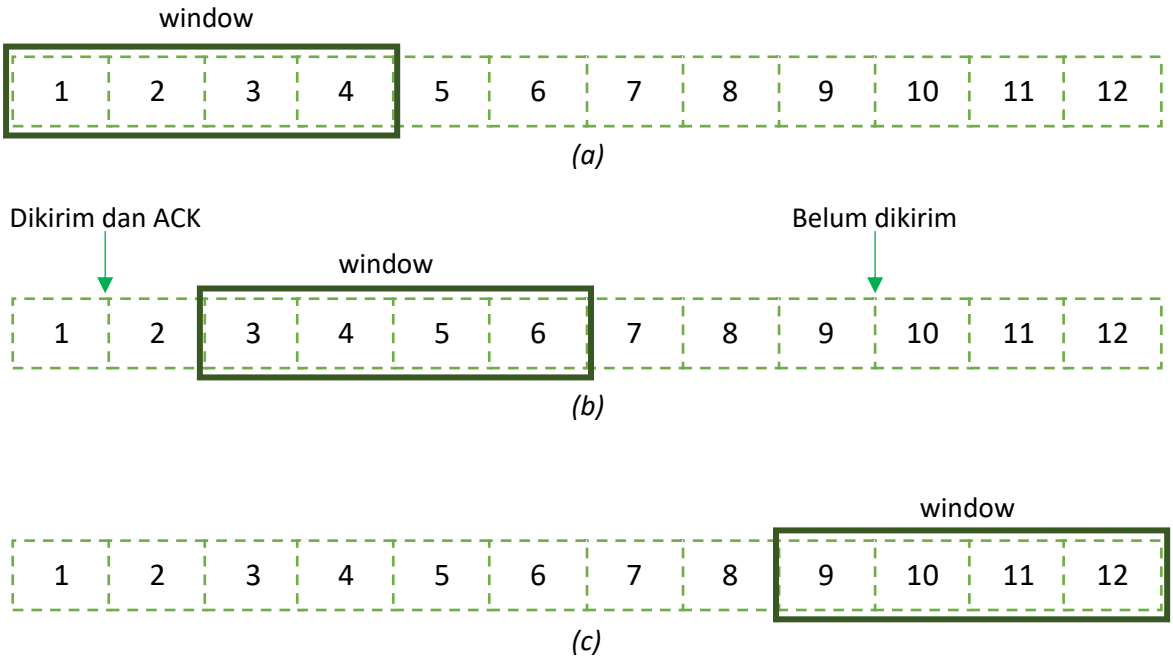
Protokol ini mampu menangani kemacetan, frame hilang dan frame rusak karena frame ditransmisikan ulang hingga pengakuan positif diterima. Namun, karakteristik ini membuat protokol PAR tidak efisien karena jumlah frame yang dikirim untuk mentransfer seluruh pesan secara andal menjadi frame yang besar karena hilangnya pengakuan.

## 8.2 PROTOKOL JENDELA GESER

Dalam sistem komunikasi data, ini dapat didefinisikan sebagai pengendalian kecepatan pengiriman data dari suatu terminal sehingga data tersebut dapat diterima oleh terminal lain. Dengan mempertahankan kecepatan transfer data yang kompatibel antara pihak pengirim dan penerima, hal ini dapat mencegah kemacetan jaringan. Komputer berkecepatan tinggi, misalnya, dapat menghasilkan lalu lintas lebih cepat daripada kemampuan jaringan untuk mentransfernya atau lebih cepat daripada kemampuan perangkat tujuan menerima dan memprosesnya. Untuk memastikan transmisi yang efektif, perangkat sumber memerlukan pengakuan dari tujuan setelah sejumlah paket telah dikirim. Ini adalah skema kontrol aliran Windowing. Jika tujuan tidak menerima satu atau lebih paket karena alasan tertentu, seperti buffer yang meluap, maka tujuan tersebut tidak menerima paket yang cukup untuk mengirim pengakuan. Sumber kemudian mentransmisikan ulang paket-paket tersebut dengan kecepatan transmisi yang lebih rendah.

Seperti yang telah kita lihat dalam topik sebelumnya bahwa kontrol aliran adalah suatu teknik yang tujuan utamanya adalah untuk mencocokkan kecepatan transmisi pengirim dengan penerima dan jaringan. Namun, hal ini tidak sama dengan pengendalian kemacetan. Pengendalian kemacetan terutama berkaitan dengan kelebihan beban yang berkelanjutan pada perangkat perantara jaringan seperti router IP. Untuk menjaga aliran data yang tepat, bidang jendela dibuat untuk menyesuaikan laju aliran aliran byte antara perangkat yang berkomunikasi. Gambar 8.1 mengilustrasikan konsep jendela geser.

Dalam contoh sederhana ini, ada jendela geser 4-byte. Bergerak dari kiri ke kanan, jendela "bergeser" saat byte dalam aliran dikirim dan diakui. Ukuran jendela dan seberapa cepat menambah atau mengurangi ukuran jendela merupakan bidang penelitian yang hebat.




**Gambar 8.1 window Geser**

**Jendela Geser: Kembali N**

Protokol Go Back N memungkinkan mesin sumber memiliki lebih dari satu frame luar biasa pada satu waktu dengan menggunakan buffer. Dengan demikian mengatasi masalah PAR. Mesin sumber menyimpan buffer dengan ukuran yang telah ditentukan yang menerima paket, menyimpannya di slot kosong yang benar di buffer, membuat bingkai dengan nomor urut yang benar dan mengirimkannya. Pengatur waktu logis yang sesuai diatur ulang ke 0 dan batas atas jendela digeser ke atas dengan menambah secara melingkar untuk mengirimkan frame berikutnya.

Jika tidak ada buffer yang kosong, lapisan fisik diperiksa untuk mengetahui apakah ada pengakuan. Jika frame yang baik diterima dengan nomor pengakuan dalam jendela saat ini, jumlah buffer yang digunakan kemudian dikurangi dan pengatur waktu logis direset ke nilai negatif untuk menunjukkan slot yang tidak digunakan. Hal ini memungkinkan untuk menggeser Batas Bawah jendela dengan menambah jumlah pengakuan yang diharapkan

secara melingkar. Prosedur ini membuat perulangan hingga pengakuan yang diharapkan sama dengan pengakuan yang diterima. Ini menghapus pengakuan yang diterima dan frame sebelumnya yang belum diakui sejauh ini.

Selanjutnya, pengatur waktu logis diperbarui jika ada bingkai buruk atau bingkai di luar jendela. Jika suatu frame habis waktunya, frame yang sama ditransmisikan ulang dan pewaktu logis direset ke 0. Oleh karena itu, frame berikutnya akan habis waktunya dan akan dikirim ulang pada iterasi loop berikutnya. Dengan demikian frame yang habis waktunya dan semua frame berikutnya ditransmisikan ulang.

Di mesin tujuan, mesin penerima menunggu hingga frame yang baik tiba. Ia memeriksa nomor urut, jika itu bukan nomor urut yang diharapkan, ia mengirimkan kembali pengakuan untuk nomor urut benar terakhir yang diterima. Jika nomor urut yang diharapkan satu, maka paket akan diteruskan ke lapisan Jaringan. Secara bersamaan, ini memperbarui nomor urut terakhir yang benar yang diterima dan secara melingkar menambah nomor urut berikutnya yang diharapkan. Dengan demikian, pengakuan dibuat dan ditransmisikan. Ini menciptakan loop kembali ke lapisan fisik untuk mengambil frame berikutnya.

**Jendela Geser: Pengulangan Selektif**

Protokol Selective Repeat bermaksud untuk memperbaiki permasalahan pada protokol Go Back N. Hal ini dicapai dengan menyediakan buffer pada host sumber dan tujuan untuk memungkinkan node sumber memiliki lebih dari satu frame yang beredar pada satu waktu dan node tujuan menerima frame yang rusak dan menyimpannya di jendelanya.

Dalam skema Pengulangan Selektif, time-out, iterasi loop, dan transmisi ulang semuanya sama dengan Go Back N kecuali bahwa node sumber mentransmisikan ulang frame terkait yang diidentifikasi dengan tidak adanya pengakuan tetapi tidak semua frame berikutnya. Oleh karena itu, node tujuan yang menyimpan jendela frame, hanya perlu mengirimkan ulang frame yang waktunya habis tetapi tidak seluruh rangkaiannya.

Di sisi penerima, node tujuan menunggu hingga frame tiba. Jika ada frame rusak, frame habis waktu, atau frame tiba di luar urutan, pemberitahuan tidak dikirim untuk nomor urut yang diharapkan. Jika ada slot kosong di buffer mesin tujuan, paket disimpan di slot yang benar dan slot tersebut ditandai sebagai digunakan. Jika semua slot penuh, paket diteruskan ke lapisan jaringan dengan flag disetel untuk mengirimkan pengakuan dan slot buffer direset ke kosong. Hal ini meningkatkan batas atas jendela dan batas bawah untuk bingkai yang diharapkan bertambah secara melingkar. Setelah itu, loop kembali untuk mengetahui slot buffer untuk nomor urut yang diharapkan. Perulangan berlanjut hingga slot yang diharapkan kosong. Dengan demikian, semua paket yang tersedia di buffer diteruskan ke lapisan jaringan secara berurutan.

Dalam hal ini, nomor urut dibuat lebih besar dari ukuran jendela untuk menghindari tumpang tindih di jendela. Hal ini memungkinkan mesin sumber dan tujuan berada dalam sinkronisasi bahkan ketika frame dan pengakuan hilang dengan kecepatan yang sangat tinggi. Dengan demikian, buffering dan pengakuan yang ditingkatkan memungkinkan protokol ini menangani kemacetan, frame rusak, dan frame hilang dengan mudah. Ini juga memerlukan nilai batas waktu yang jauh lebih tinggi dibandingkan dengan Go Back N untuk mengurangi

jumlah frame yang dikirim. Jika nilai batas waktu yang lebih rendah dipertahankan, maka akan memerlukan terlalu banyak frame untuk transmisi ulang yang tidak perlu.

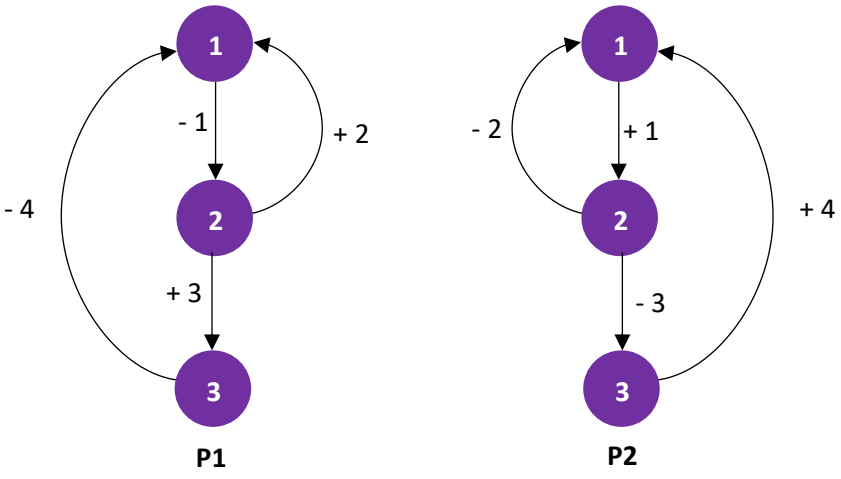
## 8.3 VERIFIKASI PROTOKOL

Protokol adalah seperangkat aturan, yang mengatur pertukaran pesan antara dua node atau proses untuk menyediakan serangkaian layanan tertentu ke lapisan protokol lokal di atasnya dan untuk memberikan serangkaian aturan atau protokol logis ke mesin rekan jarak jauhnya. Protokol diverifikasi selama tahap desain sebelum implementasi sistem atau selama tahap pengujian dan simulasi setelah implementasi sistem. Verifikasi desain dianggap dapat mengurangi biaya pengembangan dan pengujian protokol. Verifikasi desain membagi pekerjaan menjadi dua tugas. Yaitu verifikasi spesifikasi layanan dan verifikasi spesifikasi protokol. Verifikasi spesifikasi protokol berupaya mendeteksi adanya kesalahan logika dalam desain protokol.

Interaksi dan konkurensi adalah dua komponen utama dari setiap sistem lokal atau terdistribusi multi-proses. Interaksi adalah koordinasi atau sinkronisasi antar proses. Konkurensi adalah paralelisme antara proses yang berbeda. Dengan kata lain, konkurensi adalah eksekusi proses dalam sistem multi-proses lokal atau terdistribusi secara simultan dan independen dari proses lain dalam sistem yang sama.

**Model Mesin Keadaan Hingga**

Dalam model Finite State Machine (FSM), setiap proses memiliki mesin keadaan terbatas yang berkomunikasi atau grafik berlabel terarah. Grafik berlabel berarah memiliki simpul dan tepi yang masing-masing mewakili keadaan dan transisi. Transisi pengiriman pesan ditandai dengan "-" (tanda minus) dan transisi penerimaan pesan ditandai dengan "+" (tanda plus). Saluran FIFO dupleks penuh, bebas kesalahan, menghubungkan setiap pasangan proses.




**Gambar 8.2 Protokol yang didesain dengan benar**

Gambar 8.2 menunjukkan protokol yang dirancang dengan benar yang melibatkan dua proses P1 dan P2. Awalnya, kedua proses berada dalam keadaan 1. P1 mengirimkan pesan 1 ke P2 dan memasuki keadaan 2. P2 menerima pesan 1 dan memasuki keadaan 2. Pada saat

ini, P2 mengirimkan pesan 2 dan kembali ke keadaan awal atau mengirimkan pesan 3 dan memasuki keadaan baru 3. Demikian pula, P1 kembali ke keadaan awal atau menuju keadaan baru 3 tergantung pada pesan yang diterima. Ketika kedua proses berada dalam keadaan 3, satu-satunya transisi yang mungkin adalah transmisi dan penerimaan pesan 4 masing-masing oleh P1 dan P2.

**Model Petri Net**

Model Petri net juga menggunakan grafik untuk menunjukkan keadaan dan transisi dan terdiri dari empat bagian:

- **Tempat**: Dilambangkan dengan lingkaran dan mewakili keadaan sistem. Gambar 8.3 memiliki dua tempat A dan B.
- **Transisi**: Dilambangkan dengan garis horizontal atau vertikal.
- **Panah**: Setiap transisi mempunyai nol atau lebih panah masukan yang berasal dari tempat masukannya dan nol atau lebih panah masukan yang menuju ke tempat keluarannya.
- **Token**: Dilambangkan dengan titik tebal dan memberitahukan keadaan sistem saat ini. Gambar 8.3 menunjukkan bahwa sistem berada pada State A.


**Gambar 8.3 Jaring Petri dengan dua Node**

1. Transisi diaktifkan jika setiap tempat masukannya memiliki setidaknya satu token masukan.
2. Setiap transisi yang diaktifkan akan diaktifkan dan token di setiap tempat masukan dihapus untuk disimpan di setiap tempat keluaran.
3. Setelah diaktifkan, jumlah token dapat bervariasi tergantung pada jumlah tempat input dan output.
4. Satu transisi dapat terjadi pada satu waktu; namun pilihan untuk beralih ke kebakaran tidak dapat ditentukan. Jaring Petri pada Gambar 8.3 dapat digunakan untuk memodelkan proses dua fase dan oleh karena itu bersifat deterministik.

Jaring petri digunakan untuk mendeteksi kegagalan protokol serupa dengan penggunaan mesin negara terbatas. Misalnya, jika beberapa rangkaian pengaktifan menyertakan transisi Tn dua kali tanpa intervensi transisi Tn+1, protokolnya akan salah.

## 8.4 CONTOH PROTOKOL TAUTAN DATA

Protokol tautan data mengatur aliran komunikasi antara berbagai komputer. Berbagai macam komputer dan teknologi komunikasi digunakan untuk melaksanakan tugas-tugas yang bermanfaat. Ini termasuk komputer mainframe, jaringan area lokal, workstation, komputer pribadi, dan platform jaringan berbasis kepemilikan dan standar. Semua produk ini tidak dapat

dioperasikan dan tidak mudah untuk bertukar data antar sistem dan aplikasi yang berbeda. Oleh karena itu, standar dikembangkan untuk memastikan keterkaitan berbagai standar yang diadopsi oleh berbagai vendor. Untuk membangun sesi yang bermakna, serangkaian aturan tertentu perlu diadopsi oleh vendor perangkat jaringan. Beberapa contoh protokol data link adalah protokol High Level Data Link Control (HDLC) dan Point-to-Point Protocol (PPP). Pembahasan protokol HDLC dan PPP yang lebih sederhana di sini akan mengeksplorasi banyak fitur terpenting dari protokol data link.

**Kontrol Tautan Data Tingkat Tinggi (HDLC)**

Prosedur HDLC distandarisasi oleh ISO. Ini cocok untuk transmisi data dalam jumlah besar berkecepatan tinggi, sesuatu yang tidak dapat disediakan oleh prosedur kontrol dasar. Prosedur HDLC telah distandarisasi berdasarkan SDLC. Selain karakter, string bit dengan panjang yang diinginkan juga dapat dikirimkan melalui prosedur ini. Unit transmisi data disebut frame. Dengan prosedur kontrol dasar, penerimaan data diperiksa setelah beberapa frame dikirim untuk meningkatkan efisiensi transmisi. Ia juga menawarkan bentuk pengendalian kesalahan tingkat lanjut yang disebut CRC (Cyclic Redundancy Check).

Keuntungan dari prosedur ini adalah peralatan pengirim dapat mengirimkan beberapa blok data sekaligus untuk meningkatkan efisiensi transmisi. Karena peralatan penerima harus menginformasikan kepada peralatan pengirim berapa banyak data yang telah diterima, maka perlu dilampirkan nomor urut pada setiap bagian data. Unit transmisi data disebut frame. Format bingkai HDLC digambarkan pada Gambar 8.4. Setiap frame mempunyai pola bit 01111110, yang disebut flag, di awal dan akhir. Artinya, prosedur HDLC menggunakan sistem flag synchronous.

(1) Urutan bit transmisi (Bingkai Informasi)
(2) Urutan bit Transmisi (Rangka Pengawas)

(1) Urutan bit transmisi (Bingkai Informasi)

| Flag | Alamat | Control | Informasi | FCS | Flag |
|---|---|---|---|---|---|
| **F** | **A** | **C** | **I** | **FCS** | **F** |
| **0111110** | **8 Bit** | **8 Bit** | **N Bit** | **16 Bit** | **0111110** |

(2) Urutan bit transmisi (Bingkai Pengawas)

| Flag | Alamat | Control | FCS | Flag |
|---|---|---|---|---|
| **F** | **A** | **C** | **FCS** | **F** |
| **0111110** | **8 Bit** | **8 Bit** | **16 Bit** | **0111110** |

**Gambar 8.4 format bingkai HDLC**

Selain dua bendera ini, bingkai terdiri dari bidang-bidang berikut:

1. Bidang Alamat: Ini menunjukkan alamat tujuan atau sumber suatu bingkai.
2. Bidang kendali: Ini menunjukkan perintah atau respons yang ditujukan ke peralatan jarak jauh. Nomor urut yang disebutkan sebelumnya juga disertakan.
3. Bidang informasi: Berisi pesan.
4. FCS (Frame Check Sequence): Ini adalah urutan 16 bit untuk pengendalian kesalahan.

Format bingkai yang diberikan pada (2) Gambar 8.4 hanya untuk respons dan tidak menyertakan kolom informasi apa pun. Karena bidang kontrol yang menyimpan informasi kontrol dan bidang informasi yang menyimpan informasi dipisahkan dengan jelas, semua jenis kode dapat dikirim melalui prosedur HDLC. Nomor urut data juga disertakan dalam bidang kontrol, blok data berturut-turut (bingkai) dapat dikirim tanpa memeriksa penerimaan setiap blok data.

## 8.5 PROTOKOL TITIK-KE-TITIK (PPP)

PPP adalah untuk link dialup dari host residensial. Oleh karena itu, ini adalah salah satu protokol data link yang paling banyak digunakan. Protokol Point-to-Point adalah protokol lapisan data link dan beroperasi melalui link point-to-point yang menghubungkan dua rekan tingkat link yang berkomunikasi di setiap ujung link. Link ini dapat berupa saluran telepon dialup serial, SONET/ Tautan SDH, koneksi X.25, sirkuit ISDN, dll.

Point-to-Point Protocol (PPP) digunakan untuk mengirimkan datagram melalui koneksi serial sebagai protokol enkapsulasi untuk mengangkut lalu lintas IP melalui tautan point-to-point. PPP mendukung penugasan dan pengelolaan alamat IP, enkapsulasi sinkron asinkron dan berorientasi bit, multiplexing protokol jaringan, konfigurasi tautan, dll dengan menyediakan Link Control Protocol (LCP) yang dapat diperluas bersama dengan Network Control Protocols (NCPs). Keuntungan dari PPP adalah ia mampu membawa sejumlah besar protokol dan dengan demikian beroperasi melampaui protokol IP, menyediakan deteksi kesalahan pada link itu sendiri, memungkinkan host untuk menegosiasikan pilihan seperti alamat IP, ukuran datagram maksimum pada waktu start-up. , otorisasi host, dll.

**Komponen KPS**

Protokol point-to-point memiliki komponen berikut untuk mentransmisikan datagram melalui link serial point-to-point:

1. **Enkapsulasi Datagram**: PPP menggunakan protokol Kontrol Tautan Data Tingkat Tinggi (HDLC) sebagai mekanisme untuk merangkum datagram melalui tautan titik-ke-titik. Protokol HDLC mendefinisikan batas-batas di sekitar frame PPP individual dan menyediakan checksum 16-bit. Bingkai PPP menambahkan bidang protokol ke bingkai HDLC dasar untuk mengidentifikasi jenis paket yang dibawa oleh bingkai sehingga memungkinkan untuk menampung paket dari protokol selain IP, seperti IPX Novell atau Appletalk.
2. **Menerapkan LCP**: LCP kontrol tautan yang dapat diperluas digunakan untuk menyiapkan, mengonfigurasi, dan menguji koneksi data-link. LCP diimplementasikan di atas HDLC untuk menegosiasikan opsi yang berkaitan dengan data link.
3. **Menerapkan NCP**: Sekelompok protokol kontrol jaringan (NCP) digunakan untuk menyiapkan dan mengonfigurasi protokol lapisan jaringan yang berbeda seperti IP dan AppleTalk, yang dirutekan melalui tautan data. Mereka dikonfigurasi secara dinamis menggunakan NCP yang sesuai. Sebelum mentransmisikan datagram IP melalui link, kedua host yang menjalankan PPP diharuskan untuk menegosiasikan alamat IP yang

digunakan oleh masing-masing host. Protokol kontrol yang digunakan untuk negosiasi tersebut dikenal sebagai protokol kontrol protokol Internet (IPCP).

Untuk berkomunikasi melalui link point-to-point, PPP mengirimkan frame LCP untuk mengkonfigurasi data-link sehingga koneksi melalui link point-to-point dapat diatur. Ketika link sudah diatur, fasilitas opsional juga dinegosiasikan yang penting untuk LCP. Setelah itu, PPP asal mengirimkan frame NCP untuk memilih dan mengkonfigurasi satu atau lebih protokol lapisan jaringan. Hal ini menyebabkan transmisi paket dari setiap protokol lapisan jaringan melalui link. Tautan tetap terkonfigurasi kecuali frame LCP atau NCP meminta untuk menutup tautan. Terkadang beberapa peristiwa eksternal juga menutup tautan tersebut. Secara singkat, komunikasi melalui tautan point-to-point diberikan seperti di bawah ini:

- Frame LCP dari PPP asal terlebih dahulu mengkonfigurasi dan menguji data link untuk membangun koneksi.
- Setelah link terbentuk, PPP asal mengirimkan frame NCP untuk menegosiasikan fasilitas opsional dan mengkonfigurasi satu atau lebih protokol lapisan jaringan sesuai dengan LCP.
- Ketika masing-masing protokol lapisan jaringan yang dipilih telah dikonfigurasi, paket dari setiap protokol lapisan jaringan dapat dikirim melalui link. Tautan akan tetap dikonfigurasi untuk komunikasi hingga frame LCP atau NCP eksplisit menutup tautan, atau hingga terjadi peristiwa eksternal.

**Catatan**

Perhatian PPP mampu beroperasi di semua antarmuka DTE/DCE seperti RS-232-C, RS-422, dll. Namun, PPP memerlukan sirkuit dupleks untuk pengoperasiannya. Mereka mungkin berdedikasi atau dialihkan dalam mode asinkron atau sinkron.

**Kerangka KPS**

Ada enam bidang yang membentuk kerangka KPS. Hal ini diberikan di bawah ini dan juga direpresentasikan secara diagram pada Gambar 8.5.

- **Flag**: Terdiri dari satu byte yang menunjukkan awal atau akhir frame.
- **Alamat**: Alamat terdiri dari satu byte yang berisi urutan biner. PPP tidak menetapkan alamat stasiun individual.
- **Kontrol**: Terdiri dari satu byte yang berisi urutan biner, yang memerlukan transmisi data pengguna. Ini adalah layanan tautan tanpa koneksi yang mirip dengan Logical Link Control (LLC).
- **Protokol**: Terdiri dari dua byte yang mengidentifikasi protokol yang dienkapsulasi dalam bidang informasi frame.
- **Data**: Data dapat berkisar dari nol atau lebih byte yang berisi datagram untuk protokol yang ditentukan dalam bidang protokol. Panjang maksimum default bidang informasi adalah 1.500 byte. Urutan flag penutup menunjukkan akhir bidang informasi dengan 2 byte untuk bidang Frame Check Sequence (FCS).
- **Frame Check Sequence** (FCS): Memiliki 2 byte. Dalam beberapa kasus, ia juga dapat menggunakan FCS 4-byte untuk meningkatkan deteksi kesalahan tetapi dengan persetujuan sebelumnya.

| 1 byte | 1 byte | 1 byte | 2 byte | Variabel | 2 atau 4 byte |
|---|---|---|---|---|---|
| Flag | Address | Control | Protokol | Data | FCS |

**Gambar 8.5 Frame PPP**

**Protokol Kontrol Tautan PPP (PPP LCP)**

Protokol yang membedakan PPP dari HDLC adalah Link Control Protocol (LCP) dan Network Control Protocol (NCP). LCP menetapkan, mengkonfigurasi, memelihara, dan mengakhiri tautan point-to-point. Seperti yang kita ketahui sekarang bahwa PPP LCPLCP menyediakan metode untuk membangun, mengkonfigurasi, memelihara, dan mengakhiri koneksi point-to-point yang menggunakan empat langkah. Ini adalah pembuatan tautan dan negosiasi konfigurasi. Bingkai konfigurasi-pengakuan menyelesaikan langkah ini. Setelah itu kualitas link diuji apakah kualitas link tersebut cukup untuk memunculkan protokol lapisan jaringan. Fase ini bersifat opsional. Setelah menguji kualitas tautan, protokol lapisan jaringan dapat dikonfigurasi secara terpisah oleh NCP yang sesuai dan dapat diaktifkan dan dihapus kapan saja. Jika LCP menutup link, ia menginformasikan protokol lapisan jaringan sehingga mereka dapat mengambil tindakan yang tepat. Terakhir, penghentian tautan terjadi dan LCP dapat mengakhiri tautan tersebut kapan saja. Hal ini biasanya dilakukan atas permintaan pengguna namun dapat terjadi karena peristiwa fisik, seperti hilangnya operator atau berakhirnya pengatur waktu periode menganggur.

Tahukah kamu? Ada tiga kelas frame LCP. Bingkai pembentukan tautan digunakan untuk membuat dan mengonfigurasi tautan. Frame terminasi link digunakan untuk menghentikan link, dan frame pemeliharaan link digunakan untuk mengelola dan men-debug link.

**Protokol Kontrol Jaringan Protokol Point-to-Point** (PPP NCP)

Fase Network Control Protocol (NCP) dalam proses koneksi tautan PPP digunakan untuk membangun dan mengkonfigurasi protokol lapisan jaringan yang berbeda seperti IP, IPX atau AppleTalk. Setelah NCP tercapai, PPP akan membawa paket protokol lapisan jaringan yang sesuai. Selama fase ini, lalu lintas link terdiri dari kemungkinan kombinasi paket protokol LCP, NCP, dan lapisan jaringan. Protokol NCP khusus IP adalah IP Control Protocol (IPCP). Selain menangani alamat IP rekan pemanggil, protokol ini juga dapat menegosiasikan apakah akan menggunakan kompresi header atau tidak, sehingga memberikan peningkatan kecepatan yang signifikan untuk tautan berkecepatan rendah. Jika rekan yang menelepon memiliki alamat IP, ia akan memberitahukan alamat tersebut kepada rekan yang dipanggil; jika rekan pemanggil tidak memiliki alamat IP, rekan yang dipanggil dapat menetapkan alamat pemanggil dari kumpulan alamat.

## 8.6 PROTOKOL AKSES BERGANDA

Jaringan tradisional adalah saluran point-to-point berdasarkan saluran khusus untuk sepasang pengguna. Saluran-saluran ini, karena kesederhanaannya, tidak hanya ekonomis tetapi juga digunakan untuk menyediakan transmisi antara sepasang node, tidak berpengaruh

pada transmisi antara pasangan node lainnya meskipun mereka memiliki node yang sama. Kerugian dari saluran tersebut adalah bahwa saluran tersebut biasanya memerlukan topologi tetap dan sejumlah besar koneksi khusus antara sepasang saluran sehingga menimbulkan tantangan dalam merancang pemeliharaan dan efektivitas biaya. Sebaliknya, saluran siaran mulai digunakan di mana lebih dari satu penerima dapat menerima setiap pesan yang dikirimkan. Saluran siaran dikatakan baik jika suatu pesan ditujukan ke sejumlah tujuan yang lebih banyak dibandingkan satu atau sejumlah tujuan yang sangat sedikit karena hal ini menimbulkan hasil pemrosesan yang sia-sia di semua saklar yang tidak dimaksudkan dengan pesan tersebut.

Transmisi melalui suatu saluran siaran juga rawan mengganggu transmisi lainnya. Dengan demikian, transmisi antar sepasang node tidak lagi independen terhadap transmisi lainnya. Untuk menghindari gangguan tersebut, diperlukan mekanisme kendali transmisi. Mekanisme kontrol transmisi yang dikenal sebagai protokol akses ganda menentukan akses ke saluran bersama di mana alokasi sumber daya bersama sangat penting untuk karakteristik kinerja yang diinginkan dan pengoperasian jaringan yang tepat. Protokol akses ganda ini adalah skema alokasi saluran dan sebagian besar berada di lapisan khusus yang disebut lapisan Medium Access Control (MAC) di dalam lapisan data link model OSI.

**Klasifikasi Protokol Akses Berganda**

Ada banyak protokol akses ganda. Salah satunya adalah protokol akses ganda yang tidak terpusat di mana semua host bekerja berdasarkan aturan yang sama dan tidak ada satu host pun yang diizinkan untuk mengoordinasikan aktivitas host lainnya. Ini juga tidak termasuk protokol akses jenis polling. Secara umum, protokol-protokol tersebut diklasifikasikan sebagai protokol bebas konflik dan pertikaian.

- **Protokol Bebas Konflik**: Protokol ini memastikan transmisi berhasil setiap saat tanpa mengganggu transmisi lainnya. Ini selanjutnya dibagi menjadi protokol bebas konflik statis atau dinamis di mana host berkomunikasi dengan alokasi saluran secara statis atau dinamis.
- **Alokasi Saluran Statis**: Sumber daya saluran dalam skema bebas konflik statis bergantung pada waktu, frekuensi, atau frekuensi waktu campuran. Saluran dibagi berdasarkan rentang frekuensi (bandwidth) ke satu host untuk sebagian kecil waktu seperti pada time Division Multiple Access (TDMA) atau memberikan sebagian kecil rentang frekuensi ke setiap host sepanjang waktu seperti pada pembagian frekuensi akses ganda (FDMA) atau menyediakan sebagian bandwidth kepada setiap host untuk waktu yang sangat singkat seperti dalam akses ganda pembagian kode (CDMA).
- **Alokasi Saluran Dinamis**: Alokasi saluran dinamis mempertimbangkan alokasi saluran berdasarkan permintaan sehingga penggunaan saluran secara optimal dapat dipastikan. Host yang hanya memerlukan sedikit penggunaan saluran namun tetap membiarkan saluran menganggur hampir sepanjang waktu dalam bagian yang dialokasikan dalam alokasi statis dapat meninggalkan sumber daya saluran untuk host yang lebih aktif. Ini selanjutnya dapat diklasifikasikan ke dalam skema reservasi dan token passing.

- **Skema Reservasi**: Host pertama-tama mengumumkan niat mereka untuk melakukan transmisi dalam alokasi saluran dinamis dengan berbagai skema reservasi dan berhak untuk melakukan transmisi sebelum host baru memperoleh kesempatan untuk mengumumkan niat mereka untuk melakukan transmisi.
- **Skema Token Passing**: Sebuah token tunggal baik dalam bentuk logis atau fisik diedarkan di antara host-host untuk memungkinkan host mengirimkan siapa yang memiliki token tersebut sehingga interferensi antara transmisi host lain dapat dihindari.
- **Skema Pertentangan**: Berbeda dengan skema bebas konflik, host transmisi tidak dijamin berhasil dalam skema pertikaian. Protokol harus dilengkapi dengan beberapa proses resolusi untuk menyelesaikan konflik ketika terjadi sehingga semua host dapat melakukan transmisi dengan sukses. Protokol resolusi yang berbeda membangun skema perselisihan. Dalam skema pertikaian, host yang menganggur tidak melakukan transmisi sehingga tidak menggunakan sumber daya saluran.
- **Resolusi Statis**: Mengacu pada hak host pertama untuk melakukan transmisi ketika terjadi konflik. Hal ini juga didasarkan pada probabilitas dimana jadwal transmisi untuk host yang mengganggu dipilih dari distribusi tetap yang tidak bergantung pada jumlah sebenarnya dari host yang mengganggu. Contohnya adalah protokol jenis Aloha dan berbagai versi protokol Carrier Sense Multiple Access (CSMA).
- **Resolusi Dinamis**: Ini menentukan prioritas tertinggi atau prioritas terendah suatu paket berdasarkan waktu kedatangan di sistem. Penyelesaiannya juga bisa bersifat probabilistik. Beberapa protokol yang didasarkan pada skema ini adalah banyaknya paket yang mengganggu dan skema back-off eksponensial dari Ethernet.

**Aloha dan Aloha Berlubang**

Pengembangan protokol Aloha sendiri merupakan upaya pionir menuju jaringan komputer. Ia juga dikenal sebagai Aloha murni. Ini dikembangkan oleh Universitas Hawaii pada tahun 1970 di bawah keahlian Norman Abramson dan Franklin Kuo untuk proyek yang disponsori oleh DARPA. Ini meletakkan dasar bagi evolusi Ethernet. Jaringan Aloha dikembangkan dengan tujuan memungkinkan orang-orang di lokasi berbeda untuk mengakses sistem komputer utama. Berbeda dengan ARPANET, jaringan Aloha telah menggunakan radio paket.

Jaringan Aloha juga memprakarsai konsep media transmisi bersama. Aloha menggunakan frekuensi yang sama untuk setiap node sehingga memerlukan manajemen pertikaian. Aloha biasa mengirim data melalui teletype yang kecepatan datanya biasanya tidak melebihi 80 karakter per detik. Faktanya, jaringan Aloha adalah jaringan sebenarnya di mana semua komputer terhubung ke Alohanet dan mereka dapat mengirim data kapan saja tanpa campur tangan operator. Itu tidak menimbulkan batasan jumlah komputer yang terlibat. Hal ini dimungkinkan karena media yang digunakan adalah radio, sehingga tidak memerlukan biaya tetap.

**Protokol Aloha**

Protokol Aloha bekerja pada OSI layer 2 untuk membangun jaringan LAN dengan domain siaran. Versi pertama dari protokol ini bersifat dasar:

- Setiap kali pengguna memiliki frame untuk dikirim, ia hanya mengirimkan frame tersebut.
- Jika terjadi tabrakan, ia menunggu selama jangka waktu acak dan mengirimkannya kembali

Pure Aloha memiliki throughput maksimal sekitar 18,4%. Ini berarti bahwa 81,6% dari total bandwidth yang tersedia terbuang sia-sia karena stasiun mencoba untuk berbicara pada waktu yang sama. Pada protokol Slotted Aloha throughput dapat ditingkatkan hingga 36,8% dengan ketentuan stasiun tidak dapat mengirim kapan pun. Itu bisa dikirim tepat di awal slot waktu, dan dengan demikian tabrakan berkurang. Anda harus tahu bahwa Slotted Aloha masih digunakan saat ini dan digunakan pada jaringan komunikasi satelit taktis bandwidth rendah oleh Militer AS. Untuk memitigasi masalah perselisihan, sejumlah cara diusulkan. Ini diberikan di bawah ini:

- **Multiplexing Frekuensi**: Dalam hal ini, setiap node diharuskan menggunakan frekuensi radio yang berbeda. Namun hal ini memerlukan setiap node yang ditambahkan agar dapat disetel oleh semua mesin lainnya.
  Sebentar lagi akan ada ratusan frekuensi seperti itu, dan radio yang mampu mendengarkan sejumlah frekuensi ini pada saat yang sama harganya sangat mahal.
- **Time Division Multiplexing**: Dalam hal ini, setiap node diberikan slot waktu untuk mengirimkan pesan. Berbeda dengan multiplexing frekuensi, setiap node tetap memiliki satu frekuensi radio. Kerugian dari metode ini terletak pada pemborosan waktu ketika sebuah node tidak mempunyai apa-apa untuk dikirim pada slot tertentu. Hal ini membuat sebuah node harus menunggu lama untuk mengirimkan data padahal nodenya banyak.
- **Akses Berganda Carrier Sense**: Untuk mengatasi masalah slot waktu kosong, Aloha merancang teknik akses ganda indra operator yang kini telah menjadi standar de facto. Seperti yang telah Anda pelajari bahwa sistem ini tidak memiliki multiplexing tetap sama sekali. Sebaliknya setiap node mendengarkan untuk melihat apakah ada orang lain yang menggunakan saluran tersebut, dan jika mereka tidak mendengar siapa pun, mereka mulai berbicara. Namun, teknik ini menghemat waktu namun tidak selalu mudah karena jika node pertama mulai menggunakan radio, maka node tersebut mungkin akan menggunakannya selama yang diinginkannya dan oleh karena itu membiarkan node lain menunggu tanpa batas waktu. Hal ini melahirkan pemecahan pesan menjadi paket-paket kecil, dan menyatukannya di antara slot waktu dari satu node ke node lainnya. Hal ini memungkinkan node lain untuk mengirimkan paket mereka di antara keduanya, sehingga semua orang dapat berbagi media pada saat yang sama. Untuk menghindari masalah tabrakan ketika dua node mencoba untuk memulai siaran mereka pada saat yang sama, protokol Aloha merancang teknik pengakuan ketika pengirim selalu dapat mengetahui apakah frame-nya dihancurkan

dengan mendengarkan saluran. Untuk LAN, umpan balik bersifat langsung; sedangkan untuk satelit terdapat waktu tunda yang lama yaitu 270 ms sebelum pengirim mengetahuinya. Dalam hal ini, setelah mengirim paket apa pun, node mendengarkan untuk melihat apakah pesan mereka dikirim kembali oleh hub pusat. Jika mereka menerima pesannya kembali, mereka dapat melanjutkan ke paket berikutnya. Jika tidak, ini berarti bahwa beberapa tabrakan dengan paket node lain telah menghalanginya untuk mencapai tujuan yang dituju. Hal ini mendorong mereka untuk mengirim lagi setelah menunggu waktu yang acak. Sistem penghindaran tabrakan ini memungkinkan node mana pun menggunakan seluruh kemampuan jaringan jika tidak ada orang lain yang menggunakannya.

**Aloha berlubang**

Ia menggunakan paket tick jam kecil untuk memungkinkan node yang dituju mengirim paketnya segera setelah menerima tick jam. Protokol ini meningkatkan pemanfaatan saluran secara keseluruhan, dengan mengurangi kemungkinan tabrakan hingga setengahnya. Namun keuntungan ini tidak cukup dan oleh karena itu penelitian lebih lanjut tentang hal yang sama untuk jaringan kabel oleh Bob Metcalfe meningkatkan penghindaran tabrakan pada jaringan sibuk dan menetapkan standar untuk Ethernet yang dikenal sebagai CSMA/CD, pengertian operator, akses ganda, deteksi tabrakan. Pada unit sebelumnya hal ini telah dijelaskan dengan cukup rinci.

Kinerja Aloha atau Slotted Aloha ditentukan dengan bantuan throughput dan penundaan rata-rata. Throughput adalah jumlah rata-rata frame yang berhasil ditransmisikan per satuan waktu. Nilai yang tinggi menunjukkan kinerja yang baik. Distribusi Poisson dapat memodelkan laju transmisi frame dengan laju kedatangan rata-rata l frame/s. Kita dapat mengasumsikan rata-rata panjang frame tf detik maka lalu lintas saluran yang dinormalisasi atau jumlah rata-rata frame lama dan baru yang dikirimkan per waktu frame adalah

$G = \lambda\tau_f$ Erlang

Througtput kemudian diberikan oleh $S = G\lambda\tau_f$ (tidak ada tumbukan).

Probabilitas suatu frame tidak mengalami tumbukan diberikan oleh

$P_0 = e^{-2G}$ untuk Aloha

$P_0 = e^{-G}$ untuk Slotted Aloha

Throughput/waktu frame kemudian diberikan oleh

$S = G \times e^{-2G}$ untuk Aloha

$S = G \times e^{-G}$ untuk Slotted Aloha

Thoughtput Maksimum

$$\frac{dS}{dG} = e^{-2G} - 2G \times e^{-2G}$$

Maka

$G_{Max} = \frac{1}{2}$ dan $S = \frac{1}{2}e^{-1} = 0.1839$ untuk Aloha

$$\frac{dS}{dG} = e^{-G} - G \times e^{-G}$$

Maka

$G_{Max} = 1$ dan $S = e^{-1} = 0.3679$ untuk Slotted Aloha

**Mengelola Akses ke Jaringan**

Anda mungkin berpikir jika semua stasiun pada satu waktu mulai mengakses jaringan, akan terjadi kekacauan. Oleh karena itu, ada banyak metode untuk mengelola akses ke jaringan. Jika semua stasiun jaringan mencoba mengirim data sekaligus, pesan-pesan tersebut akan menjadi tidak dapat dipahami, dan tidak ada komunikasi yang dapat terjadi. Diperlukan mekanisme perangkat untuk menghindari kebuntuan tersebut. Beberapa metode penting tercantum di bawah ini dan dibahas di tempat lain dalam materi pelajaran ini:

- Akses Berganda Carrier-Sense dengan Deteksi Tabrakan (CSMA/CD)
- Akses Berganda Carrier-Sense dengan Penghindaran Tabrakan (CSMA/CA)
- Penyerahan Token
- Jajak pendapat
  - **Carrier Sense Multiple Access**: Dalam hal ini ketika pengguna ingin melakukan transmisi, dia terlebih dahulu mendengarkan media untuk memastikan apakah transmisi lain sedang berlangsung atau tidak. Ini dikenal sebagai pengertian pembawa. Jika saluran tersebut sedang digunakan, dia harus menunggu. Jika medianya menganggur, ia dapat mengirimkan. Jika saluran sedang sibuk, dia harus menunggu beberapa saat sebelum mencoba mendengarkan. Hal ini telah dijelaskan secara rinci di bagian lain tutorial.
  - **CSMA dengan Collision Detection**: Jika pengguna ingin melakukan transmisi, ia mendengarkan terlebih dahulu untuk memastikan apakah saluran tersebut gratis atau tidak. Jika salurannya menganggur, dia mentransmisikan. Jika saluran sedang sibuk, dia terus mendengarkan sampai saluran tersebut kosong, lalu segera mentransmisikannya. Selama transmisi, ia terus mendengarkan untuk mendeteksi tabrakan. Jika tabrakan terdeteksi, ia segera menghentikan transmisi, dan menunggu beberapa saat sebelum kembali ke langkah transmisi lagi. Pada dasarnya CSMA/CD memiliki tiga negara bagian. Yaitu masa transmisi, masa pertikaian, dan masa menganggur. Hal ini juga dijelaskan secara rinci di bagian lain tutorial ini.
  - **Prioritas Permintaan**: Menggunakan layanan hub cerdas untuk mengendalikan transmisi data. Sinyal permintaan dikeluarkan ke hub yang menunjukkan bahwa ia ingin melakukan transmisi. Tergantung pada keadaan, hub merespons dengan pengakuan yang memungkinkan node untuk melakukan transmisi. Demikian pula node lain diperbolehkan untuk melakukan transmisi secara bergantian.
  - **Token Passing**: Sesuai dengan namanya, ia menggunakan token atau serangkaian bit untuk memungkinkan sebuah node melakukan transmisi. Perangkat setelah menangkap token dapat mengirimkan data ke jaringan. Ketika node tertentu selesai mengirimkan datanya, node tersebut meneruskan token tersebut ke node berikutnya dalam topologi. Spesifikasi protokol menandakan berapa lama suatu perangkat dapat

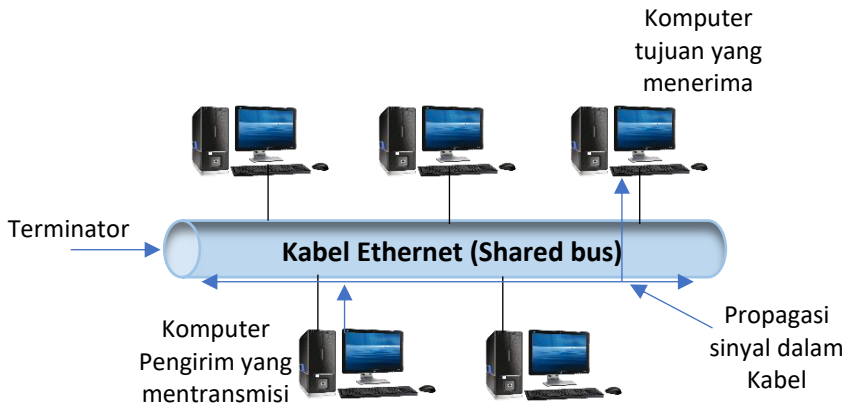
menyimpan token, berapa lama perangkat dapat mengirimkannya, dan bagaimana menghasilkan token baru jika tidak ada token yang beredar.

- **Polling**: Metode ini menggunakan pengontrol pusat untuk memastikan permintaan node dalam urutan polling. Oleh karena itu, pengontrol pusat akan mengizinkan mereka untuk melakukan transmisi dalam waktu terbatas, kemudian perangkat berikutnya akan disurvei.

## 8.7 TEKNOLOGI ETHERNET

Di antara standar LAN, IEEE 802.3 Ethernet telah menjadi salah satu media LAN yang paling banyak digunakan. Penggunaannya yang luas dan ketersediaannya yang luas menjadikannya salah satu media LAN termurah. Apalagi bisa mengusung transmisi berkecepatan tinggi. Evolusi Ethernet menjadi media yang diterima secara luas dapat ditelusuri kembali ke akhir tahun 1970an ketika standar Ethernet pertama dibuat oleh Xerox. Sekitar tahun 1984, DIX (konsorsium Digital, Intel, dan Xerox) dan IEEE menciptakan standar untuk Ethernet yang dikenal sebagai IEEE 802.1. Selanjutnya, kelompok-kelompok ini memisahkan pekerjaan mereka dan bekerja sebagai Grup Logical Link Control (LLC) yang berfokus pada konektivitas ujung ke ujung dan kemudian disebut Komite IEEE 802.2. Kelompok lain, yang disebut Data Link dan Medium Access Control (DLMAC) mengambil tanggung jawab untuk mengembangkan protokol akses menengah. Kelompok ini kemudian membentuk komite untuk Ethernet (802.3), Token Bus (802.4), dan Token Ring (802.5).

Ethernet adalah alternatif LAN berkecepatan tinggi yang paling murah. Ia mengirim dan menerima data dengan kecepatan 10 juta bit per detik. Data ditransfer antar lemari kabel menggunakan kabel koaksial berat (jaring tebal) atau kabel serat optik. Koaksial jaring tebal masih digunakan untuk jarak menengah-jauh yang memerlukan tingkat keandalan sedang. Fiber memiliki jangkauan yang lebih jauh dan memiliki keandalan yang lebih baik tetapi biayanya lebih tinggi. Untuk menghubungkan sejumlah stasiun kerja dalam ruangan yang sama, biasanya digunakan kabel koaksial ringan yang disebut jaring tipis. Media lain ini mencerminkan pandangan lama tentang komputer stasiun kerja di lingkungan laboratorium. Gambar 8.6 menunjukkan skema Ethernet dimana pengirim mentransmisikan gelombang pembawa termodulasi yang merambat dari pengirim ke kedua ujung kabel.




**Gambar 8.6 Arus sinyal melewati Ethernet**

Ethernet pertama kali dirancang dan dipasang oleh Xerox Corporation di Palo Atto Research Center (PARC) pada pertengahan tahun 1970. Pada tahun 1980 DEC Intel dan Xerox mengeluarkan spesifikasi bersama, yang telah menjadi standar de facto. Ethernet dari periode ini sering disebut DIX setelah perusahaan sponsornya Digital, Intel, dan Xerox. Ethernet yang menggunakan perangkat angka seperti hub, switch dan repeater sudah dijelaskan sebelumnya. Ethernet IEEE 802.3. Di sini kita akan mempelajari implementasi LAN beserta beberapa isu utama yang terkait.

**Tabrakan dan Domain Siaran**

Mekanisme akses media adalah bagian yang sangat penting dari teknologi Ethernet dan sekarang kita akan memahami domain tabrakan dan domain siaran. Tabrakan tidak lain adalah jatuhnya data ketika semua perangkat atau node pada satu segmen mengirim data melalui kabel fisik yang sama. Dalam kasus hub, semua node yang terhubung ke hub berada dalam domain tumbukan yang sama. Kita mungkin ingat bahwa hub pada dasarnya adalah sebuah repeater yang mengirimkan kembali sinyal apa pun yang diterimanya dari masing-masing portnya dan sinyal ini dapat diakses oleh semua node yang terhubung ke hub yang sama. Hal ini menjelaskan mengapa setiap pesan atau sinyal yang dikirim oleh node mana pun diperlakukan sebagai sinyal siaran dan oleh karena itu semua node pada hub yang sama berada dalam domain siaran yang sama.

**Bingkai Ethernet**

Hal ini juga telah dijelaskan secara rinci pada Bagian I; namun, gambaran sepintas tentang hal yang sama disajikan di sini. Ada tiga elemen dasar yang membuat Ethernet. Ini adalah media fisik, seperangkat aturan kontrol akses media, dan frame Ethernet. Ethernet mengambil paket dari protokol lapisan atas, dan menempatkan informasi header dan footer di sekitar data sebelum melintasi jaringan. Proses ini disebut enkapsulasi data atau framing. Frame Ethernet berjalan pada lapisan Data Link model OSI dan harus berukuran minimal 64 byte dan maksimum 1518 byte. Gambar 8.7 menunjukkan frame Ethernet IEEE 802.3 dan frame Ethernet.

| 7 Bytes | 1 Bytes | 6 Bytes | 6 Bytes | 2 bytes | 46 – 1500 Bytes | 4 Bytes |
|---|---|---|---|---|---|---|
| Pembukaan (P) 1010....10.. | SFD 10101011 | SA | DA | Bidang panjang | | FCS |

**Gambar 8.7 Frame Ethernet IEEE 802.3**

Di bawah ini adalah penjelasan singkat setiap bidang dalam frame Ethernet IEEE 802.3:

- **Pembukaan** (P): Ini adalah awal frame dan digunakan untuk membuat sinkronisasi bit dengan bantuan pola bolak-balik satu dan nol yang digunakan oleh penerima.
- **SFD** (Start Frame Delimiter): Memungkinkan penerima mengetahui awal frame dan berisi panjang satu byte.

- **Alamat Tujuan** (DA) dan **Alamat Sumber** (SA): Masing-masing panjangnya enam byte dan terdapat dalam perangkat keras pada kartu antarmuka Ethernet.
- **Type Field**: Dalam frame Ethernet, ini adalah field dua byte setelah alamat sumber. Setelah pemrosesan Ethernet, bidang tipe menentukan protokol lapisan atas untuk menerima data.
- **Panjang Bidang**: Ini adalah bidang dua byte yang mengikuti alamat sumber. Bidang panjang menunjukkan jumlah byte data yang mengikuti bidang ini dan mendahului bidang urutan pemeriksaan bingkai.
- **Bidang Data**: Ini adalah tempat di mana informasi yang akan dikirim terkandung dalam bingkai. Ini mengikuti bidang jenis dan panjang. Setelah proses lapisan Fisik dan lapisan Tautan selesai, data ini dikirim ke protokol lapisan atas. Dengan Ethernet, protokol lapisan atas diidentifikasi di bidang tipe. Dengan IEEE 802.3, protokol lapisan atas harus didefinisikan dalam bagian data frame. Jika data frame tidak cukup besar untuk mengisi frame ke ukuran minimum 64 byte, padding byte dimasukkan untuk memastikan setidaknya frame 64 byte.
- **Bidang FCS** (Frame Check Sequence) atau CRC (Cyclic Redundancy Check): Bidang ini berada di akhir frame. Urutan pemeriksaan bingkai menghitung ulang jumlah bingkai untuk memastikan tidak ada yang hilang atau rusak. CRC berlaku untuk semua bidang kecuali bidang pertama, kedua, dan terakhir.

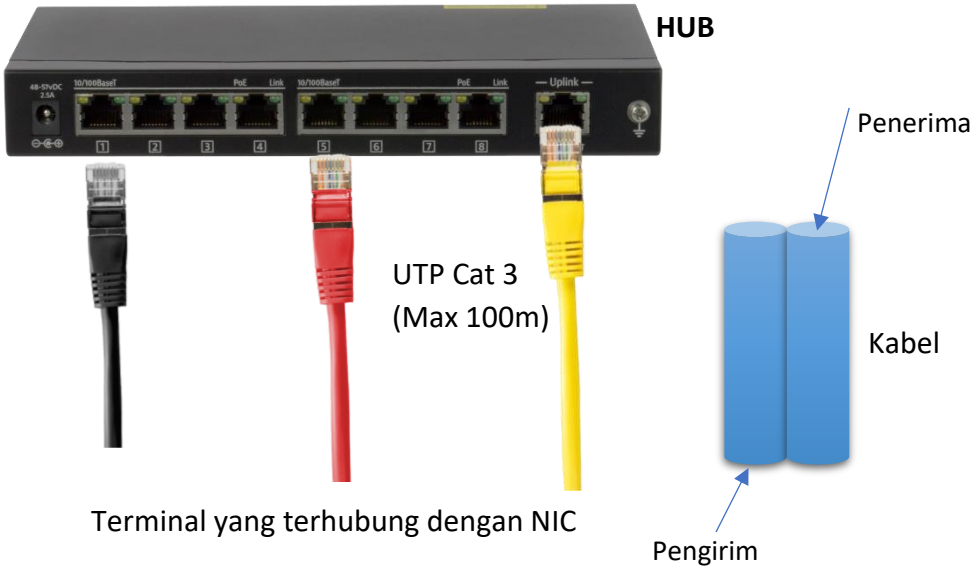
**Fast Ethernet**

**100BaseT (Fast Ethernet)**

100BaseT adalah standar LAN berkecepatan tinggi dan dianggap sebagai variasi dari 10BaseT. Ini distandarisasi sebagai IEEE 802.3u. Ini beroperasi dengan mekanisme akses sebagai CSMA/CD dan memberikan kecepatan transmisi 100 Mbps melalui hub switching Ethernet. Beberapa koneksi 10 Mbps didukung melalui beberapa port pada switch. UTP Cat 3, 4, atau 5 dapat digunakan dalam konfigurasi 4-pasangan. UTP Cat 5 umumnya digunakan untuk diameter LAN maksimal 500 meter. Tiga pasang digunakan untuk transmisi, dengan pasangan keempat digunakan untuk pensinyalan dan kontrol (CSMA/CD) dalam mode setengah dupleks. Koneksi ke node, server dan hub switching lainnya disediakan pada kecepatan 100 Mbps, mendukung sepuluh saluran 10-Mbps. Media 100 Mbps termasuk fiber (hingga 30 mil atau 50 Km tanpa repeater) dan Cat 5 UTP pada jarak 100 meter.

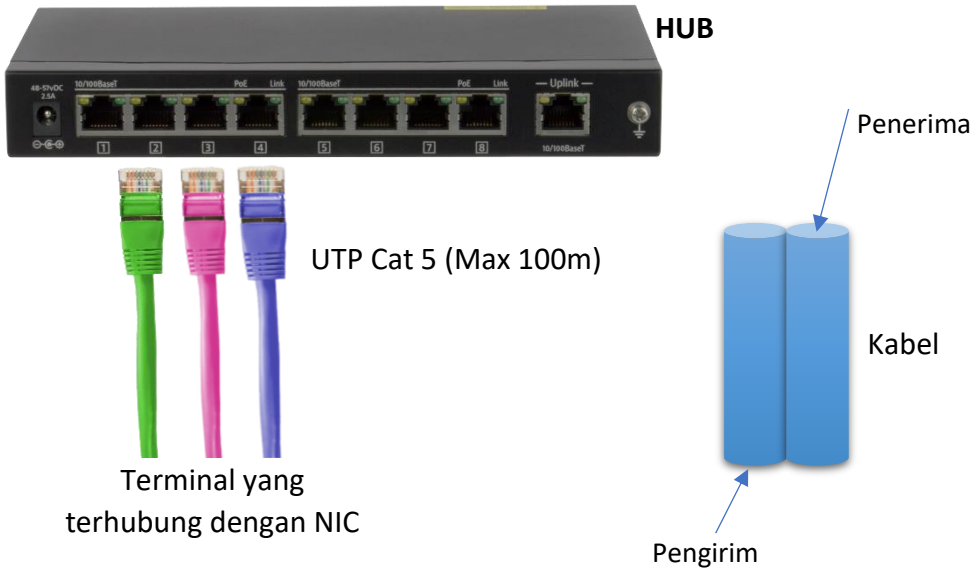
**Tipe 100Base-T**

100BaseT dapat dibagi menjadi 100BaseTX, 100BaseT4 dan 100BaseFX, tergantung pada jenis media transmisi yang digunakan seperti yang dijelaskan di atas. UTP kategori 5 dua pasang, UTP kategori 3 empat pasang, dan kabel serat optik masing-masing digunakan untuk 100BaseTX, 100BaseT4, dan 100BaseFX. Standar ini telah didefinisikan di IEEE802.3u.




**Gambar 8.8 Konfigurasi dari 100BaseTx**

Gambar 8.8 menunjukkan konfigurasi perangkat keras 100BaseTx. Seperti 100BaseTx, terminal dihubungkan ke hub dengan 100BaseTx. UTP Cat5 digunakan untuk koneksi. 100BaseTx telah dikembangkan berdasarkan 10BaseT untuk memungkinkan kecepatan transmisi yang lebih tinggi, vendor dapat dengan mudah mengembangkan peralatan periferal untuk 100BaseTx. Hampir semua hub dan NIC untuk 100BaseTx juga dapat digunakan untuk 10BaseT.

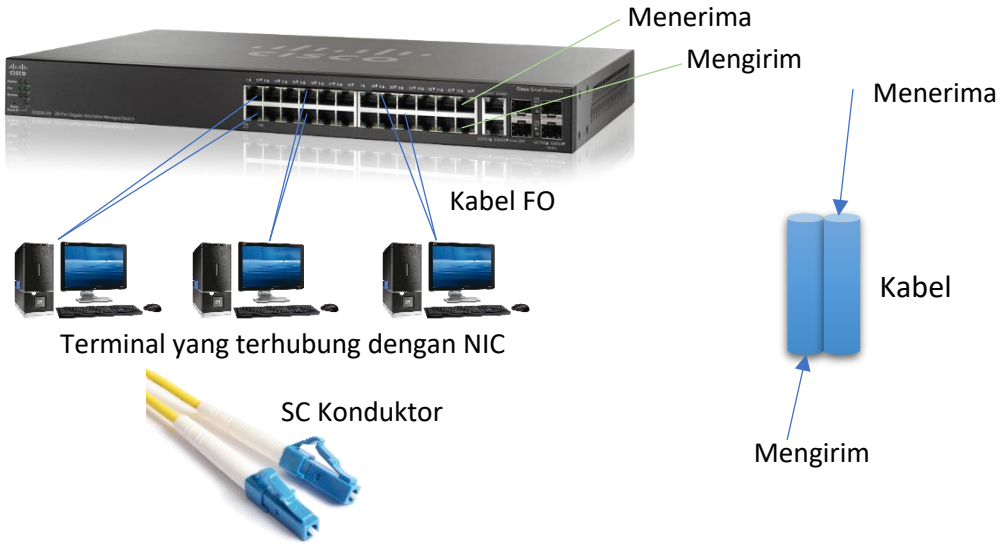



**Gambar 8.9 Konfigurasi Hardware dari 100BaseT4**

Gambar 8.9 menunjukkan konfigurasi perangkat keras 100BaseT4. Hal ini sama seperti untuk 100BaseTx. UTP Cat3 digunakan untuk koneksi. Meskipun awalnya dimaksudkan untuk digunakan sebagai jalur transmisi pada 10Mbps, kabel jenis ini sekarang menawarkan kecepatan transmisi 100Mbps sebagai hasil pengaturan khusus, termasuk peningkatan

pemrosesan sinyal dan penggunaan tiga dari empat pasang secara bersamaan untuk transmisi atau penerimaan. Hal ini memungkinkan pengenalan LAN 100Mbps bebas masalah tanpa perlu mengganti kabel 10BaseT. Namun kabel ini harus berupa kabel empat pasang.

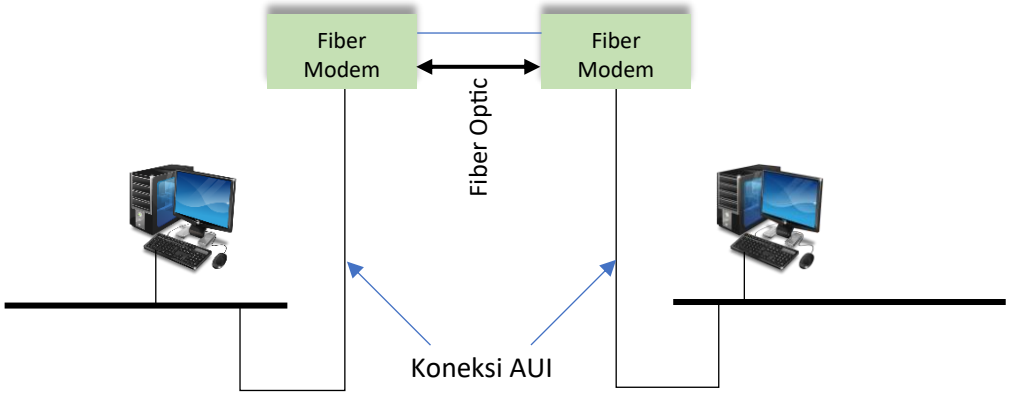
Gambar 8.10 menunjukkan konfigurasi perangkat keras 100BaseFx. Konektor SC yang bertipe push-lock direkomendasikan untuk digunakan sebagai konektor antarmuka. Namun, beberapa konektor lain termasuk konektor ST juga ditetapkan sebagai opsi. Dua kabel serat satu untuk transmisi dan yang lainnya untuk penerimaan diperlukan untuk setiap sambungan.




**Gambar 8.10 Konfigurasi Hardware dari 100BaseFx**

**Ekstensi Serat Optik**

Serat bersifat sangat fleksibel dan memberikan redaman yang lebih sedikit serta kekebalan yang baik terhadap kebisingan. Serat optik dengan modem fiber digunakan untuk memperluas LAN melampaui batasnya. Gambar 8.11 mengilustrasikan konsep modem fiber untuk memperluas koneksi Ethernet. Modem serat dimasukkan antara AUI dan kabel serat optik di kedua segmen Ethernet. Koneksi AUI ini mungkin datang langsung dari komputer atau transceiver tergantung pada jenis kabel yang digunakan. Modem serat melakukan konversi sinyal AUI menjadi representasi digital dan pulsa cahaya, yang dapat dikirim melalui kabel serat optik dan sebaliknya. Mekanisme ini dapat beroperasi secara efektif hingga beberapa kilometer. Mereka digunakan secara luas untuk menghubungkan komputer yang terletak di gedung yang berbeda.



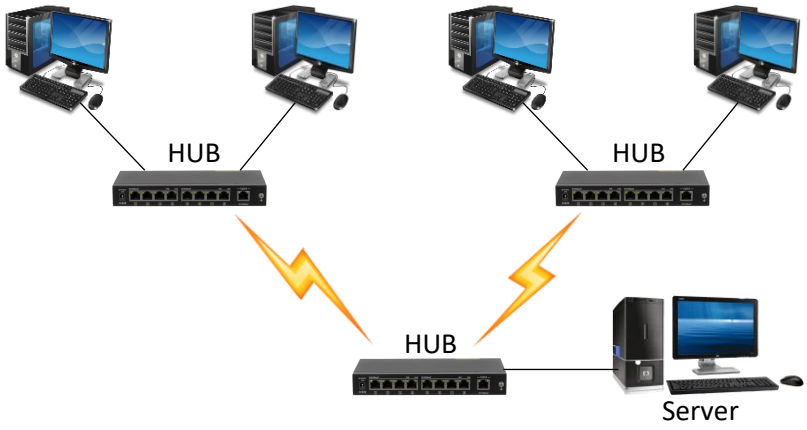

**Gambar 8.11 Ekstensi LAN menggunakan Fiber Modem dan Kabel**

## 8.8 LAN NIRKABEL

Jaringan nirkabel menyediakan konektivitas dengan menggunakan frekuensi sinyal radio untuk berkomunikasi antar komputer dan perangkat jaringan lainnya dan koneksi ke Internet di mana saja di rumah atau kantor. Jaringan nirkabel dikenal sebagai jaringan WiFi atau WLAN. LAN Nirkabel (WLAN) memungkinkan host untuk berkomunikasi dalam jarak pendek dengan bantuan sinyal radio atau inframerah sebagai pengganti kabel jaringan tradisional. WLAN membantu memperluas LAN kabel yang sudah ada seperti Ethernet dengan mengimplementasikan jalur akses ke tepi jaringan kabel. Host terhubung ke Internet melalui titik akses menggunakan adaptor jaringan nirkabel seperti adaptor Ethernet. Adaptor LAN nirkabel juga disebut sebagai NIC nirkabel atau kartu jaringan nirkabel digunakan di setiap perangkat yang ingin terhubung pada jaringan nirkabel. Umumnya, jaringan nirkabel dibangun di atas router nirkabel yang bertindak sebagai stasiun pangkalan untuk menyediakan jalur komunikasi melalui jaringan tersebut dan memungkinkan komputer terdekat untuk terhubung ke Internet atau satu sama lain.

Router nirkabel berfungsi seperti router untuk jaringan kabel. Namun, sebagian besar jaringan nirkabel menggunakan router nirkabel. Untuk mengurangi biaya jaringan nirkabel, jaringan nirkabel dapat dibangun tanpa menggunakan router. Diamati bahwa tidak ada perangkat keras nirkabel selain adaptor yang diperlukan untuk membangun LAN nirkabel kecil (WLAN). Namun, titik akses nirkabel dan/atau router nirkabel digunakan untuk meningkatkan kinerja WLAN, mengakomodasi lebih banyak komputer, dan meningkatkan jangkauan jaringan. Titik akses yang disediakan sebagai perangkat tepi dalam jaringan nirkabel merupakan alternatif pengganti router dan membantu memperluas jaringan nirkabel dengan menggabungkannya ke jaringan kabel yang sudah ada. Sebuah titik akses atau router tunggal dianggap memiliki jangkauan yang cukup untuk menjangkau sebagian besar rumah, namun gedung perkantoran memerlukan beberapa titik akses. Seiring dengan router atau titik akses, antena nirkabel digunakan untuk meningkatkan jangkauan komunikasi sinyal radio nirkabel secara signifikan. Jaringan nirkabel dengan adaptor nirkabel mengkodekan data biner ke frekuensi radio dan router nirkabel mengirimkannya. Proses sebaliknya terjadi di komputer host.

Kumpulan jaringan nirkabel terdiri dari komputer yang dilengkapi dengan antena radio berdaya rendah, yang terhubung secara nirkabel ke antena hub lain, komputer, server, periferal, dan host melalui koneksi kabel. Mereka juga menghubungkan beberapa antena hub untuk transmisi antar ruangan, lantai dan bangunan. Untuk melayani banyak host, teknologi radio spektrum tersebar digunakan untuk memanfaatkan bandwidth terbatas secara efektif. Spektrum penyebaran melibatkan penyebaran paket aliran data pada rentang frekuensi, daripada menggunakan frekuensi transmisi tunggal. Manfaat sampingan dari spektrum penyebaran adalah peningkatan keamanan, karena sinyal hampir tidak mungkin dicegat. Beberapa LAN nirkabel juga menggunakan transmisi urutan langsung yang berarti bahwa sinyal dikirim secara bersamaan melalui beberapa frekuensi dan oleh karena itu meningkatkan peluangnya untuk sampai ke hub akses. Gambar 8.12 menunjukkan contoh diagram blok jaringan nirkabel.




**Gambar 8.12 Konfigurasi Wireless LAN**

Jaringan nirkabel menjadi populer karena fitur pengaturannya yang mudah dan tidak memerlukan kabel. Komputer dapat dihubungkan di mana saja di rumah dan kantor tanpa memerlukan kabel. Beberapa fitur jaringan nirkabel diberikan di bawah ini:

- LAN Nirkabel adalah teknologi yang relatif belum matang namun menjadi populer dengan sangat cepat.
- Biaya akuisisi tidak terlalu rendah bila dibandingkan dengan LAN kabel, meskipun biaya konfigurasi ulang hampir tidak ada.
- WLAN sebagian besar merupakan campuran media kabel dan nirkabel yang memiliki titik akses atau router nirkabel yang terhubung ke jaringan kabel melalui kabel koaksial, universal serial bus (USB) atau koneksi Ethernet.
- Rentang frekuensi terletak pada pita 900 MHz, 2 GHz dan 5 GHz.
- Antena hub terletak pada titik pusat dimana garis pandang dapat dibuat dengan berbagai antena terminal.
- Bandwidth LAN radio nirkabel kira-kira 4 Mbps.
- Throughput efektif lebih banyak pada kisaran 1 hingga 2 Mbps per hub.

- Teknik transmisi inframerah juga dapat digunakan. PDA (Personal Digital Assistant) memanfaatkan inframerah secara luas untuk menjalin hubungan dengan host dan PDA lain untuk transfer data. Teknologi inframerah yang ditingkatkan baru-baru ini telah dibuktikan pada kecepatan 1,5, 4, dan bahkan 155 Mbps.
- Kinerja kesalahan dan keamanan merupakan masalah yang cukup penting.
- IEEE 802.11a dan IEEE 802.11b merupakan standar jaringan nirkabel dengan kecepatan data masing-masing hanya 2 Mbps dan 11 Mbps. Mereka memiliki batasan jarak hingga 100 kaki dari router titik akses. Ini menggunakan pita 2,4 GHz.
- IEEE 802.11g memungkinkan kecepatan hingga 54 Mbps dan terus menggunakan pita 2,4 GHz.

Perangkat umum yang digunakan dalam jaringan nirkabel adalah:

1. **Adaptor Jaringan Nirkabel**: Adaptor jaringan nirkabel digunakan untuk menghubungkan komputer ke jaringan. Adaptor nirkabel tersedia sebagai perangkat keras seperti kartu PCI Ethernet, perangkat PCMCIA, perangkat USB, dll. Beberapa perangkat adaptor jaringan nirkabel untuk komputer laptop merupakan chip sirkuit terintegrasi yang sudah terpasang di dalam komputer. Perangkat perangkat lunak yang disebut driver perangkat digunakan untuk mengkomunikasikan perangkat jaringan dengan perangkat lunak aplikasi di lingkungan sistem operasi yang berbeda. Adaptor virtual sebagai program perangkat lunak sederhana banyak digunakan di jaringan pribadi virtual (VPN).
2. **Router Nirkabel**: Router nirkabel digunakan untuk mengkonfigurasi komputer dengan adaptor jaringan nirkabel. Mereka mungkin juga memiliki saklar jaringan untuk memungkinkan beberapa komputer dihubungkan dengan kabel Ethernet dan berbagi modem kabel dan koneksi Internet DSL. Beberapa router nirkabel juga memiliki firewall bawaan untuk melindungi jaringan dari penyusup. Mereka tersedia berdasarkan protokol jaringan nirkabel yang didukungnya. Protokol jaringannya adalah 802.11g, 802.11a, 802.11b atau kombinasinya.
3. **Titik Akses Nirkabel**: Mereka adalah node yang dikonfigurasi pada jaringan area lokal nirkabel (WLAN) untuk bertindak sebagai pemancar dan penerima pusat sinyal radio WLAN dan untuk mendukung standar komunikasi nirkabel WiFi. Titik akses nirkabel (WAP) yang digunakan di jaringan rumah atau bisnis kecil umumnya berukuran kecil, perangkat keras khusus yang memiliki fitur adaptor jaringan, antena, dan pemancar radio internal. Namun, WLAN kecil dapat berfungsi tanpa titik akses. Mereka digunakan dalam mode ad hoc atau peer-to-peer, titik akses mendukung mode infrastruktur. Infrastruktur ad hoc digunakan untuk menjembatani WLAN dengan LAN Ethernet berkabel sehingga dapat ditingkatkan untuk mendukung lebih banyak host.
4. **Wireless Range Extender**: Extender jangkauan nirkabel digunakan untuk meningkatkan jarak penyebaran sinyal WLAN. Dengan demikian meningkatkan potensi sinyal untuk mengatasi hambatan dan meningkatkan kualitas sinyal jaringan nirkabel secara keseluruhan. Ekspander jangkauan nirkabel juga dikenal sebagai perluasan jangkauan atau penguat sinyal dan berfungsi sebagai relai atau pengulang jaringan

dengan menangkap dan memantulkan sinyal WiFi dari router dasar atau titik akses jaringan.

**Kesetiaan Nirkabel (Wi-Fi)**

WLAN dikenal sebagai WiFi dan beroperasi pada keluarga standar 802.11 yang ditentukan oleh IEEE. 802.11b dianggap sebagai standar pertama di 802.11 yang menikmati popularitas luas. Namun, standar seperti 802.11a, 802.11b, 802.11g, dan 802.11n tersedia untuk WiFi. Aliansi WiFi memeriksa spesifikasi produk 802.11 dan mensertifikasi produk tersebut untuk memastikan kompatibilitas dengan produk lain.

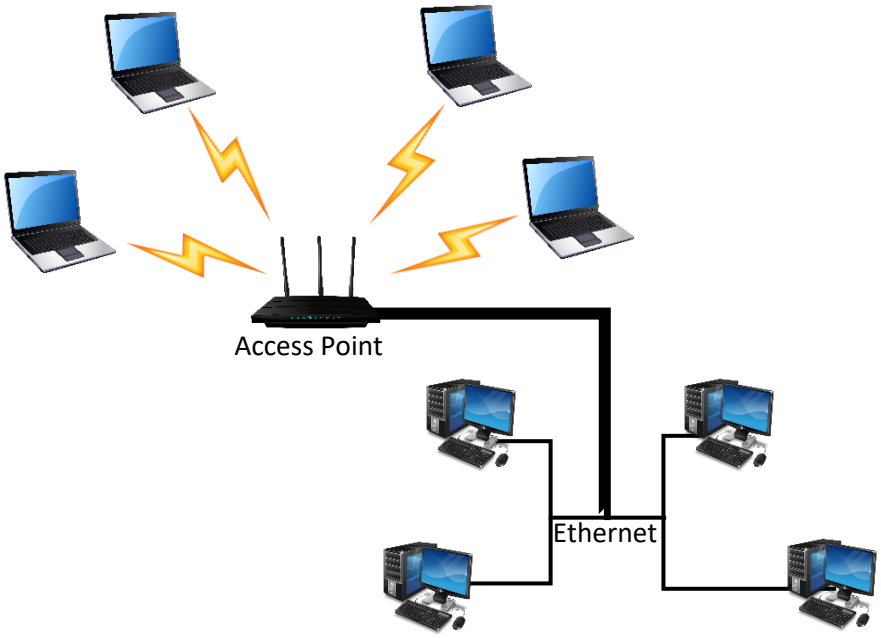
- **802.11**: Merujuk pada nama generik keluarga standar jaringan nirkabel dari IEEE. Mereka mendefinisikan aturan untuk komunikasi pada jaringan area lokal nirkabel (WLAN) dalam standar termasuk 802.11a, 802.11b dan 802.11g. 802.11 yang dikembangkan sekitar tahun 1997, mendefinisikan WLAN untuk beroperasi pada 1-2 Mbps. Itu tidak digunakan saat ini.
- **802.11a**: Ini adalah standar komunikasi WLAN yang mendukung bandwidth maksimum 54 Mbps dengan sinyal radio dalam rentang frekuensi di atas 5 GHz dan memberikan peningkatan kinerja dan pengurangan interferensi dibandingkan standar 802.11b tetapi dengan mengorbankan peningkatan biaya titik akses secara signifikan dan adaptor. Pita frekuensi 5 GHz 802.11a membatasi pemancar titik akses untuk mengirim sinyal melalui seperempat area pemancar titik akses 802.11b. Spektrum frekuensi 802.11a diatur dan didedikasikan hanya untuk perangkat 802.11a. Karena frekuensi tinggi, dinding dan penghalang lainnya juga secara signifikan mengurangi kinerja jaringan nirkabel 802.11a yang sebanding dengan jaringan 802.11b.
- **802.11b**: Ia menggunakan frekuensi dalam rentang 2,4 GHz yang tidak diatur, yang dapat dialokasikan ke perangkat radio lain dan oleh karena itu menghadapi lebih banyak interferensi radio dari perangkat tersebut. Namun, rendahnya biaya perangkat 802.11b membuatnya populer untuk perusahaan kecil seperti rumah, kantor kecil, dll. Perangkat ini mendukung kecepatan data maksimum 11 Mbps dan dianggap lebih unggul daripada dial-up. Dibandingkan dengan kinerja 802.11b dan standar lain dari keluarga yang sama, kinerjanya dianggap lebih rendah.
- **802.11g**: Terjadi sekitar tahun 2003 untuk memperluas dan meningkatkan standar 802.11b. Ini dianggap sebagai seri terbaru dari standar IEEE 802.11 untuk komunikasi LAN nirkabel (WLAN). Perangkat yang kompatibel dengan 802.11g menyediakan bandwidth maksimum 54 Mbps dan menggunakan rentang frekuensi komunikasi yang sama yaitu 2,4 Ghz seperti 802.11b sehingga perangkat yang kompatibel dengan 802.11b dapat digunakan bersama dengan perangkat 802.11g.
- **802.11n**: Ini adalah standar industri mendatang yang sedang dikembangkan untuk jaringan WiFi berkecepatan tinggi untuk menggantikan standar WiFi 802.11a, 802.11b, dan 802.11g dengan kompatibilitas ke belakang untuk jaringan area lokal. 802.11n bermaksud menyediakan Multiple Input Multiple Output (MIMO) sehingga beberapa sinyal radio secara bersamaan dapat dikirim dan diterima menggunakan beberapa antena nirkabel secara bersamaan. Hal ini akan menyebabkan peningkatan jangkauan

dan throughput jaringan nirkabel. Standar 802.11n diharapkan mendukung bandwidth lebih besar dari 100 Mbps.

**Menerapkan WLAN**

WLAN, saat ini, beroperasi pada kecepatan yang jauh lebih tinggi mulai dari 1 Mbps hingga 20 Mbps karena pembagian spektrum oleh jumlah host yang jauh lebih kecil di wilayah yang jauh lebih kecil hingga radius maksimum sekitar seratus meter. Faktor-faktor ini menyebabkan throughput yang lebih tinggi karena area dan host yang lebih kecil menyebabkan lebih sedikit interferensi, distorsi dari lingkungan, dan berkurangnya jumlah kesalahan pada sinyal radio WLAN. Throughput WLAN yang lebih tinggi membuatnya kompatibel dengan sistem operasi jaringan yang ada dan aplikasi seperti berbagi file dan printer, akses database, dll.

Topologi yang berbeda untuk mengimplementasikan WLAN adalah spektrum tersebar termasuk urutan langsung dan lompatan frekuensi, pendekatan pita sempit berdaya rendah, HiperLAN dan LAN inframerah. Jangkauan propagasi maksimum sinyal radio yang dapat diandalkan menentukan ukuran fisik jaringan nirkabel. Jaringan nirkabel sebagian besar digunakan untuk situasi sementara seperti rapat, konferensi, dll dan oleh karena itu bersifat ad hoc dan oleh karena itu disebut sebagai jaringan ad-hoc, yang terhubung ke LAN kabel yang ada. Ini adalah titik akses di tepi jaringan nirkabel untuk menjembatani lalu lintas WLAN ke LAN kabel. Terkadang, fungsi ini disediakan oleh perangkat lunak di komputer server yang menggabungkan kartu WLAN dan kartu LAN berkabel. Namun, secara umum, perangkat keras khusus sebagai perangkat titik akses digunakan untuk fungsi ini. Gambar 8.13 menunjukkan penghubung antara WLAN dan Ethernet kabel.




**Gambar 8.13 Koneksi antara WLAN dan Ethernet**

Spread Spectrum: Ini populer di WLAN dan menyediakan operasi di sejumlah pita radio termasuk 900 MHz, 2,4 GHz, dan 5 GHz. Node nirkabel dibatasi pada daya 1 watt untuk transmisi, yang tampak sebagai gangguan bagi semua kecuali penerima yang dituju karena sifat spektrum penyebarannya.

Pita Sempit Berdaya Rendah: Memungkinkan transmisi sinyal pita sempit pada tingkat daya rendah dan dianggap sebagai alternatif teknik spektrum tersebar yang beroperasi pada kecepatan data tinggi. Pendekatan ini beroperasi pada 10 Mbps di pita 5 GHz dengan daya transmisi puncak 50 mw dengan jangkauan transmisi yang dikurangi sebesar 30 meter (100 kaki) di lingkungan rumah atau kantor.

※ **HiperLAN**: Singkatan dari LAN Radio Kinerja Tinggi. Ini adalah standar teknologi nirkabel yang dikembangkan oleh European Telecommunications Standards Institute. Ini memberikan kecepatan data sekitar 24 Mbps menggunakan lima saluran yang masing-masing memiliki lebar saluran 23,5 MHz pada pita 5 GHz. Throughput tersebut mampu mendukung aplikasi multimedia.

※ **LAN Inframerah**: Ini dianggap sebagai pendekatan alternatif terhadap WLAN berbasis radio. Jaringan inframerah bekerja pada radiasi elektromagnetik dengan panjang gelombang 820 hingga 890 nanometer setara dengan frekuensi sekitar 350.000 GHz. Kelebihan IR adalah tidak memerlukan lisensi dan masalah keamanan. Selain itu, ia memberikan potensi kapasitas yang sangat besar dan pengendalian interferensi yang baik. Kelemahan dari teknologi ini adalah tidak menembus dinding; jadi WLAN inframerah terbatas pada ruangan saja. Mereka juga tidak dapat bekerja dengan baik di area luar ruangan yang terkena sinar matahari. Asosiasi Data Inframerah yang merupakan konsorsium produsen perangkat IRDA bermaksud untuk menyediakan komunikasi IR berbiaya rendah yang ditandai dengan komunikasi terarah point-to-point hingga satu meter, konektivitas 115-Kbps dan 4-Mbps dan berjalan secara ad hoc konektivitas untuk akses LAN, akses printer dan komunikasi komputer portabel ke komputer portabel. Laptop dilengkapi dengan port IRDA.

## 8.9 BLUETOOTH

Bluetooth adalah standar teknologi nirkabel terbuka yang dipatenkan untuk bertukar data dalam jarak pendek (menggunakan transmisi radio panjang gelombang pendek dalam pita ISM dari 2400-2480 MHz) dari perangkat tetap dan seluler, menciptakan jaringan area pribadi (PAN) dengan tingkat keamanan tinggi. Dibuat oleh vendor telekomunikasi Ericsson pada tahun 1994, awalnya dirancang sebagai alternatif nirkabel untuk kabel data RS-232. Dapat menghubungkan beberapa perangkat, mengatasi masalah sinkronisasi.

Bluetooth dikelola oleh Bluetooth Special Interest Group, yang memiliki lebih dari 14.000 perusahaan anggota di bidang telekomunikasi, komputasi, jaringan, dan elektronik konsumen. SIG mengawasi pengembangan spesifikasi, mengelola program kualifikasi, dan melindungi merek dagang. Untuk dipasarkan sebagai perangkat Bluetooth, perangkat tersebut harus memenuhi standar yang ditentukan oleh SIG. Jaringan paten diperlukan untuk

menerapkan teknologi dan hanya dilisensikan untuk perangkat yang memenuhi syarat; dengan demikian protokol tersebut, meskipun terbuka, dapat dianggap sebagai hak milik.

**Implementasi Bluetooth**

Bluetooth menggunakan teknologi radio yang disebut spektrum penyebaran frekuensi-hopping, yang memotong data yang dikirim dan mentransmisikan sebagian data tersebut hingga 79 pita (masing-masing 1 MHz; berpusat dari 2402 hingga 2480 MHz) dalam rentang 2.400-2.483,5 MHz (memungkinkan untuk band penjaga). Jangkauan ini termasuk dalam pita frekuensi radio jarak pendek 2,4 GHz Industri, Ilmiah, dan Medis (ISM) yang tidak berlisensi secara global.

Awalnya modulasi penguncian frekuensi Gaussian (GFSK) adalah satu-satunya skema modulasi yang tersedia; selanjutnya, sejak diperkenalkannya Bluetooth 2.0+EDR, modulasi /4-DQPSK dan 8DPSK juga dapat digunakan di antara perangkat yang kompatibel. Perangkat yang berfungsi dengan GFSK dikatakan beroperasi dalam mode kecepatan dasar (BR) yang memungkinkan kecepatan data sesaat sebesar 1 Mbit/s. Istilah Enhanced Data Rate (EDR) digunakan untuk menggambarkan skema /4-DPSK dan 8DPSK, masing-masing memberikan 2 dan 3 Mbit/s. Kombinasi mode (BR dan EDR) ini dalam teknologi radio Bluetooth diklasifikasikan sebagai “radio BR/EDR”.

Bluetooth adalah protokol berbasis paket dengan struktur master-slave. Satu master dapat berkomunikasi dengan hingga 7 budak dalam satu piconet; semua perangkat berbagi jam master. Pertukaran paket didasarkan pada jam dasar, yang ditentukan oleh master, yang berdetak pada interval 312,5 µs. Dua detak jam membentuk slot 625 µs; dua slot membentuk sepasang slot 1250 µs. Dalam kasus sederhana paket slot tunggal, master mengirimkan di slot genap dan menerima di slot ganjil; sebaliknya, budak menerima di slot genap dan mentransmisikan di slot ganjil. Paket mungkin terdiri dari 1, 3, atau 5 slot, tetapi dalam semua kasus, transmisi master akan dimulai di slot genap dan transmisi budak di slot ganjil.

Bluetooth menyediakan cara aman untuk menghubungkan dan bertukar informasi antar perangkat seperti faks, ponsel, telepon, laptop, komputer pribadi, printer, penerima Global Positioning System (GPS), kamera digital, dan konsol video game.

**Kegunaan**

Bluetooth adalah protokol komunikasi pengganti kabel standar yang terutama dirancang untuk konsumsi daya rendah, dengan jangkauan pendek (bergantung pada kelas daya, namun rentang efektif berbeda-beda dalam praktiknya; lihat tabel di bawah) berdasarkan mikrochip transceiver berbiaya rendah di setiap perangkat. Karena perangkat menggunakan sistem komunikasi radio (siaran), perangkat tersebut tidak harus saling berhadapan secara visual, namun jalur nirkabel kuasi optik harus dapat dijalankan.

| Kelas (m) | Daya maksimum yang diizinkan (mW) | Rentang (dBm) |
|---|---|---|
| Kelas 1 | 100 | 20~100 |
| Kelas 2 | 2.5 | 4~10 |
| Kelas 3 | 1 | 0~5 |

Jangkauan efektif bervariasi tergantung pada kondisi propagasi, cakupan material, variasi sampel produksi, konfigurasi antena, dan kondisi baterai. Dalam kebanyakan kasus, jangkauan efektif perangkat kelas 2 diperluas jika terhubung ke transceiver kelas 1, dibandingkan dengan jaringan kelas 2 murni. Hal ini dicapai dengan sensitivitas dan daya transmisi yang lebih tinggi pada perangkat kelas 1.

Meskipun Spesifikasi Inti Bluetooth mewajibkan jangkauan minimum, jangkauan teknologinya spesifik untuk aplikasi dan tidak terbatas. Produsen dapat menyesuaikan penerapannya sesuai kebutuhan untuk mendukung kasus penggunaan individual.

**Ringkasan**

- Protokol Stop dan Wait paling mudah diterapkan dan terbukti paling efisien pada saluran komunikasi bebas kesalahan. Namun, saluran komunikasi bebas kesalahan praktis tidak mungkin dilakukan.
- PAR juga dapat diandalkan dan mudah diimplementasikan namun harus mengorbankan bandwidth.
- Protokol Go Back N memerlukan pemeliharaan buffer dan oleh karena itu, rumit untuk menjaga mesin sumber dan tujuan tetap sinkron. Hal ini juga dianggap paling tidak efisien karena mentransmisikan ulang seluruh frame berikutnya jika ada satu frame yang hilang dan dengan demikian menimbulkan pemborosan bandwidth yang sangat besar.
- Selective Repeat merupakan penyempurnaan dari protokol Go Back N dan mencoba untuk menggunakan bandwidth secara lebih efisien dengan mengurangi jumlah transmisi ulang karena hanya mentransmisikan ulang satu frame dibandingkan seluruh rangkaian. Dengan demikian, Pengulangan Selektif dianggap sebagai pilihan yang lebih baik.
- Model Finite State Machine adalah teknik untuk memverifikasi kebenaran protokol. PPP dan HDLC adalah protokol data link yang banyak digunakan.
- Teknologi nirkabel telah membantu menyederhanakan jaringan dengan memungkinkan beberapa pengguna komputer untuk berbagi sumber daya secara bersamaan di rumah atau bisnis tanpa kabel tambahan atau mengganggu. Sumber daya ini mungkin mencakup koneksi Internet broadband, printer jaringan, file data, dan bahkan streaming audio dan video. Pembagian sumber daya semacam ini menjadi lebih umum karena pengguna komputer telah mengubah kebiasaan mereka dari menggunakan komputer tunggal yang berdiri sendiri menjadi bekerja pada jaringan dengan banyak komputer, masing-masing dengan sistem operasi yang berbeda dan perangkat keras periferal yang berbeda-beda.
- Bluetooth adalah standar teknologi nirkabel terbuka yang dipatenkan untuk bertukar data dalam jarak pendek (menggunakan transmisi radio dengan panjang gelombang pendek pada pita ISM 2400-2480 MHz) dari perangkat tetap dan seluler, sehingga menciptakan jaringan area pribadi (PAN) dengan tingkat keamanan tinggi.

**Latihan Soal**

Isilah bagian yang kosong:

1. .....menjelaskan teknik untuk mengakses saluran komunikasi bersama dan transmisi bingkai data yang andal dalam lingkungan komunikasi komputer.
2. .....tidak termasuk pengaturan atau pelepasan koneksi apa pun dan tidak menangani pemulihan bingkai karena gangguan saluran.
3. .....mengacu pada transfer aliran bit yang andal ke lapisan jaringan di mana lapisan data link memecah aliran bit menjadi bingkai.
4. .....mengontrol ketidaksesuaian antara kecepatan pengiriman dan penerimaan data host sumber dan tujuan sehingga menyebabkan paket dijatuhkan di ujung penerima.
5. Dalam protokol stop dan wait, frame pengakuan memiliki ..... bit yang dikirim kembali oleh node tujuan ke mesin sumber.
6. Pengakuan Positif dengan Protokol Transmisi Ulang (PAR) menggunakan..... untuk menentukan apakah ada frame yang hilang atau rusak.
7. Protokol Go Back N mengatasi masalah PAR dengan memungkinkan mesin sumber memiliki lebih dari..... sekaligus dengan menggunakan buffer.

Nyatakan apakah pernyataan berikut ini benar atau salah:

- Pembukaan adalah akhir dari frame dan digunakan untuk membuat sinkronisasi bit dengan bantuan pola bolak-balik satu dan nol yang digunakan oleh penerima.
- Ethernet pertama kali dirancang dan dipasang oleh Xerox Corporation.
- Kinerja Aloha atau Slotted Aloha ditentukan dengan bantuan throughput dan penundaan rata-rata.
- Ada lima kelas frame LCP.

**Uraian**

1. Apa yang dimaksud dengan protokol tautan data?
2. Keuntungan apa yang ditawarkan oleh protokol jendela geser Selective Repeat dibandingkan protokol Go Back N?
3. Apa tujuan pengendalian aliran?
4. Jelaskan bagaimana model mesin negara terbatas melakukan verifikasi protokol.
5. Apa sajakah protokol data link yang tersedia? Mengapa PPP menjadi populer?
6. Bagaimana lapisan data link melakukan transmisi data dari lapisan jaringan sumber ke lapisan jaringan tujuan?
7. Bagaimana frame dibuat dan checksum diterapkan padanya?
8. Bagaimana lapisan data link menangani kesalahan dan kehilangan frame karena beberapa masalah perangkat keras?
9. Mengapa kode Hamming dianggap penting di antara berbagai teknik deteksi dan pemulihan kesalahan?
10. Prosedur apa yang digunakan untuk mencegah aliran data biner disalahartikan sebagai tanda HDLC?

11. Jelaskan tiga teknik dimana batas frame dapat dikodekan dalam aliran bit yang ditransmisikan. Jelaskan isian karakter dan nyatakan teknik apa yang dikaitkan dengannya dan mengapa itu diperlukan.
12. Bagaimana pipelining meningkatkan throughput protokol lapisan data link?
13. IEEE telah membagi lapisan data link di LAN seperti Ethernet dan Token ring menjadi dua sub lapisan. Lapisan manakah yang berhubungan dengan deteksi kesalahan?
14. Bagaimana PPP mengirimkan datagram melalui link serial point-to-point?
15. Bagaimana cara PPP membuat tautan untuk transfer file yang diautentikasi?
16. Apa saja metode autentikasi yang diterapkan dalam teknik PPP?
17. Bagaimana cara menghindari tabrakan di jaringan CSMA/CD?
18. Bandingkan dan kontraskan metode akses CSMA/CD dan token passing.
19. Apakah Slotted Aloha selalu lebih baik dari Aloha? Jelaskan jawaban Anda dengan pembenaran.
20. Apa saja komponen dasar yang membentuk Ethernet?
21. Atas dasar apa versi Ethernet ditentukan? Daftarkan mereka.
22. Berapa frekuensi dan kecepatan data berbeda yang tersedia untuk LAN nirkabel?
23. Teknologi apa saja yang tersedia untuk LAN Nirkabel?

# BAB 9
# LAPISAN JARINGAN

**Pendahuluan**

Lapisan jaringan menangani penerusan paket dari node sumber ke node tujuan menggunakan rute yang berbeda. Oleh karena itu, lapisan jaringan mengangkut lalu lintas antar perangkat yang tidak terhubung secara lokal. Dengan melakukan hal ini, ia mengontrol pengoperasian subnet, yang melibatkan perutean paket dari sumber ke tujuan. Rute didasarkan pada tabel routing statis atau dinamis. Alamat IP tujuan diperiksa untuk paket yang diterima pada antarmuka router. Jika paket tidak dialamatkan ke router tempat paket diterima, router akan mencari alamat jaringan tujuan di tabel perutean sehingga dapat dirutekan sesuai tujuan.

Oleh karena itu, lapisan jaringan harus mengetahui topologi subnet komunikasi dan memilih jalur yang sesuai melaluinya. Rute dipilih sedemikian rupa sehingga lapisan jaringan menghindari kelebihan beban pada beberapa jalur komunikasi dan membiarkan jalur lainnya menganggur. Algoritma perutean adalah bagian dari lapisan jaringan. Algoritma perutean memungkinkan lapisan jaringan untuk memutuskan ke jalur keluaran mana paket masuk harus diteruskan. Algoritme perutean memberikan kebenaran, kesederhanaan, ketahanan, stabilitas, keadilan, dan optimalitas. Semua fungsi lapisan jaringan ini berbeda dari lapisan data link yang tujuannya adalah untuk mengirimkan bit dari satu ujung kabel ke ujung lainnya. Lapisan Jaringan adalah lapisan terendah yang berhubungan dengan transmisi end-to-end.

## 9.1 MASALAH DESAIN LAPISAN JARINGAN

Permasalahan perancangan lapisan jaringan mencakup layanan yang diberikan pada lapisan transport, perutean paket melalui subnet, pengendalian kongesti, dan koneksi beberapa jaringan secara bersamaan, dll. Permasalahan perancangan lapisan jaringan diberikan seperti di bawah ini:

- Tujuan dari lapisan jaringan adalah untuk memberikan layanan yang lancar kepada pengguna berbeda yang terhubung ke jaringan berbeda, oleh karena itu, layanan yang diberikan harus independen dari teknologi yang mendasarinya. Dengan kata lain, pengguna yang memanfaatkan layanan ini tidak perlu repot dengan implementasi fisik jaringan untuk mengirimkan pesan mereka. Ia harus mampu memberikan interoperabilitas antar berbagai jaringan yang beroperasi dan disediakan oleh vendor yang berbeda. Oleh karena itu, desain lapisan tidak boleh membatasi penggunaan koneksi ke jaringan dengan teknologi berbeda.
- Lapisan transport pada mesin host tidak perlu mengetahui bagaimana hubungan komunikasi dengan mesin tujuan dibuat. Oleh karena itu, ia harus dilindungi dari jumlah, jenis dan topologi berbeda dari subnet yang digunakannya.
- Harus ada skema pengalamatan yang seragam untuk alamat jaringan.

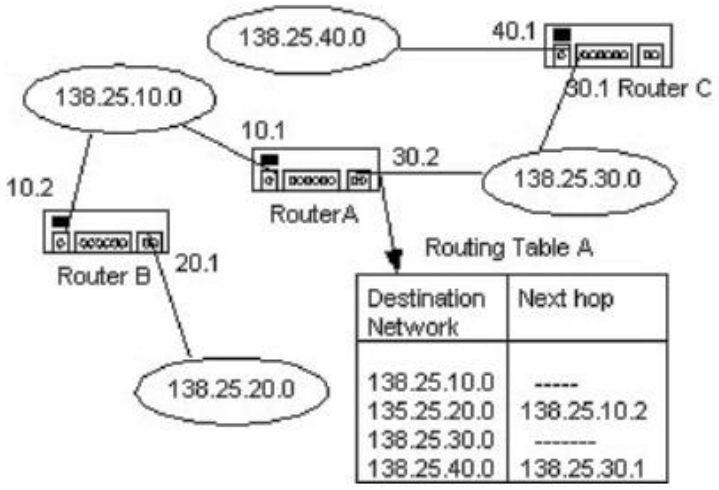
Ada dua jenis tautan komunikasi. Mereka berorientasi pada koneksi dan tidak memiliki koneksi.

- **Layanan Berorientasi Koneksi**: Dalam layanan berorientasi koneksi, setiap paket dikaitkan dengan koneksi sumber/tujuan. Paket-paket ini dirutekan sepanjang jalur yang sama, yang dikenal sebagai sirkuit virtual. Dengan demikian, ia menyediakan koneksi end-to-end kepada pengguna untuk transfer data yang andal. Ini mengirimkan data secara berurutan tanpa duplikasi atau data yang hilang dan oleh karena itu, tidak membuat saluran komunikasi dan buffer mesin penerima menjadi padat. Mesin host meminta koneksi untuk berkomunikasi dan menutup koneksi setelah transmisi data. Komunikasi telepon adalah contoh layanan berorientasi koneksi. Dalam layanan berorientasi koneksi, pengguna menggunakan bandwidth dan sumber daya lain dari jaringan selama durasi koneksi dan oleh karena itu terikat untuk membayar lebih. Layanan ini juga menjaga sumber daya jaringan tetap aktif meskipun tidak ada komunikasi selama koneksi. Ditemukan efisien untuk mengirimkan aliran data yang konstan. Jika pengguna hanya ingin mengirim satu atau dua paket data, maka biaya pengaturan koneksi akan sangat tinggi dan seringkali saluran akan tetap menganggur dan membuang bandwidth serta sumber daya jaringan. Rupanya, layanan berorientasi koneksi berguna ketika pengguna memiliki aliran data yang konstan untuk dikirimkan.
- **Layanan Tanpa Koneksi**: Dalam layanan tanpa koneksi, router memperlakukan setiap paket secara individual. Paket-paket tersebut dirutekan melalui jalur yang berbeda melalui jaringan sesuai dengan keputusan yang dibuat oleh router. Dalam layanan connectionless, jaringan atau saluran komunikasi tidak menjamin pengiriman data dari mesin host ke mesin tujuan. Data yang akan dikirim dipecah menjadi paket-paket. Paket independen ini disebut datagram, mirip dengan telegram. Paket-paket tersebut berisi alamat mesin tujuan. Layanan tanpa koneksi setara dengan sistem pos. Dalam sistem pos, surat dimasukkan ke dalam amplop yang berisi alamat tujuan. Kemudian dimasukkan ke dalam kotak surat. Surat itu akhirnya sampai di tempat tujuan melalui jaringan pos. Namun, tidak menjamin sampai di kotak surat penerima. Demikian pula, dalam layanan connectionless, paket data yang berisi alamat dikirimkan dengan harapan akhirnya sampai ke tujuan setelah dipantulkan maju mundur dalam jaringan komunikasi. Layanan connectionless dibandingkan dengan layanan berorientasi koneksi tampaknya menawarkan kelemahan dalam hal pengiriman data yang tidak dapat diandalkan namun kemungkinan hilangnya paket cukup rendah. Banyak aplikasi memiliki mekanisme deteksi kesalahan, aliran dan kontrol kemacetannya sendiri pada tingkat lapisan yang lebih tinggi dalam tumpukan protokol, yaitu lapisan transport di mesin host atau tujuan atau di kedua ujungnya.

## 9.2 PERUTEAN

Algoritme perutean yang berjalan pada lapisan jaringan memutuskan pada jalur keluaran mana paket masuk harus dikirim. Tabel routing yang dibangun di setiap router memberitahukan jalur keluar mana yang harus digunakan untuk setiap router tujuan yang mungkin. Router mencari jalur komunikasi keluar untuk digunakan dalam tabel routing setelah menerima datagram yang berisi alamat tujuan. Setelah itu, ia mengirimkan paket dalam

perjalanannya ke tujuan. Dengan demikian, peran utama lapisan jaringan adalah merutekan paket dari mesin sumber ke mesin tujuan. Algoritme yang memungkinkan untuk memilih kemungkinan rute dan struktur data yang digunakan adalah area utama dari algoritma perutean. Properti yang diinginkan dari algoritma routing adalah kebenaran, kesederhanaan, ketahanan, stabilitas, keadilan dan optimalitas.




**Gambar 9.1 Tabel routing**

Oleh karena itu, algoritma perutean didefinisikan sebagai bagian dari perangkat lunak lapisan jaringan yang memutuskan pada saluran keluaran mana paket masuk harus dikirim. Itu semua tergantung pada apakah subnet menggunakan datagram secara internal, keputusan ini dibuat baru untuk setiap paket data yang datang karena rute terbaik mungkin telah berubah sejak terakhir kali. Jika subnet menggunakan sirkuit virtual, keputusan tersebut dibuat per sesi.

Gambar 9.1 menunjukkan tabel routing untuk router A (alamat 138.25.10.1). Tabel ini mencantumkan alamat tujuan untuk setiap jaringan lokal, dan bukan untuk setiap host tujuan. Tabel ini juga mencakup hop berikutnya (alamat router berikutnya) ke mana paket harus ditransfer. Jika tidak ada hop yang disertakan, ini berarti jaringan tujuan terhubung langsung ke router. Ketika router A menerima paket, ia melacak tabel ini untuk melakukan routing. Misalnya jika paket dialamatkan ke host jaringan 138.25.40.0, maka router A mengirimkan paket tersebut ke router C (138.25.30.1). Router C memiliki tabel routing yang serupa sehingga dapat melakukan routing.

**Perutean Memainkan Peran Utama Dalam Fungsi Penerusan**

- **Perutean hop berikutnya**: Router digunakan untuk menentukan rute datagram berdasarkan tabel perutean internalnya. Tabel berisi entri yang menunjukkan datagram router mana yang harus dikirim untuk mencapai jaringan tertentu. Router menerima datagram dari sumber yang berbeda. Peran router untuk memeriksa alamat IP tujuan dan menentukan hop berikutnya akan lebih dekat dengan tujuan akhirnya ke mana datagram harus dikirim. Untuk menentukan hop berikutnya, router memelihara sekumpulan informasi untuk memungkinkan pemetaan antara ID jaringan yang

berbeda dan router lain yang terhubung. Informasi ini terkandung dalam struktur data yang dikenal sebagai tabel routing. Entri dalam tabel perutean memudahkan rincian subjaringan atau host. Jadi, ketika router menerima datagram, ia memeriksa alamat IP tujuan datagram terhadap entri routing dalam tabelnya untuk menentukan ke mana harus mengirim datagram, dan kemudian mengirimkannya pada hop berikutnya. Hop berikutnya adalah teknik yang memungkinkan router mengambil keputusan cepat tentang apa yang harus dilakukan dengan datagram karena semakin sedikit entri dalam tabel ini. Perutean antar domain tanpa kelas (CIDR) mengumpulkan rute ke supernet untuk mengurangi ukuran tabel router. Singkatnya routing hop berikutnya adalah teknik untuk mengurangi isi tabel routing, yang menyimpan informasi yang mengarah ke hop berikutnya alih-alih menyimpan informasi tentang rute lengkap.

- **Perutean khusus jaringan**: Perutean khusus jaringan juga merupakan teknik untuk mengurangi tabel perutean dan menyederhanakan proses pencarian. Sesuai dengan namanya, teknik ini memungkinkan satu entri saja untuk menentukan alamat jaringan itu sendiri yang terhubung dengan banyak host. Dengan demikian, perutean khusus jaringan tidak melibatkan entri untuk setiap host yang terhubung ke jaringan fisik yang sama dan memperlakukan semua host yang terhubung ke jaringan yang sama sebagai satu entitas tunggal. Misalnya, jika ada 500 host yang terhubung ke jaringan yang sama, hanya ada satu entri di tabel perutean, bukan 500 entri.
- **Perutean khusus host**: Ini dianggap kebalikan dari perutean khusus jaringan di mana setiap alamat host tujuan diberikan dalam tabel perutean. Oleh karena itu, ini tidak secepat hop berikutnya dan perutean khusus jaringan, namun administrator jaringan memiliki kendali lebih besar terhadap perutean.
- **Perutean default**: Ini adalah teknik lain untuk menyederhanakan perutean di mana sebuah host terhubung ke dua router dalam suatu jaringan. Satu router digunakan untuk merutekan paket ke host yang terhubung ke jaringan lain dan untuk sisa Internet, router lain digunakan.

Routing dikelompokkan menjadi dua kelas. Mereka adalah algoritma non-adaptif dan adaptif.

Algoritme non-adaptif atau perutean statis tidak bergantung pada volume lalu lintas dan topologi saat ini. Mereka memutuskan rute pengiriman datagram secara offline. Rute dihitung terlebih dahulu dan diunduh ke router saat jaringan di-boot. Dengan demikian, informasi perutean ditentukan secara manual. Ini memberikan informasi rute tetap ke setiap router. Jika tidak ada perubahan rute maka dilakukan secara manual. Prosedur ini juga disebut routing statis.

Algoritme adaptif atau perutean dinamis mampu mengubah keputusan peruteannya untuk mencerminkan perubahan topologi dan lalu lintas. Router secara otomatis memperbarui informasi perutean ketika ada perubahan pada konfigurasi jaringan. Ini nyaman karena tidak melibatkan campur tangan manusia jika terjadi perubahan pada konfigurasi jaringan. Namun kelemahannya adalah biaya overhead yang diperlukan untuk mengirim informasi perubahan konfigurasi dapat menjadi beban yang berat. Mereka juga dikenal

sebagai perutean dinamis. Untuk memperbarui informasi dalam tabel perutean, ia menggunakan salah satu protokol perutean dinamis seperti OSPF atau BGP atau lain-lain.

**Tabel Perutean**

Setiap router di jaringan memelihara tabel routing di memori yang mungkin sederhana atau kompleks. Dalam bentuk yang paling sederhana, tabel ini terdiri dari pasangan alamat IP. Ketika stasiun asal menyimpulkan bahwa tujuan yang dituju dapat dijangkau secara langsung, frame dikirim langsung ke alamat IP tujuan dalam frame. Namun, mungkin tidak perlu mengirimkannya ke router jika pengirim mengetahui bahwa ia berada di subjaringan yang sama dengan tujuan. Ketika alamat tujuan yang disamarkan dibandingkan dengan entri yang tersedia dalam tabel dan ditemukan bahwa tabel perutean tidak memiliki nilai pencarian yang cocok. Dalam situasi seperti ini, alamat khusus muncul di tabel routing yang disebut Alamat Gateway Default. Keputusan perutean didasarkan pada poin-poin berikut:

1. Alamat IP tujuan dan IP router disamarkan untuk menentukan apakah paket masuk akan diteruskan ke jaringan lain atau tidak. Jika hasilnya sama, berarti paket tersebut berada pada subnet yang sama dengan tujuan. Frame tersebut kemudian diteruskan langsung ke alamat data link tujuan.
2. Bila hasilnya tidak sama, berarti tujuannya tidak berada pada subnet yang sama. Tabel perutean diperiksa untuk mengetahui apakah alamat tujuan 32-bit yang tepat, lengkap, ditentukan yang disebut sebagai perutean khusus host. Jika rute spesifik host ditentukan, frame ditransmisikan ke tujuan IP yang ditunjukkan dalam tabel yang menyiratkan bahwa tujuan ini adalah router berikutnya dalam jalur menuju tujuan.
3. Ketika rute spesifik host tidak ditemukan dalam tabel perutean, maka alamat bertopeng digunakan untuk mencari kunci dalam tabel perutean untuk memeriksa apakah jaringan/subjaringan ditentukan dalam tabel. Jika ditentukan, frame dikirim ke alamat IP yang ditentukan dalam tabel yang menyiratkan bahwa ini adalah alamat IP router berikutnya.
4. Ketika kondisi 2 dan 3 yang diberikan di atas gagal, frame diteruskan ke alamat yang ditentukan sebagai target untuk Default Gateway.
5. Dalam situasi ketika tidak ada gateway default yang ditentukan, diasumsikan bahwa semua tujuan yang tidak ditentukan dapat dijangkau secara langsung. Alamat fisik stasiun IP tujuan diselesaikan dan frame diteruskan langsung ke tujuan. Ini terkadang disebut sebagai mengaktifkan Proxy ARP.

Jelas dari penjelasan di atas bahwa tabel perutean memerlukan setidaknya empat entri seperti mask, alamat tujuan, alamat hop berikutnya, dan antarmuka.

## 9.3 PROTOKOL PERUTEAN

Router digunakan untuk menghubungkan jaringan yang berbeda, menentukan jalur mana yang harus diambil dan meneruskan lalu lintas IP. Informasi ini diperoleh di router dengan melakukan pemrosesan per paket di mana header IP paket diperiksa untuk membuat keputusan perutean berdasarkan alamat IP tujuan dan kondisi konektivitas jaringan saat ini. Konektivitas jaringan dan informasi perutean terus dipelihara oleh router untuk meneruskan

paket secara akurat. Paket tersebut akhirnya melewati banyak router sebelum mencapai tujuan. Tabel routing di setiap router dalam cara paket mencapai tujuan indentasinya menentukan jalur optimal untuk paket tersebut. Prinsip optimalitas mendefinisikan bahwa jika router A berada pada jalur optimal dari router B ke router C, maka jalur optimal dari A ke C juga berada pada rute yang sama.

Akibatnya, himpunan rute optimal dari semua sumber ke suatu tujuan tertentu membentuk pohon yang berakar di tujuan tersebut. Pohon seperti ini disebut pohon tenggelam. Tabel perutean dapat bersifat statis atau dinamis. Tabel statis tidak sering berubah sementara tabel dinamis sering diperbarui setiap kali beberapa perubahan di Internet diumumkan seperti kegagalan beberapa rute atau penambahan rute yang lebih baik. Protokol perutean digunakan untuk tabel perutean dinamis. Mereka didasarkan pada kombinasi aturan dan prosedur yang memungkinkan router untuk saling menginformasikan tentang perubahan di Internet dan berbagi informasi tentang Internet atau lingkungan mereka.

**Perutean Unicast**

Mayoritas alamat IP adalah alamat unicast yang ditujukan untuk satu penerima. Koneksi unicast adalah koneksi satu-ke-satu. Protokol tanpa koneksi dan berorientasi koneksi dapat menggunakan alamat unicast terlepas dari apakah ada koneksi antara sepasang host tertentu. Dalam perutean unicast, router meneruskan paket masuk melalui salah satu portnya seperti yang ditentukan dalam tabel perutean. Sebuah router yang terhubung ke beberapa jaringan harus menentukan jalur optimal untuk suatu paket sehingga router memilih rute dengan metrik terpendek. Metrik didefinisikan sebagai biaya yang ditetapkan untuk melewati jaringan. Metrik total untuk rute tertentu adalah jumlah metrik jaringan yang membangun rute tersebut. Metrik yang ditetapkan untuk setiap jaringan bergantung pada protokol yang digunakan. Satuan biaya metrik adalah jumlah hop dan protokol seperti protokol informasi perutean memberikan metrik yang sama ke setiap jaringan. Jika ia menetapkan metrik 1 hop ke setiap jaringan maka paket yang melintasi 15 jaringan akan memiliki nilai metrik sebagai jumlah 15 hop. Penetapan metrik bervariasi dari satu protokol ke protokol lainnya berdasarkan layanan yang diperlukan dari jaringan.

**Perutean Interior dan Eksterior**

Internet dibagi menjadi sistem otonom sehingga protokol perutean dapat menangani Internet secara efektif dan efisien. Sistem otonom (AS) adalah sekelompok jaringan di bawah administrasi otoritas tunggal dan oleh karena itu perutean di dalam AS disebut perutean interior, sedangkan perutean antar sistem otonom disebut perutean eksterior. Terdapat banyak protokol gateway interior standar dan eksklusif. Beberapa diantaranya adalah Routing Information Protocol (RIP) dan Open Shortest Path Fist (OSPF). Protokol luarnya adalah Border Gateway Protocol (BGP).

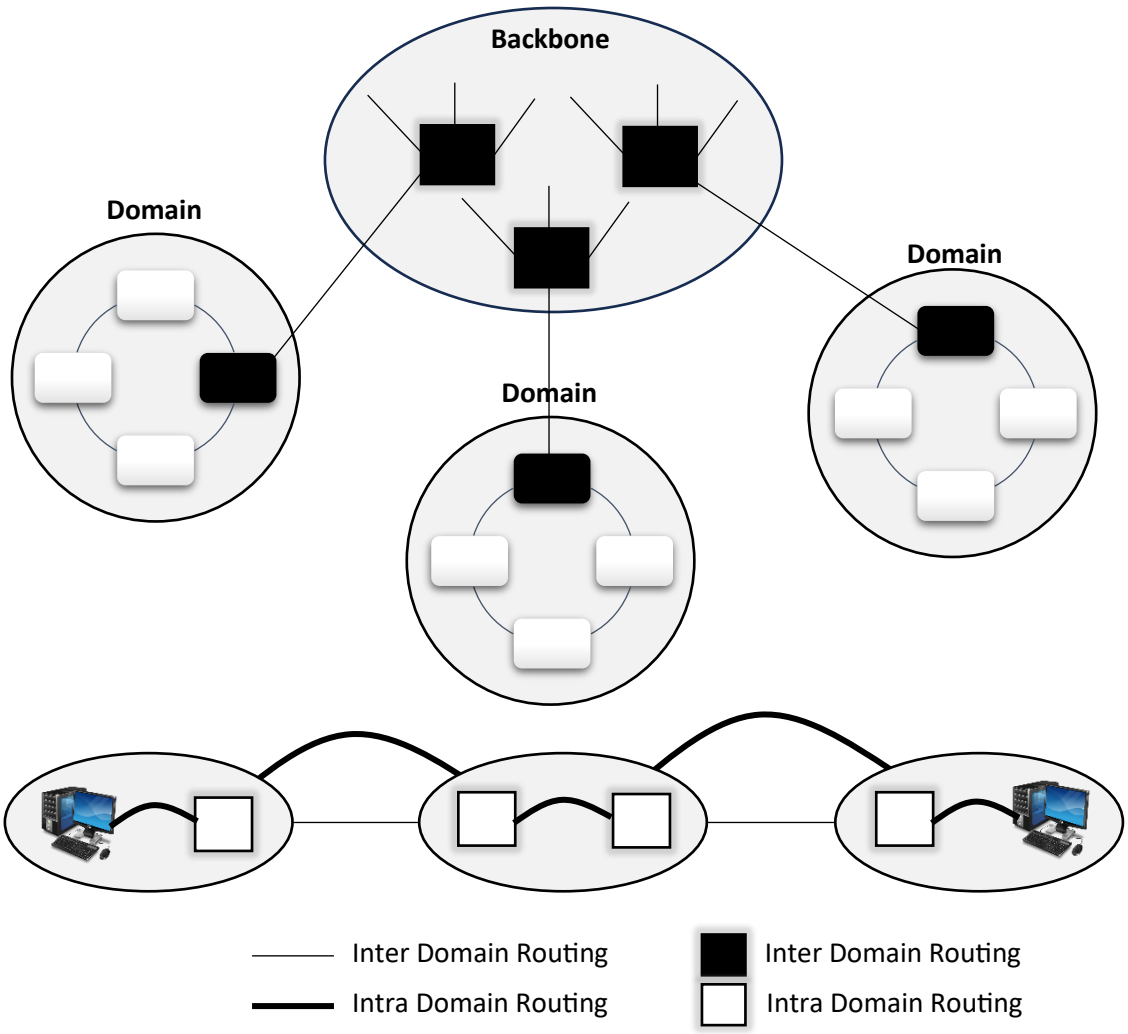
**Perutean Hierarki**

Karena sifat global dari sistem Internet dan ukuran jaringan yang terus berkembang, maka menjadi lebih sulit untuk memusatkan manajemen dan pengoperasian sistem. Oleh karena itu, sistem harus bersifat hierarkis sehingga disusun dalam beberapa tingkatan, dengan beberapa putaran grup yang terhubung satu sama lain di setiap tingkat. Router dibagi menjadi

beberapa wilayah dengan masing-masing router mengetahui semua detail tentang cara merutekan paket dalam wilayahnya sendiri tetapi tidak mengetahui apa pun tentang struktur internal wilayah lain. Oleh karena itu, perutean hierarki biasanya digunakan untuk sistem seperti yang ditunjukkan pada Gambar 9.2.

- Sekumpulan jaringan yang dihubungkan oleh router dalam area tertentu menggunakan protokol routing yang sama disebut domain.
- Dua atau lebih domain dapat digabungkan lebih lanjut untuk membentuk domain tingkat tinggi.
- Sebuah router dalam domain tertentu disebut router intra-domain. Router yang menghubungkan domain disebut router antar-domain.
- Jaringan yang terdiri dari router antar-domain disebut backbone.

Setiap domain, yang disebut juga domain operasi, merupakan titik di mana operasi sistem dibagi menjadi beberapa organisasi yang bertanggung jawab atas operasi tersebut. Domain ditentukan berdasarkan wilayah yang ditempati oleh masing-masing organisasi.




**Gambar 9.2 Hierarki Routing**

Protokol perutean dalam sistem Internet semacam itu secara garis besar dapat dibagi menjadi dua jenis:

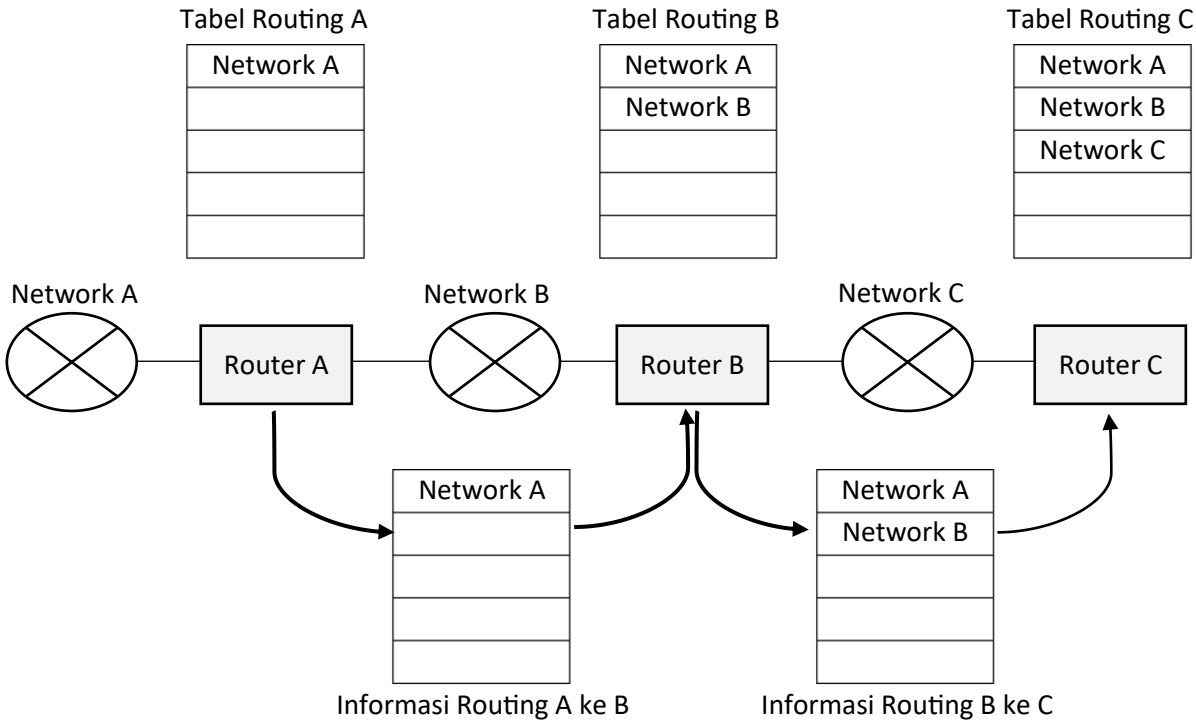
- Perutean intra-domain
- Perutean antar-domain.

Catatan Masing-masing protokol ini disusun secara hierarkis. Untuk komunikasi dalam domain, hanya perutean sebelumnya yang digunakan. Namun, keduanya digunakan untuk komunikasi antara dua domain atau lebih. Dua algoritma, Distance-Vector Protocol dan Link-State Protocol, tersedia untuk memperbarui isi tabel routing.

Ini adalah protokol sederhana berdasarkan routing vektor jarak yang menggunakan algoritma Bellman Ford untuk menghitung tabel routing.

**Perutean Vektor Jarak**

Perutean Vektor Jarak termasuk dalam kategori perutean dinamis. Jaringan komputer modern percaya pada algoritma routing dinamis dibandingkan dengan algoritma routing statis. Algoritma perutean ini bersama dengan perutean link state adalah yang paling populer. Protokol vektor jarak adalah RIP, Interior Gateway Routing Protocol (IGPR). Dalam algoritma vektor jarak, setiap router memelihara tabel routing dan menukar tabel routingnya dengan masing-masing router tetangganya sehingga tabel routing mereka diperbarui. Setiap router kemudian akan menggabungkan tabel routing yang diterima dengan tabelnya sendiri, dan kemudian mengirimkan tabel gabungan tersebut ke tetangganya. Hal ini ditunjukkan pada Gambar 9.3. Hal ini terjadi secara dinamis setelah interval waktu tetap secara default, sehingga memerlukan overhead link yang signifikan.




**Gamber 9.3 Routing Metode Jarak – Tipe Vektor**

Namun terdapat permasalahan seperti:

(1) Jika bertukar data antar router setiap 90 detik, misalnya, diperlukan waktu 90 × 10 detik agar router mendeteksi masalah di router 10 router di depan dan rute tidak dapat diubah selama periode ini.
(2) Lalu lintas meningkat karena informasi routing terus dipertukarkan.
(3) Ada batasan jumlah maksimum informasi perutean (15 untuk RIP), dan perutean tidak dapat dilakukan pada jaringan yang jumlah hopnya melebihi maksimum ini.
(4) Data biaya metrik hanya berupa jumlah lompatan, sehingga sulit untuk memilih jalur terbaik.

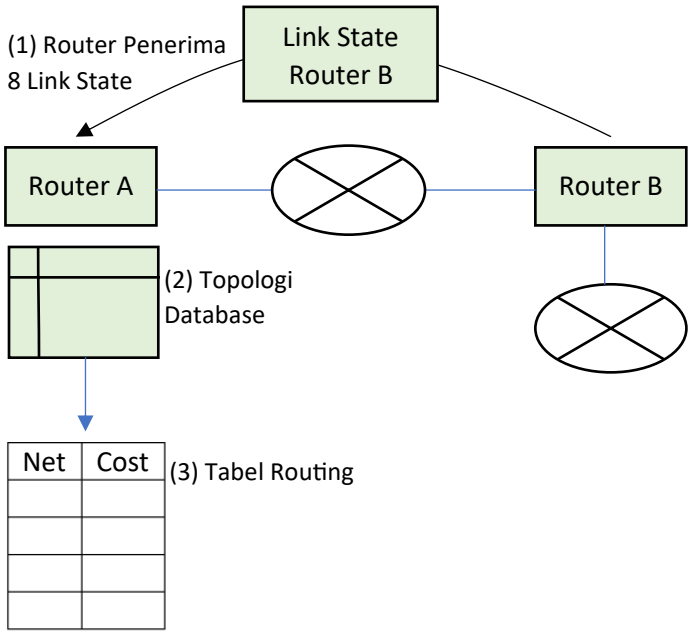
Namun, pemrosesan perutean itu sederhana, dan digunakan dalam jaringan skala kecil di mana poin-poin yang disebutkan di atas tidak menjadi masalah. Perutean vektor jarak digunakan dalam algoritma perutean ARPANET dan juga digunakan di Internet dengan nama RIP. Ia juga menemukan kegunaannya dalam versi awal DECnet dan IPX Novell.

Router AppleTalk dan CISCO menggunakan versi protokol vektor jarak yang ditingkatkan. Dalam versi yang ditingkatkan, setiap router memiliki tabel perutean yang diindeks oleh dan berisi satu entri untuk setiap router di subnet. Entri ini memiliki dua bagian. Ini adalah jalur keluar pilihan yang digunakan untuk tujuan dan perkiraan waktu atau jarak ke tujuan. Metrik yang digunakan adalah jumlah hop, waktu tunda dalam milidetik dan jumlah total paket yang antri di sepanjang jalur atau yang serupa.

**Perutean Status Tautan**

Perutean status tautan sederhana. Algoritma routing link state di mana setiap router dalam jaringan mempelajari topologi jaringan kemudian membuat tabel routing berdasarkan topologi ini. Setiap router akan mengirimkan informasi link-nya (Link-State) ke tetangganya yang pada gilirannya akan menyebarkan informasi tersebut ke tetangganya, dan seterusnya. Hal ini terjadi hingga semua router telah membangun topologi jaringan. Setiap router kemudian akan memangkas topologinya, dengan dirinya sendiri sebagai root, memilih jalur berbiaya paling rendah ke setiap router. Setelah itu, mereka membangun tabel routing berdasarkan topologi yang telah dipangkas seperti yang ditunjukkan pada Gambar 9.4.

Seluruh topologi dan penundaan diukur dan didistribusikan ke setiap router. Kemudian algoritma Dijkstra digunakan untuk mencari jalur terpendek ke setiap router lainnya. Tahukah kamu? Dalam protokol link-state, tidak ada batasan jumlah hop seperti pada protokol distance-vector, dan ini ditujukan untuk jaringan yang relatif besar seperti tulang punggung Internet. Namun beban pada router akan besar, karena pemrosesannya rumit.




**Gamber 9.4 Routing Metode Jarak – Tipe Link State**

Algoritma Dijkstra: Menghitung jalur terpendek antara dua titik di jaringan. Grafik Dijkstra terdiri dari node, lengkungan, dan node. Ini pertama-tama memilih sebuah node secara tentatif. Algoritme memeriksa node tentatif berdasarkan kriteria tertentu untuk menyatakannya sebagai node permanen. Algoritma dimulai dengan akar pohon, yang merupakan router lokal dan disebut sebagai node lokal. Node ini dinyatakan sebagai node permanen dan diberi biaya 0. Setelah itu, setiap node tetangga dari node tersebut diperiksa untuk menyatakannya sebagai node permanen terakhir. Dan simpul ini diberi biaya kumulatif. Secara singkat, perutean status tautan berkaitan dengan:

- menemukan tetangganya dan mempelajari alamat jaringan mereka,
- mengukur penundaan atau kerugian bagi masing-masing negara tetangganya,
- membangun sebuah paket yang menunjukkan semua yang baru saja dipelajarinya,
- mengirimkan paket ini ke semua router lain untuk pembelajaran dan
- menghitung jalur terpendek ke setiap router lainnya.

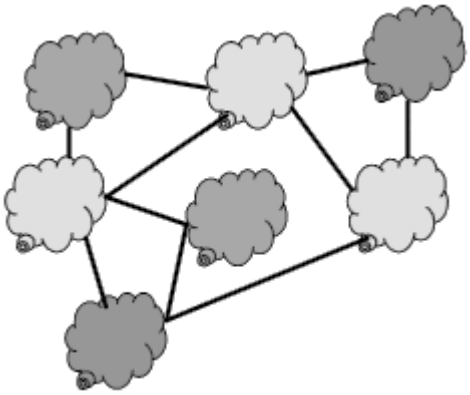
## 9.4 KERJA INTERNET

Ketersediaan sistem operasi yang berbeda, platform perangkat keras dan penyebaran sumber daya komputasi secara geografis memerlukan kebutuhan jaringan sedemikian rupa sehingga komputer dari semua ukuran dapat berkomunikasi satu sama lain, terlepas dari vendor, sistem operasi, platform perangkat keras, atau kedekatan geografis. Oleh karena itu, kita dapat mengatakan bahwa internetworking adalah skema untuk menghubungkan beberapa jaringan dengan teknologi yang berbeda. Beberapa faktor yang membuat jaringan berbeda adalah frame, paket, dan ukuran pesan, algoritma checksum, masa hidup paket maksimum, protokol berorientasi koneksi vs. tanpa koneksi, nilai timer, dll. Ketika semua router dalam jaringan memiliki protokol yang sama maka jaringan tersebut adalah disebut

homogen. Ketika jaringan-jaringan homogen ini saling berhubungan, maka akan dihasilkan sebuah internetwork.

Mungkin ada contoh, ketika router dari jaringan yang berbeda menggunakan protokol yang berbeda seperti Internet Protocol (IP), Systems Network Architecture (SNA), Asynchronous Transfer Mode (ATM), Novel NCP/IPX dan AppleTalk adalah beberapa di antaranya. Jaringan ad-hoc dan seluler nirkabel menggunakan mis. Bluetooth adalah yang lain. Oleh karena itu, untuk menghubungkan beberapa jaringan dengan teknologi yang berbeda diperlukan penggunaan perangkat keras dan perangkat lunak tambahan. Perangkat keras tambahan ini ditempatkan di antara jaringan dan perangkat lunak pada setiap komputer yang terpasang. Sistem jaringan yang saling berhubungan ini disebut internetwork atau Internet.

**Contoh Internetwork**



**Gambar 9.5 Internetworking dari Perbedaan Jaringan Homogeneus**

** Nuansa mewakili jaringan homogen dari berbagai jenis*

Untuk mengembangkan standar internetworking, Defense Advanced Research Projects Agency (DARPA) mendanai proyek penelitian. ARPAnet, sebuah proyek DARPA, memperkenalkan dunia jaringan dengan konsep rangkaian protokol seperti layering, jauh sebelum inisiatif ISO ke arah ini. DARPA melanjutkan penelitiannya untuk rangkaian protokol internetworking. Hal ini dapat dilihat pada protokol host-to-host NCP (Network Control Program) awal hingga rangkaian protokol TCP/IP, yang bentuknya sekarang sekitar tahun 1978. DARPA terkenal karena perintisnya dalam peralihan paket melalui jaringan radio dan satelit. saluran dan ARPAnet dinyatakan sebagai jaringan operasional dengan tanggung jawab pengelolaannya kepada Badan Komunikasi Pertahanan (DCA) pada tahun 1975. TCP/IP belum dikembangkan.

ARPAnet pada dasarnya adalah jaringan berdasarkan jalur sewaan yang dihubungkan oleh node switching khusus, yang dikenal sebagai Internet Message Processors (IMP). Banyak peneliti yang terlibat dalam penelitian TCP/IP pada tahun 1979. Hal ini memotivasi DARPA untuk membentuk komite informal untuk mengoordinasikan dan memandu desain protokol dan arsitektur komunikasi. Komite tersebut disebut Dewan Kontrol dan Konfigurasi Internet (ICCB).

Implementasi nyata pertama dari Internet adalah ketika DARPA mengubah mesin jaringan penelitiannya ARPAnet untuk menggunakan protokol TCP/IP baru. Setelah transisi ini,

yang dimulai pada tahun 1980 dan selesai pada tahun 1983, DARPA mewajibkan semua komputer yang ingin terhubung ke ARPAnetnya harus menggunakan TCP/IP. Militer AS mengadopsi TCP/IP sebagai protokol standar pada tahun 1983 dan merekomendasikan agar semua jaringan yang terhubung ke ARPAnet mematuhi standar baru.

Keberhasilan ARPAnet lebih dari harapan para pendirinya dan internetworking TCP/IP menjadi tersebar luas. Hasilnya, jaringan area luas (WAN) baru dibuat di AS dan terhubung ke ARPAnet menggunakan protokol TCP/IP. Pada gilirannya, jaringan lain di seluruh dunia, yang tidak harus berbasis pada protokol TCP/IP, ditambahkan ke rangkaian jaringan yang saling berhubungan. Fasilitas komputasi di seluruh Amerika Utara, Eropa, Jepang, dan belahan dunia lainnya saat ini terhubung ke Internet melalui sub-jaringan mereka sendiri, yang merupakan jaringan terbesar di dunia. Pada tahun 1990, ARPAnet dihilangkan dan Internet dinyatakan sebagai jaringan global formal.

DARPA juga mendanai proyek untuk mengembangkan protokol TCP/IP untuk Berkeley UNIX di VAX dan mendistribusikan kode yang dikembangkan secara gratis dengan sistem operasi UNIX mereka. Rilis pertama dari Berkeley Software Distribution (BSD) yang menyertakan kumpulan protokol TCP/IP tersedia pada tahun 1983 (4.2BSD). Hal ini menyebabkan penyebaran TCP/IP di antara universitas dan pusat penelitian dan telah menjadi subsistem komunikasi standar untuk semua konektivitas UNIX. Ada banyak versi terbaru kode BSD yang tersedia. Ini adalah 4.3BSD (1986), 4.3BSD Tahoe (1988), 4.3BSD Reno (1990) dan 4.4BSD (1993).

**Ringkasan**

- Peran utama lapisan jaringan adalah menerima paket dari sumber dan mengirimkannya ke mesin tujuan. Lapisan jaringan menyediakan layanan yang independen terhadap teknologi router. Ini melindungi lapisan transport dari detail jaringan router dan memfasilitasi pengalamatan jaringan agar konsisten di seluruh jaringan.
- Layanan lapisan jaringan tersedia dalam mode berorientasi koneksi dan tanpa koneksi. Layanan berorientasi koneksi hanya berguna ketika pengguna ingin mengirimkan aliran data yang konstan.
- Algoritme perutean yang memerlukan pemilihan jalur atau rute dari banyak kemungkinan rute dalam jaringan adalah bagian dari perangkat lunak router. Mereka terdiri dari dua tipe dasar yaitu non-adaptif atau statis dan dinamis atau adaptif. Pemilihan algoritma routing tergantung pada rata-rata penundaan minimum untuk paket dan jumlah hop sebelum mencapai mesin tujuan.
- Link State Routing berupaya menemukan tetangganya dan mempelajari alamat jaringannya serta memungkinkan router memilih jalur terpendek. Perutean hierarki menggunakan beberapa grup untuk merutekan paket. Perutean siaran dan multicast digunakan untuk meneruskan satu paket ke beberapa penerima tergantung pada apakah mereka termasuk dalam grup siaran atau multicast.

- Jalur terpendek ke setiap tujuan dalam jaringan ditemukan dengan melintasi pohon dan algoritma jalur terpendek pertama yang paling umum adalah algoritma Dijkstra.
- Algoritme vektor jarak digunakan untuk menentukan jalur mana yang merupakan jalur terbaik ke setiap tujuan berdasarkan rincian yang diiklankan tentang jalur dan jarak untuk setiap tujuan yang disimpan dalam database lokal.

**Latihan Soal**

Nyatakan apakah pernyataan berikut ini benar atau salah:

1. Algoritme perutean memungkinkan lapisan jaringan memutuskan ke jalur keluaran mana paket masuk harus diteruskan.
2. Ada tiga jenis hubungan komunikasi.
3. Layanan berorientasi koneksi berguna ketika pengguna memiliki aliran data yang konstan untuk dikirimkan.
4. Layanan berorientasi koneksi setara dengan sistem pos.
5. Dalam layanan berorientasi koneksi, paket-paket dirutekan sepanjang jalur yang sama, yang dikenal sebagai sirkuit virtual.

**Isilah bagian yang kosong:**

1. Routing Vektor Jarak termasuk dalam kategori ..... routing.
2. Algoritma Dijkstra digunakan untuk mencari..... jalur ke setiap router lainnya.
3. .....protokol sederhana berdasarkan routing vektor jarak yang menggunakan algoritma Bellman Ford.
4. Protokol perutean dalam sistem Internet seperti itu secara garis besar dapat dibagi menjadi...jenis.
5. Perutean di dalam AS disebut sebagai..... perutean.

**Uraian**

1. Diskusikan peran lapisan jaringan dalam model OSI.
2. Apa isu utama yang menjadi perhatian dalam desain lapisan jaringan?
3. Jelaskan secara singkat cara kerja algoritma hierarki.
4. Apa tujuan utama penggunaan router dalam suatu jaringan?
5. Bedakan antara:
   (a) Layanan tanpa koneksi dan berorientasi koneksi
   (b) Perutean Interior dan Eksterior
   (c) Perutean status tautan dan vektor jarak

# BAB 10
# LAPISAN JARINGAN DI INTERNET

**Pendahuluan**

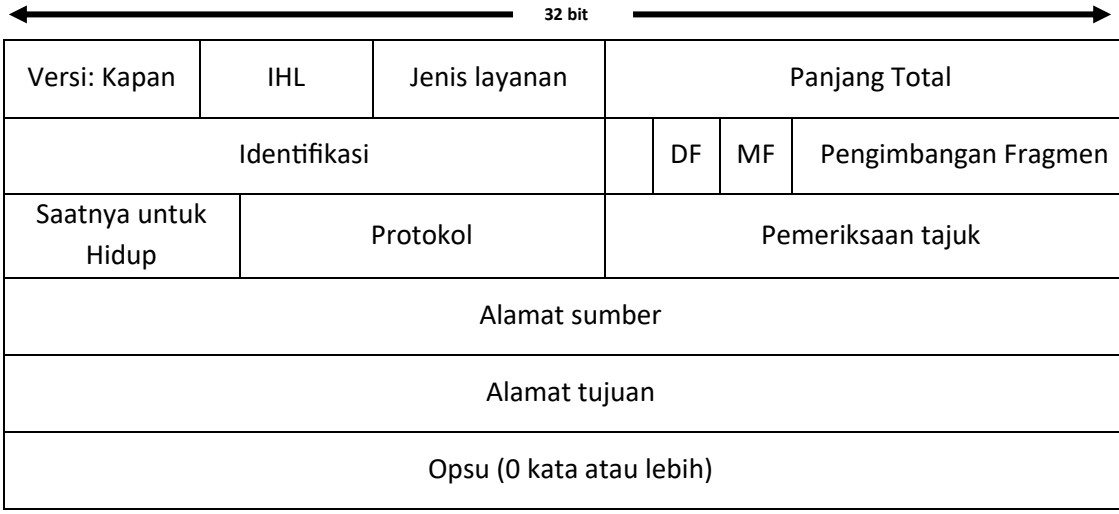
Internet dianggap sebagai interkoneksi subnet atau sistem otonom. Mereka beroperasi pada lapisan jaringan. Untuk memfasilitasi subnet ini agar terhubung secara virtual satu sama lain untuk mentransfer paket dari mesin sumber ke mesin tujuan, terdapat beberapa tulang punggung dengan bandwidth tinggi dan router cepat. Ada juga beberapa jaringan tingkat menengah yang terpasang pada tulang punggung berkecepatan tinggi. Terlampir pada jaringan tingkat menengah ini adalah LAN universitas, perusahaan, penyedia layanan internet, dll.

Perekat yang mengikat Internet adalah IP (Internet Protocol) dari lapisan jaringan. Ini memberikan upaya terbaik untuk mengangkut datagram dari mesin sumber ke mesin tujuan tanpa mempertimbangkan apakah mesin ini berada di jaringan yang sama atau tidak. Langkah-langkah yang terlibat dalam komunikasi di Internet diberikan di bawah ini:

- Lapisan transport tepat di atas lapisan jaringan memecah aliran data menjadi datagram. Besar kecilnya ukuran datagram bisa sampai 64 KB namun praktisnya sekitar 1500 byte sehingga bisa masuk ke dalam frame Ethernet. Setiap datagram atau fragmen adalah sebuah paket.
- Setiap datagram ditransmisikan melalui Internet. Datagram besar tidak terfragmentasi secara transparan, bila diperlukan, menjadi unit-unit yang lebih kecil.
- Ketika semua bagian mencapai mesin tujuan, mereka disusun kembali oleh lapisan jaringan menjadi datagram asli.
- Datagram yang telah disusun kembali diserahkan ke lapisan transport, yang memasukkannya ke dalam aliran data input proses penerimaan.
- IP adalah protokol connectionless yang tidak dapat diandalkan.

## 10.1 PROTOKOL IP

Berbeda dengan TCP, ini adalah layanan tipe connectionless dan beroperasi pada lapisan ketiga model referensi OSI. Artinya, sebelum transmisi data, tidak diperlukan koneksi logis. Jenis protokol ini cocok untuk transmisi data secara sporadis ke sejumlah tujuan. Ini tidak memiliki fungsi seperti kontrol urutan, pemulihan dan kontrol kesalahan, kontrol aliran tetapi mengidentifikasi koneksi dengan nomor port. Datagram IP memiliki header berukuran tetap 20 byte dan teks dengan panjang variabel bagian opsional. Format header datagram IP digambarkan pada Gambar 10.1. Format header dikirimkan dari kiri ke kanan, dengan bit urutan tinggi bidang Versi dikirimkan terlebih dahulu.




**Gambar 10.1 Header IP (internet Protocol)**

Enkapsulasi data menambahkan header IP ke data. Header IP terdiri dari lima atau enam kata 32-bit; kata keenam dikaitkan dengan bidang opsi IP. Berbagai bidang header IP diberikan seperti di bawah ini:

- Versi mengacu pada versi protokol IP yang digunakan dan melacak versi protokol milik datagram. Versi IP saat ini adalah 4.
- Panjang Header Internet (IHL) menunjukkan panjang bidang header dalam kata 32-bit. Nilai minimum bidang header adalah 5 yang berlaku ketika tidak ada opsi. Nilai maksimum dari 4 bit yang diajukan adalah 15 yang membatasi header menjadi 60 byte dan dengan demikian bidang Opsi menjadi 40 byte.
- Jenis layanan memungkinkan host untuk menunjukkan subnet jenis layanan apa (misalnya keandalan dan kecepatan) yang diinginkannya. Ini mengacu pada semua jenis layanan yang didukung IP. Jenis layanan yang diinginkan biasanya ditentukan oleh aplikasi tingkat pengguna. Contoh jenis layanan mencakup throughput minimum dan maksimum, yang diminta oleh aplikasi seperti File Transfer Protocol (FTP) dan Simple Mail Transfer Protocol (SMTP).
- Panjang total semua yang ada di datagram (maks. 64 KB). Jika dikurangi dari bidang IHL, ini menunjukkan ke IP panjang sebenarnya dari bidang data.
- Identifikasi memungkinkan host tujuan untuk menentukan datagram mana yang menjadi milik fragmen yang baru tiba:
- DF artinya Jangan Pecah-pecah.
- MF untuk Lebih Banyak Fragmen.
- Fragmen offset menunjukkan lokasi sumber datagram saat ini. Ukuran unit fragmen dasar adalah 8 byte.
- Waktu untuk hidup yang menghitung lompatan dinyatakan dalam hitungan detik. Hitungan nol menunjukkan bahwa paket tersebut dibuang. TTL digunakan oleh IP untuk mencegah datagram yang hilang terus berputar di sekitar jaringan. IP mencapai tujuan ini dengan menginisialisasi bidang TTL ke jumlah maksimum router yang dapat

dilintasi paket di jaringan. Setiap kali datagram melintasi router, IP mengurangi field TTL sebesar 1.

- ☞ Protokol menunjukkan tujuan yang mengangkut proses untuk memberikan datagram (TCP, UDP, atau lainnya).
- ☞ Header checksum memverifikasi header saja. Algoritmenya adalah menjumlahkan semua setengah kata 16-bit yang ada, menggunakan aritmatika komplemen.
- ☞ Alamat Sumber/Tujuan memberitahukan nomor jaringan dan nomor host.
- ☞ Opsi memberikan jalan keluar untuk memungkinkan versi protokol berikutnya memiliki informasi yang tidak ada dalam desain aslinya, untuk memungkinkan peneliti mencoba ide-ide baru, dan untuk menghindari pengalokasian bit header ke informasi yang jarang diperlukan. Pada kehadirannya, ini mencakup informasi kontrol opsional. Contoh informasi opsional mencakup catatan rute, yang mencakup catatan setiap router yang dilalui datagram selama perjalanannya mengelilingi jaringan.

**Alamat IP**

Menggunakan Internet sudah menjadi hal biasa. Sekarang kita akan memahami bagaimana Internet menafsirkan alamat Internet. Alamat Internetnya ditulis sebagai www.hotmail.com, misalnya kita menulis satu alamat lagi sebagai server.institusi.domain. Alamat www.hotmail.com bukan alamat sebenarnya; ini adalah versi teks dari alamat Internet, yang pada dasarnya merupakan representasi biner. Sekarang kita bandingkan www.hotmail.com, dan server.insstitution.domain. WWW adalah nama server yang dimiliki oleh institusi (dalam hal ini adalah hotmail) dan server ini terhubung ke Internet ke server domain yaitu (com dalam hal ini) yang memelihara database alamat server yang berbeda menggunakan domain yang sama com. Nama domain tidak memiliki relevansi geografis dan dua situs dengan nama domain yang sama mungkin ada di dua ujung dunia ini.

Kasus di atas merupakan kasus yang paling sederhana. Dalam contoh lain, suatu organisasi mungkin cukup besar dan memiliki beberapa server lain untuk tujuan berbeda seperti server web, server email, server cetak, dll. Misalkan kita sekarang mengambil contoh www.sun.planet.universe.in. Alamat ini memiliki lima bagian yang dipisahkan oleh tiga titik. Jika kita mencoba memahami alamat ini, alamat ini akan menunjukkan bahwa grup Planet (planet) berada di bawah sub domain Semesta yang merupakan bagian dari domain India dan memelihara satu server dari banyak server, yang terhubung ke Internet melalui webnya. server. Demikian pula organisasi mana pun dengan beberapa departemen dapat membuat alamat untuk subdomainnya dengan server berbeda yang dikelola di sana.

Internet adalah kumpulan beberapa jaringan independen, yang saling berhubungan satu sama lain. Sekarang setiap jaringan independen mungkin memiliki beberapa host. Dengan mengingat hal ini, kini Anda dapat memikirkan alamat rumah Anda. Rumah Anda memiliki nomor rumah unik, yang tidak diberikan ke rumah lain mana pun di wilayah Anda. Dalam hal ini, rumah Anda dapat dianggap sebagai tuan rumah. Lokalitas Anda dapat dianggap sebagai jaringan dan kota Anda sebagai domain. Anda dapat menulis alamat Anda di notasi pengalamatan Internet sebagai houseno.locality.city. Jika Anda ingin memberitahukan alamat Anda kepada orang asing, maka Anda harus menambahkan nama negara Anda di alamat Anda.

Dalam hal ini akan menjadi houseno.locality.city.country. Sekarang, jika ada orang yang ingin mengirimkan surat atau mengunjungi rumah Anda, pertama-tama dia harus datang ke negara Anda dan kemudian ke kota Anda. Setelah itu dia akan menghubungi lokasi Anda dan kemudian rumah Anda dengan nomor rumah Anda. Analogi yang sama berlaku dalam hal pengalamatan Internet.

Kita telah mencatat bahwa host di Internet memiliki dua bagian. Ini adalah identifikasi jaringan dan identifikasi host pada jaringan. Dengan cara ini, alamat host terdiri dari dua bagian yaitu alamat jaringan dan alamat host. Kedua bagian ini bersama-sama membuat alamat IP sepanjang 32 bit untuk host tertentu di Internet. Alamat IP yang akan kita lihat pada pembahasan selanjutnya ditulis dalam empat oktet yang masing-masing dipisahkan oleh sebuah titik. Ini mungkin memiliki bentuk seperti 197.23.207.10.

**Pengalamatan IPv4**

Alamat IPv4 secara unik digunakan sebagai pengidentifikasi, yang bekerja pada lapisan jaringan untuk mengidentifikasi sumber atau tujuan paket IP. Saat ini, versi IP yang digunakan disebut IPv4. Dalam versi ini, setiap node di Internet mungkin memiliki satu atau lebih antarmuka, dan kita diharuskan mengidentifikasi setiap perangkat ini dengan alamat unik yang ditetapkan untuk masing-masing perangkat tersebut. Artinya setiap node diberi satu atau lebih alamat IP untuk memanggil TCP/IP. Ini adalah alamat logis dan memiliki 32 bit.

Secara teknis, alamat IP dinyatakan menggunakan notasi biner dengan panjang string 32 bit. Agar string ini mudah diingat, notasi desimal titik digunakan, di mana titik atau titik memisahkan empat angka desimal dari 0 hingga 255 yang mewakili 32 bit. Karena ada 32 bit maka setiap bilangan desimal berisi 8 bit dan disebut oktet.

Misalnya, alamat IPv4 11000000101010000000101000011001 dinyatakan sebagai 192.168.10.25 dalam notasi desimal bertitik. Berikut langkah-langkah mengubah alamat IPv4 dari notasi biner ke notasi desimal putus-putus:

- Memecah alamat sepanjang 32 bit menjadi segmen blok 8-bit: 11000000 10101000 00001010 00011001
- Tuliskan ekuivalen desimal setiap segmen: 192 168 10 25
- Pisahkan blok dengan titik: 192.168.10.25 Gambar 10.2 menunjukkan struktur alamat IP.

| 11000000 | 10101000 | 00001010 | 00011001 |
|---|---|---|---|
| 192 | 168 | 10 | 25 |

**Gambar 10.2 Aalamat IP dalam notasi desimal bertitik**

**Notasi Desimal Bertitik**

Kita telah melihat bahwa alamat IPv4 dinyatakan sebagai angka 32-bit dalam notasi desimal bertitik. Alamat IP mungkin memiliki bagian tetap dan bagian variabel tergantung pada alokasi total alamat untuk Anda atau organisasi Anda. Bagian tetap dari alamat mungkin dari satu oktet hingga tiga oktet dan oktet sisanya akan tersedia untuk bagian variabel. Alamat IPv4 ditetapkan menggunakan bagian ini. Semua bit dalam oktet tetap diatur ke 1 sedangkan

oktet variabel diatur ke 0 bit. Setelah itu, ubah hasilnya menjadi notasi desimal putus-putus. Misalnya, Anda dapat mengambil alamat IP sebagai 192.168.10.25. Sekarang atur semua bit tetap ke 1 dan atur semua bit variabel ke 0. Hasilnya adalah 11111111 11111111 00000000 00000000. Saat mengubahnya menjadi notasi desimal bertitik, hasilnya adalah 255.255.0.0. Notasi desimal putus-putus dengan bagian tetap dan variabel ini digunakan sebagai awalan alamat ke 192.168.10.25 dan dinyatakan sebagai 192.168.10.25, 255.255.0.0. Cara mengekspresikan panjang prefiks sebagai angka desimal bertitik dikenal sebagai notasi network mask atau subnet mask.

**Klasifikasi Alamat IPv4**

Standar Internet mengizinkan alamat berikut:

1. **Unicast**: Ditugaskan ke antarmuka jaringan tunggal yang terletak di subnet tertentu dan memfasilitasi komunikasi satu-ke-satu. Ini adalah alamat unik secara global untuk identifikasi perangkat di jaringan. Ini dapat dipahami sebagai nomor rumah di suatu wilayah tertentu. Ini mencakup awalan subnet dan bagian ID host.
   (a) Awalan subnet: Awalan subnet pada dasarnya adalah pengidentifikasi jaringan atau bagian alamat jaringan dari alamat IP unicast. Perlu dicatat bahwa semua node pada subnet fisik atau logis yang sama harus menggunakan awalan subnet yang sama, yang pada akhirnya menjadi unik dalam seluruh jaringan TCP/IP.
   (b) ID Host: ID host, yang merupakan bagian alamat host dari alamat IP unicast, mengidentifikasi node jaringan yang dihubungkan dengan beberapa perangkat. Ini juga unik dalam segmen jaringan.
2. **Multicast**: Digunakan untuk satu atau lebih antarmuka jaringan yang terletak di berbagai subnet. Ini memungkinkan komunikasi satu-ke-banyak. Ini mengirimkan paket tunggal dari satu sumber ke banyak tujuan. Alamat-alamat ini adalah bagian dari skema pengalamatan Kelas D.
3. **Siaran:** Ini dialokasikan ke semua antarmuka jaringan yang terletak di subnet dan digunakan untuk komunikasi satu-ke-semua di subnet. Ini mengirimkan paket dari satu sumber ke semua antarmuka di subnet. Alamat siaran selanjutnya dapat diklasifikasikan menjadi siaran jaringan, siaran subnet, siaran terarah semua subnet, dan siaran terbatas.

Alamat Internet selanjutnya diklasifikasikan ke dalam kelas yang berbeda. Hal ini didasarkan pada jumlah bit yang digunakan untuk awalan alamat subnet tunggal dan jumlah bit yang digunakan untuk ID host. Oleh karena itu, ia mengalokasikan jumlah jaringan dan jumlah host per jaringan. Ada lima kelas alamat seperti yang diberikan di bawah ini:

1. **Kelas A**: Menggunakan nomor jaringan 8 bit yang bit pertamanya selalu nol seperti ditunjukkan pada Tabel 10.1. Ini dicadangkan untuk alamat IP unicast. Jika jumlah host dalam suatu jaringan sangat besar, kelas ini digunakan. Ia menggunakan satu-satunya oktet untuk menentukan panjang awalan. Jumlah jaringan yang dapat ditampung adalah 28 atau 128. Namun dari 128 alamat tersebut, 2 digunakan untuk keperluan administratif sehingga tersedia 126 alamat sebagai panjang awalan. 3 oktet sisanya digunakan untuk mengidentifikasi hingga 224 atau 16.777.214 ID host.

2. **Kelas B**: Menggunakan 16 bit untuk alamat jaringan dan alamat host. Dalam hal ini dua bit pertama selalu 10. Ini dicadangkan untuk alamat IP unicast. Ia menggunakan 2 oktet untuk jaringan tertentu sementara sisanya dua oktet untuk ID host. Mereka terutama digunakan untuk jaringan berukuran menengah hingga besar. Alamat Kelas B dapat diberikan ke 16,384 jaringan dengan hingga 65,536 host per jaringan.
3. **Kelas C**: Ini dicadangkan untuk alamat IP unicast. Mereka dimaksudkan untuk jaringan kecil. 3 oktet pertama menentukan jaringan tertentu dan oktet terakhir menentukan ID host. Alamat Kelas C dapat digunakan hingga 2.097.152 jaringan dengan hingga 254 host per jaringan. Tiga bit pertamanya selalu disetel ke 110.
4. **Kelas D**: Ini mendefinisikan alamat IP multicast.
5. **Kelas E**: Alamat ini dicadangkan untuk penggunaan eksperimental. Tabel ini mewakili klasifikasi alamat IPv4.

**Tabel 10.1 Klasisikasi Alamat IPv4**

| **Alamat 32-bit** | | | | | **Jumlah jaringan yang mungkin** | **Jumlah maksimum host atau rode** |
|---|---|---|---|---|---|---|
| **klasifikasi** | **Oktet 1** | **Oktet 2** | **Oktet 3** | **Oktet 4** | | |
| Kelas A | 0bbbbbbb | xxxxxxxx | xxxxxxxx | Xxxxxxx | $2^7$= 128 | $2^{24}$= 16.777.216 |
| Kelas B | 10bbbbbb | bbbbbbbb | xxxxxxxxx | xxxxxxxx | $2^{14}$= 16,384 | $2^{14}$ = 65.536 |
| Kelas C | 110bbbbb | bbbbbbbb | bbbbbbbb | Xxxxxxxx | $2^{21}$= 2,097,152 | $2^8$= 256 |
| Kelas D | 1110bbbb diikuti dengan alamat multicast 28 bit | | | | | |
| Kelas E | 1111; disimpan | | | | | |

Alokasi alamat IPv4 berdasarkan skema di atas terkadang terbukti membuang-buang alamat. Setiap organisasi dengan alamat Kelas A mungkin memiliki 16.777.214 host. Mungkin, tidak ada organisasi yang memiliki lebih dari 100.000 host. Dalam hal ini alamat IPv4 yang besar hanya terbuang sia-sia. Sebelumnya, metode Classless Inter-Domain Routing (CIDR) digunakan untuk mengalokasikan alamat IPv4 berdasarkan kebutuhan organisasi. Badan yaitu Internet Corporation for Assigned Names and Numbers (ICANN) atau Penyedia Layanan Internet (ISP) bertanggung jawab untuk menentukan kebutuhan organisasi untuk mengalokasikan alamat IPv4 berdasarkan Kelas yang disyaratkan.

Dalam kasus alamat individual, alamat publik digunakan. Alamat pribadi juga dialokasikan berdasarkan konektivitas yang diproksi atau diterjemahkan ke Internet. Terlihat bahwa pengguna yang merupakan bagian dari organisasi mana pun atau tergabung dalam ISP tidak memerlukan konektivitas langsung ke Internet. Oleh karena itu organisasi atau ISP tersebut hanya memerlukan beberapa alamat publik untuk node mereka seperti server proxy, router, firewall, dan penerjemah, dll. agar dapat terhubung langsung dengan Internet. Oleh

karena itu, beberapa alamat dicadangkan untuk penggunaan pribadi dan berbeda dengan alamat publik.

Alamat adalah pengidentifikasi yang ditetapkan ke perangkat yang terhubung ke node di Internet. Ini menceritakan tentang sumber atau tujuan paket IP. Alamat diklasifikasikan berdasarkan tujuannya sebagai unicast, multicast, dan siaran. Jumlah segmen jaringan dan host pada jaringan ditentukan berdasarkan alamat Kelas A, B dan C untuk komunikasi unicast.

**Subnetting untuk Alamat IP**

Selama beberapa tahun terakhir, Internet telah meningkatkan jumlah host yang terhubung dengannya dan oleh karena itu alamat IPv4 yang belum tersedia semakin langka. Anda mungkin bingung di sini karena 32 bit memberikan 232 alamat unik yang menghasilkan sekitar 4,3 miliar alamat berbeda. Namun kondisi ini tidak terjadi karena perbedaan kelas alamat IPv4. Misalkan sebuah organisasi berukuran sedang mendapatkan alamat Kelas B berdasarkan populasi penggunanya saat ini, katakanlah 1000. Ia menggunakan 1000 alamat berbeda. Namun manajemen organisasi memiliki kemampuan untuk menetapkan 216 = 65.536 pengidentifikasi berbeda. Artinya terdapat 65.536 alamat yang terbuang. Karena semuanya termasuk dalam nomor jaringan kelas B yang sama, maka tidak dapat diklaim kembali oleh organisasi lain mana pun.

Administrator jaringan mungkin menyarankan penggunaan alamat jaringan Kelas C, yang mungkin memerlukan setidaknya empat jaringan kelas C. Nanti, misalkan, jumlah pengguna bertambah dan organisasi mengajukan permohonan untuk jaringan kelas C lain, jaringan tersebut mungkin tidak mendapatkan hasil yang sama atau jika berhasil, harus melewati banyak dokumen dan penundaan. Selain itu, ada sudut pandang lain dari masalah ini sehubungan dengan perutean tambahan. Dengan banyaknya jaringan Kelas C, Anda perlu memiliki lebih banyak nomor jaringan agar router dapat dilacak. Akibatnya kinerja jaringan menurun. Solusi dari masalah ini terletak pada peningkatan jumlah bit pada alamat IP atau Classless Inter Domain Routing (CIDR).

Kita juga dapat menggunakan teknik yang disebut subnetting untuk membagi secara efisien ruang alamat yang dialokasikan ke suatu organisasi ke pengguna berbeda yang dibagi di antara subnet berbeda dalam jaringan organisasi. Oleh karena itu subnetting adalah suatu proses di mana ruang alamat dari awalan alamat unicast dibagi secara efisien untuk alokasi di antara subnet-subnet jaringan organisasi. Seperti kita ketahui bahwa alamat unicast memiliki porsi yang tetap dan variabel. Bagian tetap dari awalan alamat unicast memiliki nilai yang ditentukan. Bagian variabel dari awalan alamat unicast memiliki bit di luar panjang awalan, yang perlu diatur ke 0. Subnet menggunakan bagian variabel dari awalan alamat unicast untuk ditugaskan ke subnet jaringan organisasi.

Untuk menerapkan subnetting, Anda perlu mengikuti beberapa panduan:

- Menilai jumlah kebutuhan subnet.
- Menilai jumlah ID host untuk setiap subnet.

Setelah ini, satu set prefiks alamat subnet dengan rentang alamat IP yang valid dapat ditentukan. Langkah-langkah berikut diikuti untuk subnetting:

1. Perkirakan jumlah bit host untuk subnetting.

2. Tentukan awalan alamat subnet yang baru.
3. Tentukan kisaran alamat IP untuk setiap awalan alamat subnet baru.

Sekarang kita dapat mempelajari bagaimana awalan subnet dari sebuah alamat IP ditentukan. Langkah-langkah berikut memberi Anda cara untuk menentukannya tanpa menggunakan bilangan biner:

1. Tulislah bilangan n (panjang awalan) sebagai hasil penjumlahan dari 4 bilangan dengan mengurangkan n secara berturut-turut 8. Misalnya, 22 adalah 8+8+6+0.
2. Dalam tabel dengan empat kolom dan tiga baris, tempatkan oktet desimal alamat IP di baris pertama. Baris kedua kemudian akan berisi empat digit jumlah seperti yang telah ditentukan pada langkah 1.
3. Kolom yang mempunyai angka 8 pada baris kedua, tuliskan oktet yang sesuai dari baris pertama hingga baris ketiga. Jika ada 0 pada kolom di baris kedua, tempatkan 0 di baris ketiga.
4. Kolom pada baris kedua yang mempunyai angka antara 0 sampai 8, ubah bilangan desimal pada baris pertama menjadi biner. Sekarang pilih bit tingkat tinggi untuk jumlah bit yang ditunjukkan pada baris kedua dan beri nol untuk bit yang tersisa dan kemudian ubah kembali ke angka desimal. Ini akan menjadi entri di kolom itu. Sebagai contoh, entri pada kolom ketiga pada baris pertama adalah 10. Oleh karena itu, ekuivalen binernya adalah 00001010. Sekali lagi, kolom ketiga pada baris kedua memiliki 6. Artinya kita harus mengambil 6 bit dari sisi bi tinggi dan mengonversinya menjadi sisa dua bit sebagai 00. Ini akan memberi kita bilangan biner 00001000 yang merupakan desimal yang setara dengan 8. Oleh karena itu, entri 8 akan masuk ke kolom itu.

| | | | |
|---|---|---|---|
| **192** | **168** | **10** | **25** |
| **8** | **8** | **6** | **0** |
| **192** | **168** | **8** | **0** |

Ini memberikan awalan subnet untuk konfigurasi alamat IPv4 192.168.10.25/22 sebagai 192.168.204.0/ 22.

Sekarang, kita harus mengekstrak awalan subnet dari alamat IPv4 sembarang menggunakan subnet mask sembarang. Untuk tujuan ini operasi matematika logika AND digunakan. Perbandingan logis antara alamat IP 32-bit dan subnet mask 32-bit dilakukan. Ini memberikan awalan subnet. Misalnya, kita dapat mempertimbangkan kemungkinan alamat berikut untuk Kelas C.

| Jaringan Kelas C | Representasi Sedikit | Rentang Alamat |
|---|---|---|
| 210.195.8.0 | 11010010-11000011-00001000-xxxxxxxx | 210.195.8.0-211.195.8.255 |
| 210.195.9.0 | 11010010-11000011-00001001-xxxxxxxx | 210.195.9.0-211.195.9.255 |
| 210.195.10.0 | 11010010-11000011-00001010-xxxxxxxx | 210.195.10.0-211.195.10.255 |

| | | |
|---|---|---|
| 210.195.11.0 | 11010010-11000011-00001011-xxxxxxxx | 210.195.11.0-211.195.11.255 |

Jaringan Kelas C ini menentukan kumpulan alamat yang berdekatan dari 210.195.8.0 hingga 210.195.11.255. Saat memeriksa alamat-alamat ini, diamati bahwa 22 bit pertama sama untuk setiap alamat. Artinya, salah satu jaringan Kelas C ini memiliki nomor jaringan 22 bit diikuti dengan pengenal lokal 10 bit untuk host. Router kemudian dapat mengekstrak nomor jaringan menggunakan operasi logika AND antara subnet mask 22-bit dan alamat IP. Untuk contoh ini, kita dapat mengatakan bahwa sebuah router dapat mewakili empat jaringan menggunakan entri tunggal 210.195.8.0/22, dimana /22 menunjukkan nomor jaringan memiliki panjang 22 bit. Demikian pula, alamat 210.195.8.0/20 akan terdiri dari 20 bit pertama dan seterusnya. Ini menunjukkan bahwa kami mengelompokkan jaringan-jaringan kecil yang berbeda dan diperlakukan sama untuk tujuan perutean.

Beri tahu kami, ambil contoh. Alamat IPv4 kami adalah 210.195.8.0 dan subnet mask 22 bit adalah 255.255.252.0.

$$11010010 - 11000011 - 000010xx - xxxxxxxx\ (IP\ Address)$$

Dan

$$\frac{11111111 - 11111111 - 11111100 - 00000000}{\underset{(210)}{11010010} - \underset{(195)}{11010011} - \underset{(8)}{00001000} - \underset{(0)}{00000000}}\ \frac{(22\ bit\ subnet\ mask)}{(network\ number)}$$

Hasil logika bit-wise AND dari 32 bit alamat IPv4 dan subnet mask adalah awalan subnet 210.195.8.0. Oleh karena itu dapat dicatat bahwa bit-bit di bagian alamat tetap (di mana bit-bit di subnet mask diatur ke 1), bit-bit awalan subnet disalin dari alamat IPv4, yang pada dasarnya mengekstraksi awalan subnet dari alamat IPv4. Di sisi lain, bit-bit di bagian variabel alamat yang disetel ke nol, bit awalan subnet juga disetel ke 0 dan dengan demikian membuang bagian ID host dari alamat IPv4.

## 10.2 PENGENDALIAN KEMACETAN

Kemacetan menyebabkan tersendatnya saluran komunikasi. Jika terlalu banyak paket yang ada di suatu bagian subnet, kinerja subnet akan menurun. Oleh karena itu, saluran komunikasi suatu jaringan disebut macet jika paket-paket yang melintasi jalur tersebut mengalami penundaan yang sebagian besar melebihi penundaan propagasi jalur. Disebut sangat padat ketika paket tidak pernah mencapai tujuan yang menunjukkan bahwa penundaan mendekati tak terhingga. Penyebab kemacetan bukan hanya satu, tapi banyak. Ketika laju lalu lintas masukan melebihi kapasitas jalur keluaran, bagian masukan dari subnet akan tersumbat dan menimbulkan kemacetan. Kemacetan juga terjadi ketika router terlalu lambat untuk melakukan antrian buffer, memperbarui tabel, dll. Kurangnya kapasitas buffer router juga merupakan salah satu dari banyak faktor kemacetan. Namun, meningkatkan memori router mungkin berguna sampai titik tertentu. Melampaui batas waktu tertentu, kemacetan akan semakin parah karena batas waktu transmisi ulang akan menambah beban

lalu lintas. Secara singkat, penyebab kemacetan adalah kemacetan pada beberapa jalur input, prosesor yang lambat, bandwidth yang rendah, jumlah buffer yang terbatas, dan lain-lain.

Tahukah kamu? Pengendalian kemacetan dan pengendalian aliran adalah dua fenomena yang berbeda. Kemacetan adalah fenomena global yang melibatkan semua host, semua router, pemrosesan store-and-forward di dalam router, dll., sedangkan kontrol aliran berkaitan dengan lalu lintas point-to-point antara host sumber tertentu dan host tujuan tertentu. Contoh pengendalian kemacetan adalah situasi ketika jaringan store-and-forward dengan jalur 1-Mbps dan 1000 komputer mini besar, separuhnya mencoba mentransfer file dengan kecepatan 100 kbps ke separuh lainnya. Contoh pengontrol aliran adalah ketika jaringan serat optik berkapasitas 1000 gigabit/detik di mana superkomputer mencoba mentransfer file ke komputer pribadi dengan kecepatan 1Gbps.

**Prinsip Umum Pengendalian Kemacetan**

Menurut teori kendali, jaringan komputer yang juga merupakan suatu sistem dibagi menjadi dua kelompok. Yaitu solusi loop terbuka dan loop tertutup. Solusi loop terbuka: berikan desain yang baik untuk memastikan bahwa masalah tidak terjadi. Alat perancangan mencakup keputusan untuk menerima lalu lintas baru, membuang paket, dan menjadwalkan paket di berbagai titik dalam jaringan. Keputusan solusi loop terbuka tidak bergantung pada kondisi jaringan saat ini.

Solusi loop tertutup: membuat keputusan berdasarkan konsep putaran umpan balik. Putaran umpan balik memungkinkan sistem putaran tertutup memantau sistem untuk mendeteksi kapan dan di mana kemacetan terjadi. Setelah itu, informasi tersebut diteruskan ke tempat-tempat di mana tindakan dapat diambil. Hal ini memungkinkan untuk menyesuaikan operasi sistem untuk memperbaiki masalah.

Pemantauan sistem bergantung pada persentase seluruh paket yang dibuang karena kurangnya ruang buffer, rata-rata panjang antrian, jumlah paket yang habis waktu dan dikirim ulang, rata-rata penundaan paket, dan standar deviasi penundaan paket. Informasi kemacetan yang dipantau diberikan ke semua tempat tindakan ketika router mendeteksi kemacetan; ia segera mengirimkan paket peringatan terpisah ke sumber lalu lintas. Hal ini dilakukan dengan mencadangkan sedikit atau field di setiap paket yang diisi di setiap paket keluar jika terjadi keadaan padat yang ditemui oleh router untuk memperingatkan tetangganya. Kedua, host atau router mengirimkan paket secara berkala untuk mengetahui secara eksplisit tentang kemacetan sehingga lalu lintas di sekitar area yang padat dapat dialihkan ke jalur tujuan alternatif.

Kemacetan dapat dikendalikan seperti yang diberikan di bawah ini:

1. Meningkatkan bandwidth dalam jaringan. Menambah jalur tambahan untuk sementara akan meningkatkan bandwidth antara titik-titik tertentu.
2. Bagi lalu lintas untuk mengikuti beberapa rute.
3. Tingkatkan sumber daya. Misalnya saja menggunakan router cadangan.
4. Kurangi beban dengan menolak layanan kepada beberapa pengguna atau merendahkan layanan kepada beberapa atau semua pengguna.
5. Perkirakan jadwal dan permintaan pengguna dengan cara yang lebih dapat diprediksi.

**Manajemen Lalu Lintas**

Fasilitas manajemen lalu lintas memungkinkan memaksimalkan sumber daya jaringan yang tersedia dan memastikan efisiensi penggunaan sumber daya yang belum dialokasikan secara eksplisit. Manajemen lalu lintas terutama akan bergantung pada prioritas transmisi dan ketersediaan bandwidth. Dalam prioritas transmisi, lalu lintas yang sensitif terhadap penundaan diberi prioritas transmisi yang lebih tinggi. Dukungan terhadap ketersediaan bandwidth berkaitan dengan alokasi bandwidth untuk setiap VCC, kontrol penerimaan koneksi (CAC) yang mencegah pengguna jaringan mengalokasikan lebih banyak bandwidth daripada yang dapat disediakan oleh jaringan, kebijakan lalu lintas untuk memastikan bahwa VCC, setelah dibuat, tidak berusaha menggunakan lebih banyak bandwidth daripada yang jaringan saat ini memiliki pembuangan sel yang tersedia dan selektif yang berhubungan dengan langganan kapasitas buffer port keluaran sesaat.

**Memperkirakan Rata-rata Keterlambatan Paket**

Rata-rata kecepatan kedatangan paket di router untuk diproses = $\lambda$ paket per detik
Rata-rata kecepatan pemrosesan paket satu per satu di router = $\mu$ paket per detik
Pemanfaatan saluran = $\rho = \lambda/\mu$

Dari teori Queuing, rata-rata penundaan yang dialami sebuah paket di router sebelum diteruskan diberikan oleh:

$$T = \lambda/\mu\,(1/1-\rho)$$

Dari penjelasan di atas, jelas bahwa penundaan rata-rata mendekati tak terhingga ketika pemanfaatan mendekati satu kesatuan.

**Kebijakan Pencegahan Kemacetan**

Sistem loop terbuka dirancang untuk meminimalkan kemacetan di tempat asalnya. Menerapkan kebijakan pencegahan kemacetan di berbagai lapisan akan memecahkan masalah dalam kasus sistem loop terbuka. Kebijakan pada lapisan data link, jaringan dan transport yang mempengaruhi kemacetan diberikan di bawah ini:

(a) **Lapisan data link**: Permasalahan seperti transmisi ulang paket, caching yang tidak sesuai, pengakuan paket yang diterima dari mesin tujuan dan kontrol aliran mempengaruhi kemacetan pada lapisan ini.

(b) **Lapisan jaringan**: Pengaturan saluran virtual dan datagram di dalam subnet, antrian dan penerusan paket di router, menjatuhkan paket di router, algoritma perutean, manajemen masa pakai paket, dll merupakan faktor-faktor yang mempengaruhi kemacetan di lapisan ini.

(c) **Lapisan transport**: Transmisi ulang paket, caching yang rusak, pengakuan paket yang diterima dari mesin tujuan, mekanisme kontrol aliran, batas waktu paket habis, dll. mempengaruhi kemacetan pada lapisan ini.

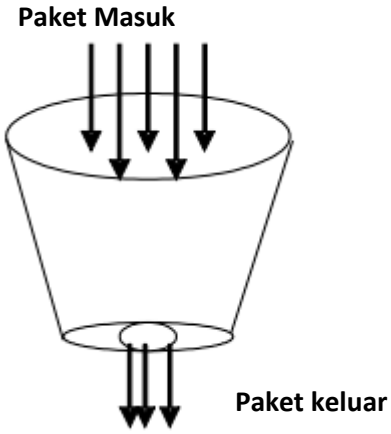
**Pembentukan Lalu Lintas**

Salah satu penyebab utama kemacetan adalah kemacetan lalu lintas. Penyebab lainnya adalah pengiriman paket dengan kecepatan yang tidak dapat diprediksi. Oleh karena itu, pendekatan pembentukan lalu lintas mencakup transmisi paket pada kecepatan yang seragam dan kecepatan yang lebih dapat diprediksi dalam kasus metode loop terbuka. Dengan

demikian, pembentukan lalu lintas berupaya untuk mengatur kecepatan rata-rata transmisi data. Misalnya, jaringan ATM lebih memanfaatkan metode ini. Untuk mengurangi kemacetan, pengguna dan subnet menyepakati pola lalu lintas tertentu dalam sirkuit virtual. Perjanjian tersebut sangat penting untuk transfer koneksi audio dan video real-time, yang tidak menoleransi kemacetan. Pemantauan pola lalu lintas disebut kebijakan lalu lintas.

**Ember Bocor**

Algoritme ember bocor menemukan kegunaannya dalam konteks pembentukan lalu lintas jaringan atau pembatasan laju. Algoritme ini memungkinkan untuk mengontrol kecepatan di mana data dimasukkan ke dalam jaringan dan dengan demikian menangani lonjakan kecepatan data. Implementasi bucket bocor dan implementasi token bucket sebagian besar digunakan untuk algoritma pembentukan lalu lintas. Algoritma leaky-bucket digunakan untuk mengontrol laju lalu lintas yang dikirim ke jaringan dan membentuk lalu lintas yang meledak menjadi aliran lalu lintas yang stabil. Gambar 10.3 menunjukkan algoritma leaky bucket.




**Gambar 10.3 Algoritme Ember Yang Bocor**

Dalam algoritma ember bocor, ember dengan volume, katakanlah, b byte dan dengan lubang di bagian bawah dipertimbangkan. Jika bucket kosong, berarti b byte tersedia sebagai penyimpanran. Sebuah paket dengan ukuran kurang dari b byte tiba di bucket, maka akan diteruskan. Jika ukuran paket bertambah lebih dari b byte, paket tersebut akan dibuang atau dimasukkan ke dalam antrian. Diasumsikan juga bahwa ember bocor melalui lubang di bagian bawahnya dengan kecepatan konstan r byte per detik. Aliran keluar dianggap pada tingkat yang konstan ketika ada paket di dalam keranjang, dan nol ketika keranjang kosong. Hal ini menjelaskan bahwa jika data mengalir ke dalam bucket lebih cepat daripada data yang keluar melalui lubang, maka bucket akan meluap. Hal ini mengakibatkan data masuk selanjutnya dibuang hingga volume yang cukup tersedia lagi di bucket untuk menerima data baru.

Kerugian yang terkait dengan algoritma leaky-bucket adalah penggunaan sumber daya jaringan yang tersedia tidak efisien. Tingkat kebocoran adalah parameter tetap. Jika volume lalu lintas sangat rendah, sebagian besar sumber daya jaringan seperti bandwidth tidak digunakan secara efisien. Algoritme leaky-bucket tidak memungkinkan aliran individu

melonjak hingga kecepatan port untuk secara efektif menggunakan sumber daya jaringan pada saat tidak ada pertikaian sumber daya dalam jaringan.

Algoritme ember bocor menggunakan parameter laju rata-rata dan laju ledakan untuk mengontrol arus lalu lintas. Kecepatan rata-rata didefinisikan sebagai jumlah rata-rata paket per detik yang bocor dari lubang di dasar ember dan masuk ke jaringan. Burst rate adalah laju akumulasi paket dalam bucket dan dinyatakan dalam paket per detik. Misalnya, jika laju burst rata-rata adalah 10 paket per detik, maka burst 10 detik memungkinkan 100 paket terakumulasi dalam bucket. Misalnya, jika kecepatan rata-rata adalah 10 paket per detik dan 100 paket telah terakumulasi dalam bucket, maka waktu virtualnya adalah 10 detik lebih cepat dari waktu saat ini.

**Algoritma Token Bucket**

Algoritme ember bocor memiliki pola keluaran yang kaku pada laju rata-rata yang tidak bergantung pada lalu lintas yang meledak. Dalam banyak aplikasi, ketika semburan besar terjadi, keluarannya dibiarkan dipercepat. Hal ini memerlukan algoritma yang lebih fleksibel, sebaiknya yang tidak pernah kehilangan data. Oleh karena itu, algoritma token bucket menemukan kegunaannya dalam konteks pembentukan lalu lintas jaringan atau pembatasan laju. Token bucket adalah algoritma kontrol yang menentukan kapan lalu lintas harus ditransmisikan. Pesanan ini datang berdasarkan keberadaan token di dalam ember. Ember berisi token. Masing-masing token mewakili paket dengan ukuran yang telah ditentukan. Token dalam ember dihapus agar dapat mengirim paket. Ketika token hadir, aliran untuk mengirimkan lalu lintas terjadi di hadapan token. Tidak ada token berarti tidak ada aliran yang mengirimkan paketnya. Oleh karena itu, suatu aliran mentransmisikan lalu lintas hingga tingkat ledakan puncaknya dengan adanya token yang memadai di dalam keranjang.

Jadi, algoritma token bucket menambahkan token ke bucket setiap 1/r detik. Kapasitas ember adalah b token. Ketika token tiba dan embernya penuh, token tersebut dibuang. Jika paket berisi n byte tiba dan n token dikeluarkan dari bucket, paket tersebut diteruskan ke jaringan. Ketika paket berisi n byte tiba tetapi kurang dari n token yang tersedia. Dalam kasus seperti ini, tidak ada token yang dikeluarkan dari bucket dan paket tersebut dianggap tidak sesuai. Paket yang tidak sesuai dapat dibuang atau dimasukkan ke dalam antrean untuk transmisi berikutnya ketika token yang cukup telah terkumpul di dalam keranjang. Mereka juga dapat ditularkan tetapi ditandai sebagai non-konforman. Kemungkinannya adalah mereka akan dihapus jika jaringan kelebihan beban. Keuntungan dari algoritma ini adalah menghemat hingga ukuran maksimum bucket. Artinya, semburan hingga jumlah paket dapat dikirim dengan kecepatan maksimal dalam jangka waktu tertentu.

## 10.3 KUALITAS PELAYANAN

*Quality of Service* (QoS) menentukan kemampuan jaringan untuk menyediakan layanan yang dapat diprediksi melalui berbagai teknologi termasuk frame relay, *Asynchronous Transfer Mode* (ATM), Ethernet, SONET dan jaringan IP-routed. Jaringan dapat menggunakan salah satu atau semua teknologi ini. QoS juga memastikan bahwa meskipun memberikan prioritas untuk satu atau lebih aliran, tidak membuat aliran lainnya gagal. Aliran dapat berupa

kombinasi alamat sumber dan tujuan, nomor soket sumber dan tujuan, serta pengidentifikasi sesi atau paket apa pun dari aplikasi tertentu atau dari antarmuka masuk. QoS terutama digunakan untuk mengontrol sumber daya seperti bandwidth, peralatan, fasilitas area luas dan sebagainya, membuat penggunaan sumber daya jaringan lebih efisien, menyediakan layanan yang disesuaikan, menyediakan aplikasi yang sangat penting dan koeksistensi, dll.

Lalu lintas ke jaringan komputer sering kali mendapat prioritas yang sama dan jaringan komputer biasanya tidak membedakan antara lalu lintas browser yang tidak penting dan aplikasi bisnis penting. Kualitas layanan (QoS) jaringan komputer dievaluasi sehubungan dengan prioritas lalu lintas untuk memahami mengapa QoS diinginkan di intranet dan Internet. Bandwidth dianggap sebagai subjek penting untuk layanan Internet dan intranet. Jumlah data yang dikirimkan melalui Internet telah meningkat secara eksponensial dan aplikasi baru seperti audio dan video nyata; VoIP, konferensi video, dll. terus menuntut peningkatan bandwidth. Aplikasi Internet konvensional seperti WWW, FTP, telnet; dll. tidak dapat mentolerir kehilangan paket tetapi kurang sensitif terhadap penundaan variabel. Namun, sebagian besar aplikasi real-time dapat mengkompensasi hilangnya paket dalam jumlah yang wajar tetapi biasanya sangat penting terhadap penundaan variabel yang tinggi. Oleh karena itu, bandwidth memegang peranan penting dalam memberikan kualitas layanan yang baik. QoS didefinisikan sebagai kerangka kebijakan yang menggambarkan kualitas aliran data tertentu dalam hal bandwidth, penggunaan buffer, prioritas, penggunaan CPU, dll. Namun, tumpukan protokol IP hanya menyediakan satu QoS dalam hal upaya terbaik di mana paket ditransmisikan dari titik ke titik tanpa jaminan bandwidth khusus atau penundaan waktu minimum. Model lalu lintas upaya terbaik menangani semua permintaan Internet dengan prioritas yang sama dan melayani permintaan tersebut dengan strategi siapa cepat dia dapat.

**Arsitektur QoS Dasar**

QoS memungkinkan layanan yang lebih baik untuk aliran tertentu dalam jaringan dengan meningkatkan prioritas suatu aliran atau membatasi prioritas aliran lainnya. Alat manajemen antrean, kebijakan dan pembentukan, alat efisiensi tautan, dll. digunakan untuk mengendalikan arus dan kemacetan. Dengan demikian, alat QoS bertujuan untuk mengatasi sebagian besar masalah kemacetan. Arsitektur dasar QoS melibatkan tiga bagian mendasar untuk implementasi QoS. Teknik-teknik tersebut adalah identifikasi dan penandaan QoS untuk mengoordinasikan QoS dari ujung ke ujung antar elemen jaringan, QoS dalam satu elemen jaringan, misalnya, alat antrian, penjadwalan, dan pembentuk lalu lintas, serta manajemen kebijakan QoS dan fungsi akuntansi untuk mengontrol dan mengatur akhir- lalu lintas ke ujung di seluruh jaringan.

Identifikasi dan Penandaan QoS dilakukan melalui klasifikasi dan reservasi. Klasifikasi mengacu pada mengidentifikasi dan memberikan layanan preferensial untuk suatu jenis lalu lintas. Dalam klasifikasi, paket mungkin ditandai atau tidak. Jika paket teridentifikasi tetapi tidak ditandai, maka dikatakan paket tersebut berbasis per-hop. Jika paket ditandai, byte prioritas IP diatur. Metode umum untuk mengidentifikasi aliran adalah Daftar Kontrol Akses (ACL), Perutean Berbasis Kebijakan, Tingkat Akses Berkomitmen (CAR), Pengenalan Aplikasi Berbasis Jaringan (NBAR), dll.

**Konsep QoS**

Manajemen Kemacetan: Sifat lalu lintas data yang padat, terkadang meningkatkan jumlah lalu lintas lebih dari kecepatan tautan. Dalam situasi seperti ini, QoS memungkinkan router untuk menempatkan paket ke dalam antrian yang berbeda dan melayani antrian tertentu lebih sering berdasarkan prioritas daripada buffer lalu lintas dalam satu antrian dan membiarkan paket pertama yang masuk menjadi paket pertama yang keluar. Permasalahan seperti ini dimasukkan ke dalam alat manajemen kemacetan untuk menanganinya. Dengan demikian, alat manajemen kemacetan dapat mencakup antrian prioritas, antrian khusus, antrian adil tertimbang, dll.

Manajemen Antrian: Antrian di buffer mungkin terisi dan meluap. Sebuah paket akan di-drop jika antrian sudah penuh dan router tidak dapat mencegah paket tersebut di-drop meskipun paket tersebut merupakan paket dengan prioritas tinggi. Hal ini disebut sebagai penurunan ekor. Hal ini dapat dicegah dengan memastikan bahwa antrian tidak terisi dan menyediakan ruang untuk paket berprioritas tinggi atau mengizinkan beberapa aturan untuk membuang paket dengan prioritas lebih rendah sebelum membuang paket dengan prioritas lebih tinggi. Mekanisme yang disebut deteksi acak dini tertimbang menjalankan kedua fungsi ini.

- **Efisiensi Tautan**: Terkadang, tautan berkecepatan rendah menjadi penghambat paket yang lebih kecil. Keterlambatan serialisasi yang disebabkan oleh paket besar memaksa paket kecil menunggu lebih lama. Penundaan serialisasi adalah waktu yang dibutuhkan untuk menempatkan paket pada link. Penundaan serialisasi (Misalnya, penundaan serialisasi untuk paket 2400-byte pada tautan 56-kbps adalah 343 milidetik) akan membuat paket suara, yang berada di belakangnya dalam antrian, mengalami penundaan yang sangat besar sebelum paket meninggalkan router, a situasi, yang tidak diinginkan untuk paket suara. Proses fragmentasi tautan dan interleave membagi paket besar menjadi paket-paket lebih kecil yang menyisipkan paket suara.
- **Penghapusan bit overhead**: Efisiensi juga dapat ditingkatkan dengan menghilangkan terlalu banyak bit overhead. Misalnya, header RTP memiliki header 40 byte dan payload sedikitnya 20 byte. Dalam kasus seperti ini, biaya overhead adalah dua kali lipat dari muatan. Beberapa teknik kompresi dapat diterapkan untuk memperkecil header ke ukuran yang lebih mudah diatur.
- **Pembentukan dan pengawasan lalu lintas**: Pembentukan digunakan untuk mencegah masalah overflow dalam buffer dengan membatasi potensi bandwidth penuh dari paket aplikasi. Kadang-kadang, dalam banyak topologi jaringan yang memiliki link bandwidth tinggi yang terhubung dengan link bandwidth rendah di situs terpencil mungkin meluap link bandwidth rendah. Oleh karena itu, pembentukan digunakan untuk menyediakan arus lalu lintas dari link dengan bandwidth tinggi lebih dekat ke link dengan bandwidth rendah untuk menghindari meluapnya link dengan bandwidth rendah. Pemolisian digunakan untuk membuang lalu lintas yang melebihi laju yang dikonfigurasi tetapi jika dibentuk, lalu lintas tersebut di-buffer.

**Tingkat QoS ujung ke ujung**

Hal ini mengacu pada kemampuan jaringan untuk memberikan layanan yang dibutuhkan oleh lalu lintas jaringan tertentu dari ujung ke ujung atau ujung ke ujung di bawah batasan jaringan seperti bandwidth, penundaan, jitter, karakteristik kerugian, dll. Faktor-faktor ini menggambarkan seberapa erat hubungan ujung ke ujung. layanan berfungsi. QoS melibatkan kerangka kebijakan atau seperangkat aturan yang menentukan suatu tindakan. Kerangka kebijakan menyediakan layanan tertentu untuk klien, aplikasi, dan jadwal tertentu. Tiga tingkat dasar QoS end-to-end dapat disediakan di jaringan heterogen. Yaitu jenis layanan terpadu, layanan terdiferensiasi, dan layanan masuk masuk.

- **Batasan Kinerja**: Batasan kinerja juga mempertimbangkan batas token bucket dan batas bandwidth secara bersamaan untuk menjamin pengiriman paket dalam kebijakan bandwidth keluar untuk layanan yang terintegrasi dan terdiferensiasi.
- **Ukuran Token Bucket**: Ketika aplikasi mengirimkan informasi lebih cepat daripada server mengirimkan data keluar dari jaringan, buffer akan terisi. Untuk menghindari situasi seperti itu, ukuran token bucket diterapkan untuk menentukan jumlah informasi yang dapat diproses oleh server pada waktu tertentu. Paket yang melebihi batas ini tidak dianggap. Namun, dalam layanan terintegrasi, paket apa pun yang melebihi ukuran paket tidak dibatasi tetapi dibuang dan tidak akan diizinkan untuk permintaan koneksi RSVP. Ukuran keranjang token maksimum dianggap 1 GB.
- **Batas Kecepatan Token**: Batas kecepatan adalah jumlah bit per detik yang diperbolehkan masuk ke dalam jaringan. Bandwidth yang diminta untuk suatu aplikasi dibandingkan dengan batas laju token. Ketika bandwidth yang diminta melebihi batas kecepatan, permintaan ditolak. Batas tarif token hanya digunakan untuk kontrol penerimaan dalam layanan terintegrasi. Nilai ini dapat berkisar dari 10 Kbps hingga 1 Gbps.

**Ringkasan**

- Alamat IPv4 secara unik digunakan sebagai pengidentifikasi, yang bekerja pada lapisan jaringan untuk mengidentifikasi sumber atau tujuan paket IP. Saat ini, versi IP yang digunakan disebut IPv4. Dalam versi ini, setiap node di Internet mungkin memiliki satu atau lebih antarmuka, dan kita diharuskan mengidentifikasi setiap perangkat ini dengan alamat unik yang ditetapkan untuk masing-masing perangkat tersebut. Artinya setiap node diberi satu atau lebih alamat IP untuk memanggil TCP/IP. Ini adalah alamat logis dan memiliki 32 bit.
- Perancang protokol internet mendefinisikan alamat IP sebagai angka 32-bit dan sistem ini, yang dikenal sebagai protokol internet versi 4 (ipv4), masih digunakan sampai sekarang. Namun, karena pertumbuhan internet yang sangat besar dan perkiraan menipisnya alamat yang tersedia, sistem pengalamatan baru (ipv6), menggunakan 128 bit untuk alamatnya.
- Ketika terlalu banyak paket yang ada di suatu bagian subnet, kinerja subnet akan menurun. Oleh karena itu, saluran komunikasi suatu jaringan disebut macet jika paket-

paket yang melintasi jalur tersebut mengalami penundaan yang sebagian besar melebihi penundaan propagasi jalur. Disebut sangat padat ketika paket tidak pernah mencapai tujuan yang menunjukkan bahwa penundaan mendekati tak terhingga.

- Pengendalian kemacetan dan pengendalian aliran adalah dua fenomena yang berbeda. Kemacetan adalah fenomena global yang melibatkan semua host, semua router, pemrosesan store-and-forward di dalam router, dll., sedangkan kontrol aliran berkaitan dengan lalu lintas point-to-point antara host sumber tertentu dan host tujuan tertentu.
- Menurut teori kendali, jaringan komputer yang juga merupakan suatu sistem, dibagi menjadi dua kelompok. Yaitu solusi loop terbuka dan loop tertutup.
- Fasilitas manajemen lalu lintas memungkinkan memaksimalkan sumber daya jaringan yang tersedia dan memastikan efisiensi penggunaan sumber daya yang belum dialokasikan secara eksplisit. Manajemen lalu lintas terutama akan bergantung pada prioritas transmisi dan ketersediaan bandwidth. Dalam prioritas transmisi, lalu lintas yang sensitif terhadap penundaan diberi prioritas transmisi yang lebih tinggi.
- Algoritma leaky bucket digunakan dalam konteks pembentukan lalu lintas jaringan atau pembatasan laju. Algoritme ini memungkinkan untuk mengontrol kecepatan di mana data dimasukkan ke dalam jaringan dan dengan demikian menangani lonjakan kecepatan data.

**Latihan Soal**

Isilah bagian yang kosong:

1. ……. adalah kumpulan beberapa jaringan independen, yang saling berhubungan satu sama lain.
2. …….. pada dasarnya adalah pengidentifikasi jaringan atau bagian alamat jaringan dari alamat IP unicast.
3. …… dicadangkan untuk alamat IP unicast.
4. CIDR adalah singkatan dari…….
5. Secara teknis, alamat IP dinyatakan menggunakan notasi biner dengan …… string panjang bit.

Nyatakan apakah pernyataan berikut ini benar atau Salah:

1. Kualitas layanan (QoS) jaringan komputer dievaluasi berdasarkan prioritas lalu lintas.
2. Bandwidth tidak berperan dalam memberikan kualitas layanan yang baik.
3. Model lalu lintas upaya terbaik menangani semua permintaan Internet dengan prioritas yang sama dan melayani permintaan tersebut dengan strategi siapa cepat dia dapat.
4. Alat manajemen kemacetan dapat mencakup antrian prioritas, antrian khusus, antrian adil tertimbang, dll.
5. Proses fragmentasi link dan interleave membagi paket kecil menjadi paket besar dengan menyisipkan paket suara.

6. Shaping digunakan untuk mencegah masalah overflow pada buffer dengan membatasi potensi bandwidth penuh dari paket aplikasi.

**Uraian**

1. Jelaskan Protokol IP. Apa bedanya dengan protokol TCP.
2. Apa alamat IP itu? Jelaskan format alamat IP.
3. Diskusikan pengalamatan IPV4 beserta klasifikasinya.
4. Jelaskan konsep subnetting.
5. Menjelaskan prinsip umum kemacetan.
6. Apa yang Anda pahami tentang QoS? Jelaskan struktur dasar QoS.
7. Diskusikan dua algoritma berikut:
   (a) Ember Bocor
   (b) Keranjang Token
8. Apa dua jenis pengendalian kemacetan? Dimana pengendalian kemacetan diterapkan pada setiap kasus?

# BAB 11
# LAPISAN TRANSPORTASI

**Pendahuluan**

Lapisan transport menghilangkan kekhawatiran lapisan atas dengan menyediakan transfer data yang andal dan hemat biaya. Ini memfasilitasi kontrol end-to-end dan pertukaran informasi dengan kualitas layanan yang dibutuhkan oleh program aplikasi. Jadi, lapisan keempat model referensi OSI adalah lapisan transport yang menyediakan transfer data transparan antara mesin sumber dan tujuan menggunakan layanan lapisan jaringan seperti IP. Hal ini memungkinkan layanan transportasi data internetworking yang andal dan transparan bagi lapisan atas. Protokol lapisan transport mengelola kontrol end-to-end dan pengecekan kesalahan untuk memastikan transfer data selesai. Fungsi yang disediakan pada lapisan ini adalah pemetaan alamat transport ke alamat jaringan, membuat multiplexing dan pemisahan koneksi transport, kontrol aliran, manajemen sirkuit virtual serta pengecekan dan pemulihan kesalahan. Tugas lapisan transport juga mencakup memecah pesan dari lapisan sesi menjadi beberapa segmen. Protokol lapisan transport termasuk Protokol Kontrol Transmisi (TCP), Protokol Datagram Pengguna (UDP), Protokol Pengikat Nama dan protokol transport OSI menyediakan transmisi berorientasi koneksi atau tanpa koneksi. Kualitas pelayanan juga merupakan salah satu fungsi dari lapisan transportasi.

## 11.1 PELAYANAN TRANSPORTASI

Fungsi dasar dari lapisan transport adalah untuk merespon permintaan layanan dari lapisan sesi dan mengeluarkan permintaan layanan ke lapisan jaringan. Untuk menyelesaikan tugas ini, ia menerima data dari lapisan sesi, membaginya menjadi unit-unit yang lebih kecil jika diperlukan, meneruskan unit-unit yang lebih kecil ini ke lapisan jaringan dan memastikan bahwa paket-paket data disusun kembali dengan benar di mesin tujuan. Lapisan transport melakukan indentasi untuk menjalankan semua fungsi ini secara efisien dan menjaga lapisan sesi tetap terisolasi dari perubahan yang diperlukan dalam teknologi perangkat keras. Lapisan transport menyediakan layanan berikut:

**Pelayanan yang Diberikan kepada Lapisan Atas**

Lapisan transport bersama dengan lapisan jaringan bertujuan untuk memberikan layanan yang efisien, andal, dan hemat biaya kepada penggunanya melalui proses di lapisan aplikasi. Perangkat lunak dan perangkat keras yang digunakan pada lapisan transport disebut entitas transport. Entitas transport terletak di kernel sistem operasi atau kartu antarmuka jaringan atau proses pengguna jarak jauh atau paket perpustakaan yang dimaksudkan untuk aplikasi jaringan.

Tahukah kamu? Seperti, lapisan jaringan, transport juga menyediakan layanan berorientasi koneksi dan tanpa koneksi. Dalam kondisi normal, dalam kedua kasus, koneksi dibuat untuk mentransfer data dan setelah transfer data berhasil, koneksi dilepaskan.

Lapisan transport membuat koneksi jaringan berbeda untuk koneksi transport yang diperlukan oleh lapisan sesi. Ketika koneksi transport memerlukan throughput yang tinggi,

lapisan transport membuat beberapa koneksi jaringan yang kemudian membagi data di antara beberapa koneksi jaringan untuk meningkatkan throughput. Ia juga mengatur bandwidth dan dengan demikian mengurangi biaya pembuatan koneksi. Ia melakukannya dengan multiplexing beberapa koneksi transport ke koneksi jaringan yang sama. Multiplexing selalu transparan terhadap lapisan sesi. Lapisan transparan ini mengisolasi lapisan atas dari teknologi, desain, dan ketidaksempurnaan subnet.

**Kualitas Pelayanan**

Lapisan transport menjembatani kesenjangan layanan yang disediakan oleh jaringan dan oleh karena itu meningkatkan kualitas layanan yang diberikan kepada pengguna. Parameter yang mungkin untuk kualitas layanan yang ditawarkan oleh lapisan transport adalah penundaan pembuatan sambungan, probabilitas kegagalan pembuatan sambungan, throughput, penundaan transit, rasio kesalahan sisa, prioritas perlindungan, ketahanan, dll.

Penundaan pembuatan koneksi: Ini adalah jumlah waktu ketika pengakuan diterima dari mesin tujuan yang dimintai koneksi. Tentu saja, semakin sedikit penundaannya, semakin baik layanannya.

Kemungkinan kegagalan pembuatan koneksi: Karena kemacetan dalam jaringan, kurangnya ketersediaan ruang dalam tabel, beberapa masalah internal, dll., menyebabkan koneksi tidak diatur dalam penundaan pembuatan.

- **Throughput**: Ini menentukan jumlah byte data pengguna yang ditransfer per detik dalam interval waktu yang ditentukan. Untuk setiap link komunikasi diukur secara terpisah.
- **Penundaan transit**: Ini adalah kesenjangan waktu antara data yang dikirimkan dari mesin sumber hingga penerimaan data yang sama oleh mesin tujuan. Seperti throughput, untuk setiap link komunikasi diukur secara terpisah.
- **Rasio kesalahan sisa**: Ini adalah bagian dari data yang hilang dibandingkan dengan total data yang dikirim melalui jaringan oleh mesin sumber.
- **Prioritas perlindungan**: Didefinisikan sebagai kemampuan lapisan transport untuk memberikan Perlindungan terhadap pihak ketiga yang mencoba mengganggu data. Ini menentukan prioritas sambungan-sambungan penting sehingga sambungan-sambungan berprioritas tinggi dilayani sebelum sambungan-sambungan berprioritas rendah jika terjadi kemacetan.
- **Ketahanan**: Ini adalah kemampuan lapisan transport untuk mengakhiri koneksi secara spontan jika terjadi kemacetan.

Lapisan transport tidak selalu dapat memenuhi seluruh parameter seperti yang disebutkan di atas. Ia mencoba menerapkan trade off antara parameter kualitas layanan. Proses ini disebut negosiasi opsi.

**Pelayanan Transportasi Primitif**

Mereka digunakan untuk mengakses layanan transportasi oleh lapisan aplikasi atau pengguna. Setiap layanan transportasi didefinisikan dengan primitif transportasi yang unik. Lapisan jaringan menyediakan layanan yang tidak dapat diandalkan sedangkan lapisan transport berupaya menyediakan layanan yang dapat diandalkan di atas layanan yang tidak

dapat diandalkan. Beberapa primitif transportasi adalah LISTEN, CONNECT, SEND, ACCEPTED dan RECEIVE.

Transport Protocol Data Unit (TPDU) adalah istilah yang digunakan untuk pertukaran data dari entitas transport ke entitas transport. TPDU terkandung dalam paket yang dipertukarkan oleh lapisan jaringan. Paket-paket tersebut kemudian dimasukkan ke dalam frame yang dipertukarkan oleh lapisan data link. Di mesin tujuan, ketika sebuah frame tiba, lapisan data link memproses header frame dan meneruskan konten bidang payload frame ke entitas jaringan. Proses serupa terjadi pada lapisan jaringan.

Situasi di atas dapat dipahami dari contoh, ketika mesin jarak jauh, misalnya, mesin klien meminta mesin lain, misalnya, server untuk koneksi. Mesin klien mengeluarkan TPDU CONNECT ke server. Server telah mengirimkan TPDU LISTEN ke jaringan untuk memblokir koneksi hingga mesin klien muncul. Saat menerima TPDU CONNECT, ia membuka blokir mesin server dan TPDU CONNECTION ACCEPTED dikirim kembali ke mesin klien dan dengan demikian koneksi dibuat dengan membuka blokir mesin klien juga. Setelah ini, primitif SEND dan RECEIVE memungkinkan pertukaran data.

Berikut adalah langkah-langkah yang diterapkan oleh mesin klien untuk membuat koneksi:

(a) Buat soket
(b) Hubungkan soket ke alamat mesin server
(c) Kirim/Terima data
(d) Tutup stopkontak

Berikut adalah langkah-langkah yang diterapkan oleh mesin server untuk membuat koneksi:

(1) Buat soket
(2) Ikat soket ke nomor port yang diketahui semua klien
(3) Dengarkan permintaan koneksi
(4) Terima permintaan koneksi
(5) Kirim/Terima data

## 11.2 ELEMEN PROTOKOL TRANSPORTASI

Untuk membangun layanan yang dapat diandalkan antara dua mesin pada jaringan, protokol transport diimplementasikan yang mirip dengan protokol data link yang diterapkan pada lapisan 2. Perbedaan utama terletak pada kenyataan bahwa lapisan data link menggunakan saluran fisik antara dua router sedangkan lapisan data link menggunakan saluran fisik antara dua router. lapisan transport menggunakan subnet. Berikut ini adalah permasalahan penerapan protokol transport:

※ **Jenis Layanan**: Lapisan transport juga menentukan jenis layanan yang diberikan kepada pengguna dari lapisan sesi. Komunikasi point-to-point yang bebas kesalahan untuk menyampaikan pesan sesuai urutan pengirimannya adalah salah satu fungsi utama dari lapisan transport. Namun, layanan tersebut mungkin dapat diandalkan atau dapat diandalkan dalam batas tertentu atau mungkin tidak dapat diandalkan seluruhnya. Urutan pesan yang diterima mungkin sama atau mungkin tidak sama

dengan urutan pengirimannya. Ketika koneksi dibuat antara dua proses, lapisan transport menentukan jenis layanan yang akan diberikan ke lapisan sesi pada saat itu.

※ **Pengendalian Kesalahan**: Deteksi kesalahan dan pemulihan kesalahan merupakan bagian integral dari layanan yang andal dan oleh karena itu diperlukan untuk melakukan mekanisme pengendalian kesalahan secara end-to-end. Untuk mengontrol kesalahan dari segmen yang hilang atau duplikat, lapisan transport mengaktifkan nomor urut segmen unik ke paket pesan yang berbeda, membuat sirkuit virtual, yang hanya mengizinkan satu sirkuit virtual per sesi. Mekanisme timeout juga digunakan untuk menghapus paket dari segmen jaringan yang salah rute dan tetap berada di jaringan melebihi waktu yang ditentukan. Kontrol kesalahan ujung ke ujung menggunakan checksum juga digunakan untuk menangani kerusakan data.

※ **Kontrol Aliran**: Aturan mendasar dari kontrol aliran adalah menjaga sinergi antara proses yang cepat dan proses yang lambat. Lapisan transport memungkinkan proses yang cepat mengimbangi proses yang lambat. Ucapan terima kasih dikirim kembali untuk mengelola kontrol aliran end-to-end. Algoritma Go back N digunakan untuk meminta pengiriman ulang paket yang dimulai dengan nomor paket N. Selective Repeat digunakan untuk meminta paket tertentu untuk dikirim ulang.

※ **Pembuatan/Pelepasan Koneksi**: Lapisan transport membuat dan melepaskan koneksi di seluruh jaringan. Hal ini mencakup mekanisme penamaan sehingga suatu proses pada satu mesin dapat menunjukkan dengan siapa ia ingin berkomunikasi. Lapisan transport memungkinkan untuk membuat dan menghapus koneksi di seluruh jaringan untuk melakukan multiplexing beberapa aliran pesan ke satu saluran komunikasi.

※ **Multiplexing/Demultiplexing**: Lapisan transport membuat koneksi jaringan terpisah untuk setiap koneksi transport yang diperlukan oleh lapisan sesi. Untuk meningkatkan throughput, lapisan transport membuat beberapa koneksi jaringan. Ketika masalah throughput tidak penting, maka beberapa koneksi transport akan dimultipleks ke dalam koneksi jaringan yang sama, sehingga mengurangi biaya untuk membangun dan memelihara koneksi jaringan. Ketika beberapa koneksi dimultipleks, mereka memerlukan demultiplexing di pihak penerima. Dalam kasus lapisan transport, komunikasi hanya terjadi antara dua proses dan bukan antara dua mesin. Oleh karena itu, komunikasi pada lapisan transport juga dikenal sebagai komunikasi peer-to-peer atau proses-ke-proses.

※ **Fragmentasi dan perakitan ulang**: Ketika lapisan transport menerima pesan besar dari lapisan sesi, pesan tersebut dipecah menjadi unit-unit yang lebih kecil tergantung pada kebutuhan. Proses ini disebut fragmentasi. Setelah itu, diteruskan ke lapisan jaringan. Sebaliknya, ketika lapisan transport bertindak sebagai proses penerima, ia menyusun ulang potongan-potongan pesan sebelum menyusunnya kembali menjadi sebuah pesan.

※ **Pengalamatan**: Transport Layer berkaitan dengan pengalamatan atau pelabelan sebuah frame. Ini juga membedakan antara koneksi dan transaksi. Pengidentifikasi koneksi adalah port atau soket yang memberi label pada setiap frame sehingga

perangkat penerima mengetahui dari proses mana frame tersebut dikirim. Ini membantu melacak percakapan banyak pesan. Port atau soket mengatasi banyak konservasi di lokasi yang sama. Misalnya, baris pertama alamat pos dianalogikan dengan port dan membedakan beberapa penghuni rumah yang sama. Aplikasi komputer mendengarkan informasi pada portnya sendiri dan oleh karena itu lebih dari satu aplikasi berbasis jaringan dapat digunakan pada saat yang bersamaan. Pengidentifikasi transaksi menangani bingkai permintaan atau respons. Itu adalah peristiwa yang terjadi satu kali saja.

## 11.3 PROTOKOL TRANSPORTASI SEDERHANA

Beberapa contohnya adalah:

- ✓ Contoh Layanan Primitif
- ✓ Contoh Entitas Transportasi
- ✓ Contoh sebagai Mesin Keadaan Hingga

**Contoh Layanan Primitif**

Primitif layanan abstrak yang juga disebut sebagai panggilan sistem berorientasi pada koneksi seperti DENGARKAN, SAMBUNGKAN, KIRIM, TERIMA, dan PUTUSKAN. Berikut ini adalah daftarnya beserta fungsinya:

(1) **DENGARKAN**: Menyiarkan kesediaan untuk menerima koneksi dan memberikan ukuran antrian.
(2) **TERIMA**: Blokir penelepon kecuali ada upaya komunikasi.
(3) **CONNECT**: Secara aktif mencoba membuat koneksi.
(4) **KIRIM**: Mengirim data melalui koneksi.
(5) **MENERIMA**: Menerima data dari koneksi.
(6) **TUTUP**: Lepaskan koneksi.

Dalam arsitektur server klien, suatu mesin (klien) meminta ke mesin lain (server) untuk membuat koneksi guna menyediakan beberapa layanan. Layanan yang berjalan di server berjalan di port. Port adalah pengidentifikasi aplikasi. Mesin klien harus mengetahui alamat mesin server untuk mendapatkan layanan yang diinginkan dari port ini dan untuk terhubung ke mesin server. Namun, mesin server tidak boleh mengetahui alamat atau port mesin klien pada saat inisiasi koneksi. Paket pertama yang dikirimkan oleh mesin klien sebagai permintaan ke mesin server berisi rincian tentang klien yang selanjutnya digunakan oleh server untuk mengirimkan informasi apa pun. Mesin klien bertindak sebagai perangkat aktif yang mengambil langkah pertama untuk membuat koneksi sedangkan mesin server secara pasif menunggu permintaan tersebut dari beberapa klien.

**Contoh Entitas Transportasi**

Lapisan transport menggunakan primitif lapisan jaringan untuk mengirim dan menerima TPDU. Entitas transportasi berada di:

- kernel sistem operasi host,
- proses pengguna terpisah,
- paket rutinitas perpustakaan yang berjalan dalam ruang alamat pengguna, atau

- chip co-prosesor atau papan jaringan yang dicolokkan ke backplane host. Antarmuka ke lapisan jaringan diberikan seperti di bawah ini: to_net(int cid, int q, int m, pkt_type pt, unsigned char *p, int byte); from_net(int *cid, int *q, int *m, pkt_type *pt, unsigned char *p, int *bytes); Paket lapisan jaringan yang digunakan diberikan di bawah ini:
  - **Permintaan Panggilan**: Dikirim untuk membuat sambungan
  - **Panggilan Diterima**: Respon terhadap PERMINTAAN PANGGILAN
  - **Clear Request**: Dikirim untuk melepaskan koneksi
  - **Konfirmasi Clear:** Respons terhadap PERMINTAAN CLEAR
  - **Data**: Digunakan untuk mengangkut data
  - **Kredit**: Paket kontrol untuk mengelola jendela

Ketika informasi dilewatkan sebagai parameter prosedur dan bukan sebagai paket keluar atau masuk yang sebenarnya, lapisan transport dilindungi dari rincian protokol lapisan jaringan. Entitas transport ditangguhkan secara transparan dalam to_net hingga ada ruang di jendela. Terlepas dari mekanisme penangguhan yang transparan ini, beberapa prosedur eksplisit yang diminta oleh entitas transport untuk memblokir/membuka blokir itu sendiri diberikan di atas:

- **sleep**() – Prosedur ini dipanggil ketika entitas transport secara logis perlu menunggu kejadian eksternal terjadi. Setelah memanggil prosedur tidur, entitas transport (aliran utama) diblokir.
- **wakeup**() – Prosedur ini dipanggil oleh prosedur penanganan kejadian (yaitu packet_arrival() ); - Untuk membuka blokir entitas transportasi yang sedang tidur (aliran utama).

Program pengguna memanggil sebagian besar prosedur di entitas transport secara langsung. Namun, ada dua prosedur yang secara efektif (perangkat lunak) mengganggu rutinitas dan dipanggil hanya ketika aliran utama entitas transportasi sedang tidur. Mereka diberikan seperti di bawah ini:

- packet_arrival() – Ini dipicu oleh kejadian kedatangan paket. Lapisan jaringan yang mendasarinya membuat prosedur ini.
- clock() – Peristiwa detak jam memicu prosedur ini.

Mekanisme kontrol aliran berdasarkan kredit digunakan dalam contoh entitas transportasi:

- Saat aplikasi memanggil RECEIVE, pesan kredit khusus dikirim ke entitas transport pada mesin sumber dan dicatat dalam array samb.
- Saat SEND dipanggil, entitas transport memeriksa apakah kredit telah diterima pada koneksi yang ditentukan.
  - Jika demikian, pesan dikirimkan dalam beberapa paket, jika diperlukan, dan kredit dikurangi;
  - Jika tidak, entitas transportasi mengubah dirinya menjadi tidur sampai kredit diterima.

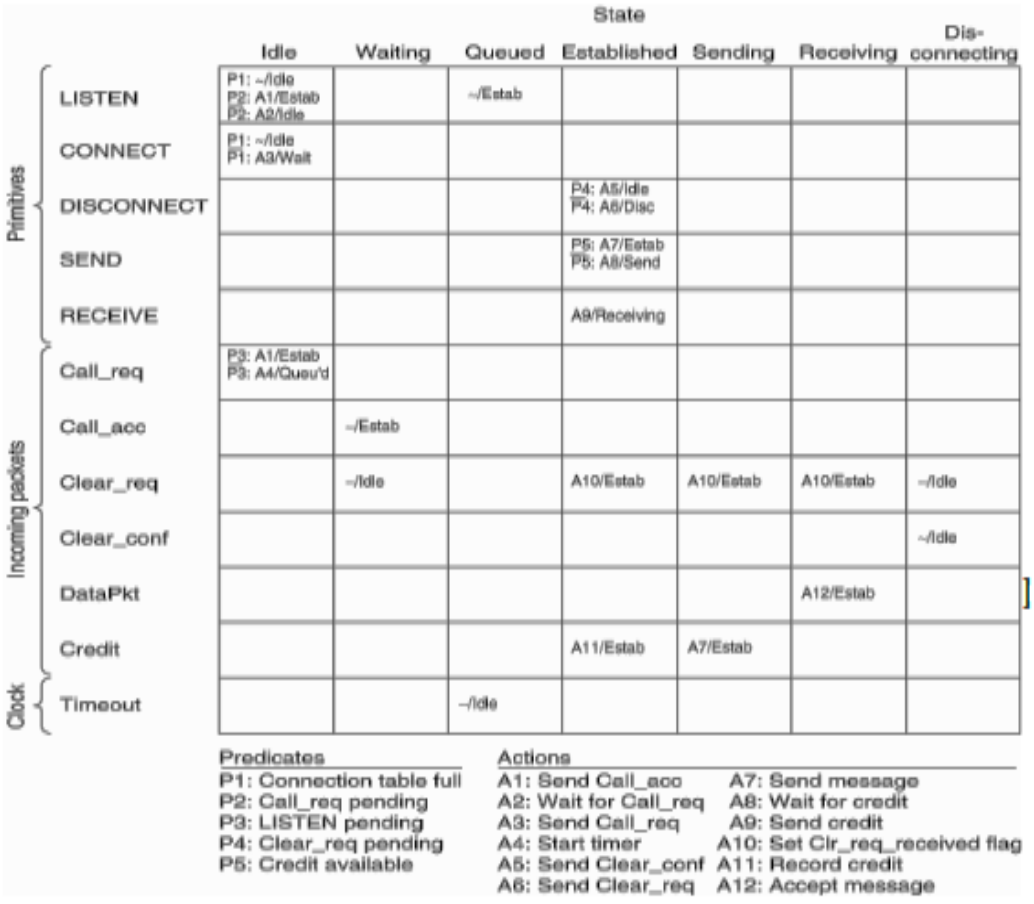
Dalam entitas transport, setiap koneksi dinyatakan dalam salah satu dari tujuh keadaan berikut:

(a) Idle : koneksi belum terjalin.
(b) Menunggu : connect telah dijalankan, call request terkirim.

(c) Antri : permintaan panggilan telah tiba; belum ada dengarkan.
(d) Didirikan :koneksi telah dibuat.
(e) Mengirim : pengguna sedang menunggu izin untuk mengirim paket.
(f) Menerima :penerimaan telah dilakukan.
(g) Memutuskan :pemutusan telah dilakukan secara lokal.

**Contoh sebagai Mesin Keadaan Hingga**

Gambar 11.1 menunjukkan contoh mesin keadaan terbatas. Dalam mesin keadaan terbatas, setiap entri mempunyai predikat opsional, tindakan opsional, dan keadaan baru. Protokol utama dari Transport Layer adalah *Transmisi Control Protocol* (TCP) dan *User Datagram Protocol* (UDP). TCP memungkinkan layanan pengiriman data yang andal dengan deteksi dan koreksi kesalahan ujung ke ujung. UDP memfasilitasi layanan pengiriman datagram dengan overhead rendah dan tanpa koneksi. Kedua protokol tersebut bertanggung jawab untuk mengirimkan data antara lapisan sesi dan lapisan jaringan.



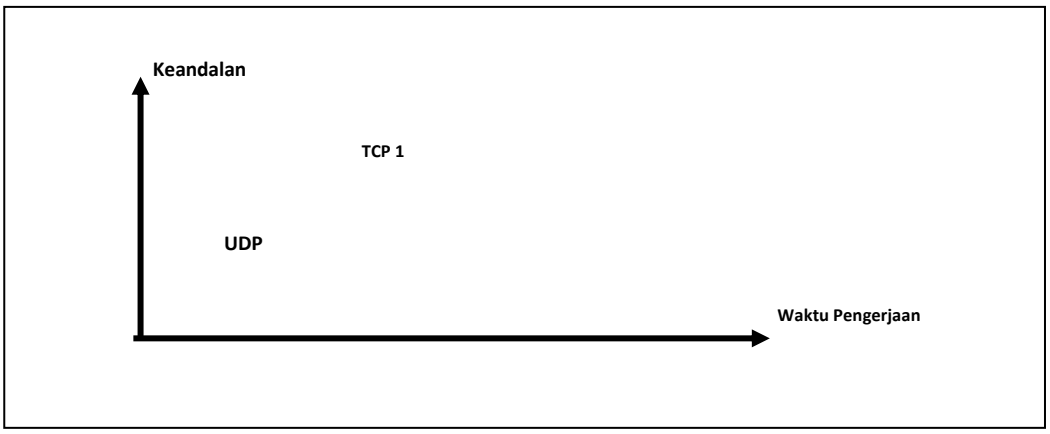

**Gambar 11.1 Contoh Finite State Model**

**Protokol Datagram Pengguna (UDP)**

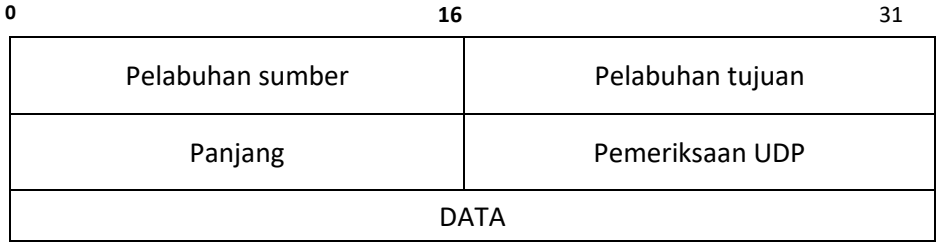
Protokol Datagram Pengguna memungkinkan program aplikasi memiliki akses langsung ke layanan pengiriman datagram seperti layanan pengiriman yang disediakan IP. Hal ini memungkinkan aplikasi untuk bertukar pesan melalui jaringan dengan overhead protokol minimum. UDP adalah protokol datagram connectionless yang tidak dapat diandalkan dimana

terminal pengirim tidak memeriksa apakah data telah diterima oleh terminal penerima. Layanan yang tidak dapat diandalkan menunjukkan bahwa tidak ada jaminan bahwa data sampai ke ujung jaringan penerima dengan benar. Lebih jelasnya dapat dipahami pada Gambar 11.2.

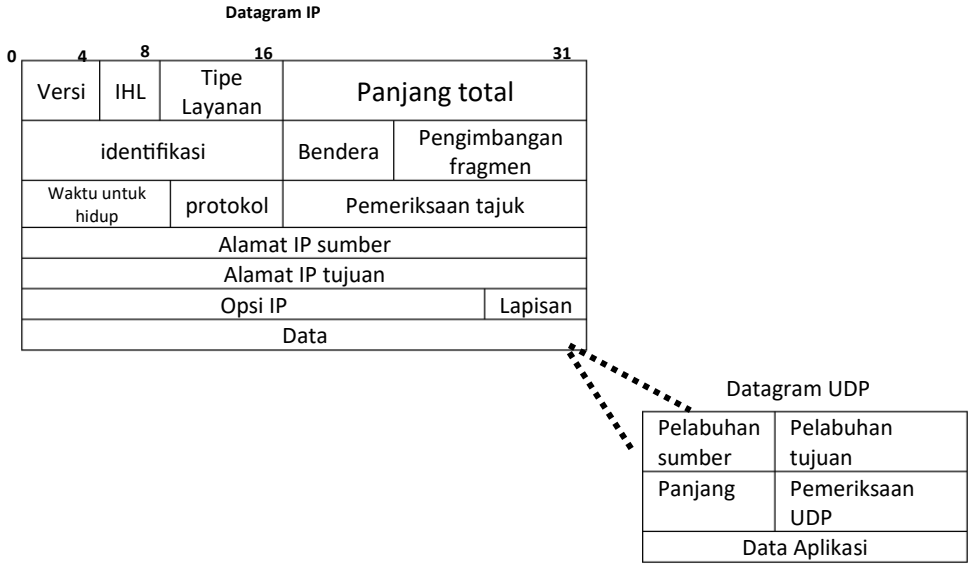
Namun, protokol ini memungkinkan untuk menghilangkan berbagai proses sehingga mengurangi beban pada CPU. UDP memiliki nomor Port Sumber dan Port Tujuan 16-bit. Gambar 11.3 menunjukkan struktur data header UDP. Kesederhanaan header UDP berasal dari sifat sederhana dari layanan yang disediakannya.




**Gambar 11.2 Perbandingan antara TCP dan UDP**




**Gambar 11.3 Format Datagram UDP**




**Gambar 11.4 korespondensi antara datagram UDP dan IP**

Berikut penjelasan singkat masing-masing bidang:

(a) Port Sumber: Port sumber menentukan nomor port aplikasi yang berkaitan dengan data pengguna.
(b) Pelabuhan Tujuan: Sesuai dengan namanya, ini berkaitan dengan aplikasi tujuan.
(c) Panjang: Ini menggambarkan panjang total datagram UDP, termasuk data dan informasi header.
(d) UDP Checksum: Ini memberikan opsi pemeriksaan integritas.

Pada titik ini, penting untuk memahami konsep layering serta kebutuhan akan header. Hubungan antara IP dan UDP telah digambarkan pada Gambar 11.4.

Catatan Ada sejumlah alasan bagus untuk memilih UDP sebagai layanan transportasi data. Ketika jumlah data yang dikirimkan sedikit, UDP dianggap sebagai pilihan yang paling efisien untuk protokol lapisan transport karena biaya overhead untuk membangun koneksi dan memastikan pengiriman yang andal mungkin lebih besar daripada pekerjaan transmisi ulang seluruh data. Aplikasi untuk model respons-kueri juga bekerja sangat baik untuk menggunakan UDP. Responsnya digunakan sebagai pengakuan positif terhadap kueri. Ketika respons tidak diterima dalam jangka waktu tertentu, aplikasi memulai kueri lain. Beberapa contoh penggunaan UDP adalah Remote file server (NFS), terjemahan nama (DNS), intra-domain routing (RIP), manajemen jaringan (SNMP), aplikasi multimedia dan telepon.

**Protokol Kontrol Transmisi**

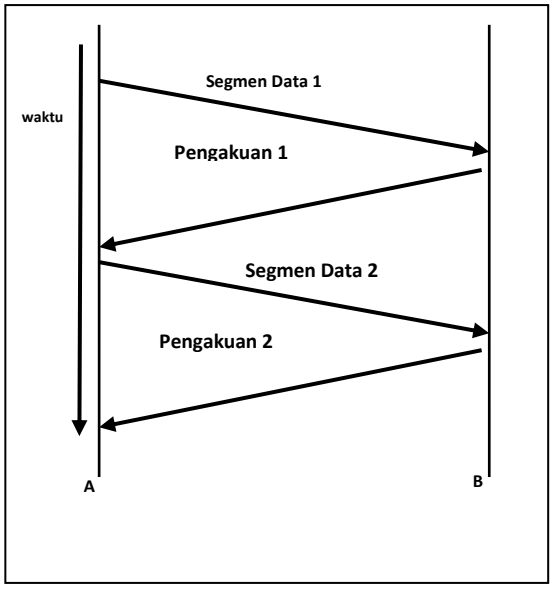
Protokol Kontrol Transmisi (TCP) dirancang untuk menyediakan transfer data end-to-end yang andal melalui internetwork yang tidak dapat diandalkan di mana TCP mengadaptasi properti internetwork secara dinamis. Internetwork mungkin memiliki topologi, bandwidth, throughput, penundaan, ukuran paket, dll yang berbeda untuk jaringan berbeda yang membangun internetwork. Setiap mesin yang mendukung TCP memiliki entitas TCP yang menerima aliran data pengguna dari proses lokal dan memecahnya menjadi beberapa bagian yang tidak melebihi 64k byte untuk mengirimkan setiap bagian sebagai datagram IP terpisah.

**Model Layanan TCP**

Model layanan TCP terdiri dari soket, yang digunakan untuk membuat titik akhir untuk layanan TCP di mesin host. Ini menentukan format pengalamatan, jenis layanan dan protokol. Setiap soket memiliki nomor soket yang terdiri dari alamat IP host dan nomor 16-bit lokal ke host tersebut yang disebut sebagai port. Beberapa port yang terkenal adalah 21 untuk FTP, 23 untuk telnet, 25 untuk SMTP, 79 untuk finger, 80 untuk HTTP, dll. TCP menyediakan layanan jenis koneksi dengan koneksi full duplex point-to-point. Artinya, koneksi logis harus dibuat sebelum komunikasi. Koneksi TCP adalah aliran byte, bukan aliran pesan. Ukuran segmen TCP ditentukan oleh Unit Transfer Maksimum (MTU) jaringan, yang umumnya terdiri dari 1500 byte. Oleh karena itu, transmisi data dalam jumlah besar dapat dilakukan secara terus-menerus. Ini memastikan transmisi data yang sangat andal untuk lapisan atas menggunakan protokol IP. Hal ini dimungkinkan karena TCP menggunakan pengakuan positif untuk mengkonfirmasi pengirim tentang penerimaan data yang tepat seperti yang ditunjukkan pada Gambar 11.5. Pengirim terus mengirimkan data pada interval yang konstan hingga menerima

pengakuan positif. Pengakuan negatif menyiratkan bahwa segmen data yang gagal perlu dikirim ulang.

Apa yang terjadi jika sebuah paket hilang di jaringan dan gagal mencapai tujuan akhirnya? Ketika host A mengirimkan data, ia memulai penghitung waktu habis. Jika penghitung waktu berakhir tanpa menerima pengakuan, host A berasumsi bahwa segmen data telah hilang. Akibatnya, komputer pengirim mengirimkan ulang duplikat segmen yang gagal. Protokol TCP menggunakan protokol jendela geser. Fungsi lainnya termasuk kontrol urutan, pemulihan dan kontrol kesalahan, kontrol aliran dan identifikasi nomor port. TCP memiliki fungsi untuk menangani data mendesak atau prioritas. Ketika beberapa data penting diterima, proses yang sedang berlangsung pada mesin penerima diinterupsi dan diinstruksikan untuk membaca aliran data untuk menemukan data penting tersebut. Akhir dari data yang mendesak selalu ditandai, sehingga proses mengetahui bahwa itu telah berakhir.




**Gambar 11.5 Model Layanan TCP**

Gambar 11.6 menunjukkan format segmen data TCP. Header TCP mencakup bidang port sumber dan tujuan untuk mengidentifikasi aplikasi yang sambungannya dibuat. Bidang urutan dan nomor pengakuan mendasari teknik pengakuan positif dan transmisi ulang. Pemeriksaan integritas diakomodasi menggunakan kolom checksum. Oleh karena itu, TCP, tidak seperti UDP, TCP adalah protokol aliran byte berorientasi koneksi yang andal.

**Protokol TCP**

Setiap byte pada koneksi TCP terdiri dari nomor urut 32-bitnya sendiri. Entitas TCP pengirim dan penerima mentransfer data dalam segmen, yang ditentukan oleh perangkat lunak TCP. Segmen TCP memiliki header tetap 20-byte diikuti oleh nol atau lebih byte data. Fungsionalitas TCP mendukung agregasi data dari beberapa penulisan menjadi satu segmen atau memisahkan data dari satu penulisan ke beberapa segmen. Segmen TCP harus sedemikian rupa sehingga sesuai dengan MTU setiap jaringan. Ketika segmen TCP ditransmisikan, pengatur waktu juga diatur. Jika timer segmen TCP berbunyi sebelum

pengakuan diterima, pengirim mengirimkan segmen tersebut lagi. Oleh karena itu dikatakan bahwa TCP adalah pengiriman end-to-end yang dapat diandalkan.

- **Andal:** TCP menyediakan pengiriman data yang andal menggunakan mekanisme Pengakuan Positif dengan Transmisi Ulang (PAR). PAR adalah mekanisme dimana data dikirimkan berulang kali hingga sistem jarak jauh mendengar bahwa data telah sampai dengan benar. Unit data yang dipertukarkan antara host sumber dan tujuan disebut segmen seperti yang ditunjukkan pada Gambar 11.6. Jelas dari Gambar 11.6 bahwa setiap segmen memiliki checksum untuk memverifikasi bahwa data tiba di tujuan tanpa kerusakan. Ketika segmen data diterima tanpa kerusakan, penerima mengirimkan pengakuan positif kembali ke sumbernya. Ketika segmen data rusak, mesin tujuan akan membuangnya. Ketika mesin sumber tidak menerima pengakuan positif apa pun dalam periode waktu habis yang ditentukan, mesin tersebut mentransmisikan ulang segmen data.
- **Berorientasi koneksi**: TCP membuat koneksi logis end-to-end antara host sumber dan tujuan. Jabat tangan yaitu pertukaran informasi kontrol antara host sumber dan tujuan untuk mengatur dialog sebelum data dikirim. TCP menunjukkan fungsi kontrol dalam suatu segmen dengan mengatur bendera di bidang Bendera di header segmen. TCP menggunakan jabat tangan tiga arah yang menunjukkan bahwa tiga segmen dipertukarkan. Gambar 11.7 menggambarkan bentuk paling sederhana dari jabat tangan tiga arah. Host A memulai koneksi dengan mengirimkan segmen ke host B dengan set bit "Sinkronisasi nomor urut" (SYN). Segmen ini menunjukkan kepada host B bahwa host A meminta untuk membuat koneksi. Segmen tersebut juga menunjukkan kepada host B nomor urut yang akan digunakan host A sebagai nomor awal untuk segmennya sehingga data dapat disusun dalam urutan yang benar. Host B membalas host A dengan segmen yang memiliki set bit “Pengakuan” (ACK) dan SYN. Segmen Host B mengakui penerimaan segmen A dan memberi tahu host A Nomor Urutan host B akan dimulai. Terakhir, host A mentransmisikan segmen yang mengakui penerimaan segmen host B. Jadi, host A mentransfer data aktual pertama.

Pertukaran data ini juga menandakan bahwa TCP host A mempunyai indikasi bahwa TCP jarak jauh aktif dan siap menerima data. Ketika koneksi dibuat, data dapat dipertukarkan. Segera setelah mesin sumber dan tujuan menyelesaikan pertukaran data, mereka memulai jabat tangan tiga arah dengan segmen yang berisi bit “Tidak ada lagi data dari pengirim” (disebut bit FIN) untuk melepaskan koneksi. Dengan demikian, pertukaran data end-to-end menggunakan koneksi logis antara mesin sumber dan host dapat dicapai.

**Tajuk Segmen TCP**

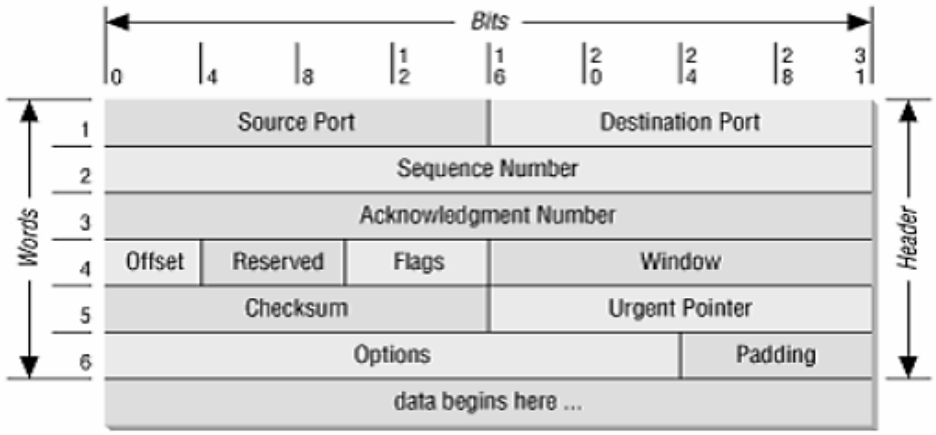
Gambar 11.6 menunjukkan tata letak segmen TCP:

- Nomor Pelabuhan Sumber dan Tujuan (Soket): Keduanya bersama-sama mengidentifikasi koneksi antara dua host.
- Nomor Urutan dan Pengakuan: Bidang ini menjalankan fungsinya dan panjangnya 32 bit karena setiap byte data diberi nomor dalam aliran TCP.

- Panjang header TCP: Ini menunjukkan berapa banyak kata 32-bit yang terkandung dalam header TCP.
- Option Field: Panjangnya bervariasi dan mencakup panjang header TCP.

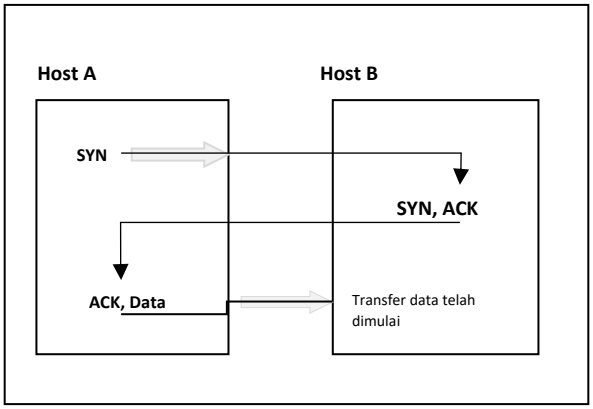
Header segmen juga menyertakan enam flag 1 bit. Setiap bit menunjukkan URG, ACK PSH, RST, SYN dan FIN. Bidang bendera URG diatur ke 1 jika Penunjuk Urgent sedang digunakan, yang menunjukkan byte, offset dari nomor urut saat ini di mana data mendesak dapat ditemukan. Bit ACK diatur ke 1 untuk menunjukkan bahwa nomor Pengakuan valid. Jika ACK bernilai 0, hal ini menunjukkan bahwa segmen tersebut tidak berisi pengakuan sehingga field Nomor pengakuan diabaikan.

PSH mengindikasikan untuk mendorong data ke suatu proses pada saat kedatangan dan tidak melakukan buffering sampai buffer penuh telah diterima. Bit RST digunakan untuk menolak akses ke segmen yang tidak valid atau menolak upaya untuk membuka koneksi. Terkadang karena hot crash atau alasan lain, permintaan koneksi tidak jelas. Bit SYN membuat koneksi, jika diatur ke 1. Bit FIN menunjukkan pelepasan koneksi setelah selesainya transmisi data. Segmen SYN dan FIN memiliki nomor urut dan karenanya diproses dalam urutan yang benar.




**Gambar 11.6 Format Segmen Data pada Protokol TCP**

- **Aliran Byte Berkelanjutan**: TCP menganggap data yang dikirimkannya sebagai aliran byte yang berkelanjutan, bukan sebagai paket independen. Hal ini mengharuskan TCP untuk berhati-hati dalam menjaga urutan byte yang dikirim dan diterima. Bidang nomor urut dan nomor pengakuan di header segmen TCP melacak byte. Untuk melacak aliran data dengan benar, setiap akhir proses diharuskan mengetahui nomor awal ujung lainnya. Ujung sumber dan tujuan dari proses menyinkronkan sistem penomoran byte dengan menukar segmen SYN selama jabat tangan. Bidang nomor urut di segmen SYN memiliki Nomor Urutan Awal (ISN). Ini dianggap sebagai titik awal untuk sistem penomoran byte. Setelah itu, setiap byte data diberi nomor secara berurutan dari ISN dimulai dengan ISN+1 untuk byte data nyata pertama yang akan dikirim.




**Gambar 11.7 Handshake Tiga arah**

Kontrol aliran di TCP ditangani dengan menggunakan protokol jendela geser ukuran variabel. Bidang jendela menunjukkan berapa banyak byte yang dapat dikirim mulai dari pengakuan byte. Segmen pengakuan (ACK) memiliki fungsi pengakuan positif dan kontrol aliran. Pengakuan menunjukkan kepada pengirim jumlah data yang diterima dan data yang dapat diterima selanjutnya. Nomor pengakuan adalah nomor urut byte berikutnya yang akan diterima penerima.

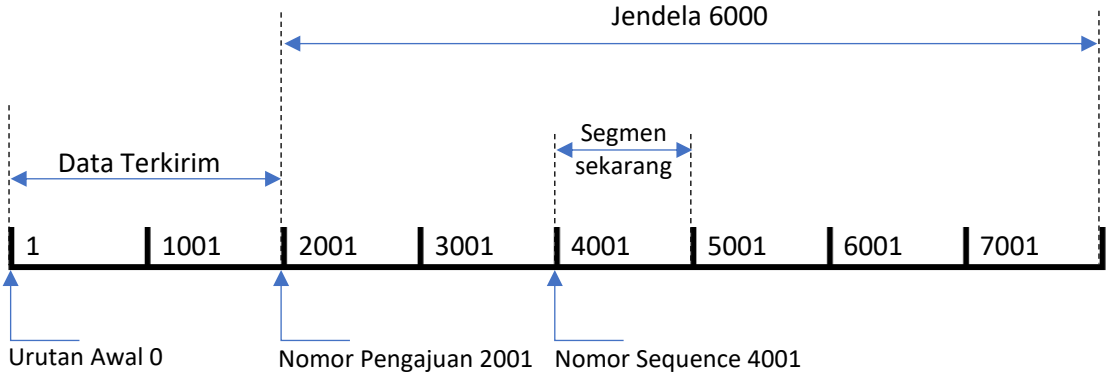
Gambar 11.8 mengilustrasikan aliran data TCP yang dimulai dengan ISN 0. Mesin tujuan telah menerima dan mengakui 2000 byte. Oleh karena itu, nomor pengakuan saat ini adalah 2001. Mesin tujuan memiliki ruang buffer yang cukup untuk 6000 byte berikutnya. Mesin sumber saat ini sedang mentransmisikan segmen 1000 byte yang dimulai dengan nomor urut 4001. Mesin sumber tidak menerima pengakuan untuk byte tersebut mulai tahun 2001 dan seterusnya, namun terus mentransmisikan data selama berada di dalam jendela. Ketika mesin sumber memenuhi jendela dan tidak menerima pengakuan atas data yang dikirim sebelumnya, setelah waktu habis, mesin akan mengirimkan data lagi mulai dari byte pertama yang tidak diakui. Pada Gambar 11.8 transmisi ulang dimulai dari byte 2001 ketika tidak ada pengakuan lebih lanjut yang diterima. Hal ini membuat mesin sumber percaya bahwa data diterima dengan andal di lokasi jaringan yang jauh.

TCP juga memastikan pengiriman data yang diterima dari IP ke aplikasi yang benar. Nomor port 16-bit mengidentifikasi aplikasi. Port mesin sumber dan mesin tujuan disertakan dalam kata pertama header segmen. Dengan demikian, lapisan transport meneruskan data ke dan dari lapisan aplikasi dengan benar.

**Manajemen Koneksi TCP**

Jabat tangan tiga arah digunakan untuk membuat koneksi TCP di mana mesin host menjalankan primitif CONNECT, menentukan alamat IP dan port yang memerlukan koneksi, ukuran segmen TCP maksimum yang bersedia diterima dan opsional beberapa data pengguna. Primitif CONNECT meneruskan segmen TCP dengan bit SYN disetel ke 1 dan bit ACK disetel ke 0 dan menunggu respons. Urutan kejadian diilustrasikan pada Gambar 11.8. Entitas TCP di tujuan memeriksa segmen tersebut ketika mencapai tujuan untuk memastikan apakah ada proses yang telah melakukan LISTEN pada port yang disediakan di kolom Destination Port. Jika

tidak, ia akan mengirimkan balasan dengan bit RST aktif untuk menolak koneksi. Koneksi TCP bersifat dupleks penuh, yang dapat dianggap sebagai sepasang koneksi simpleks.



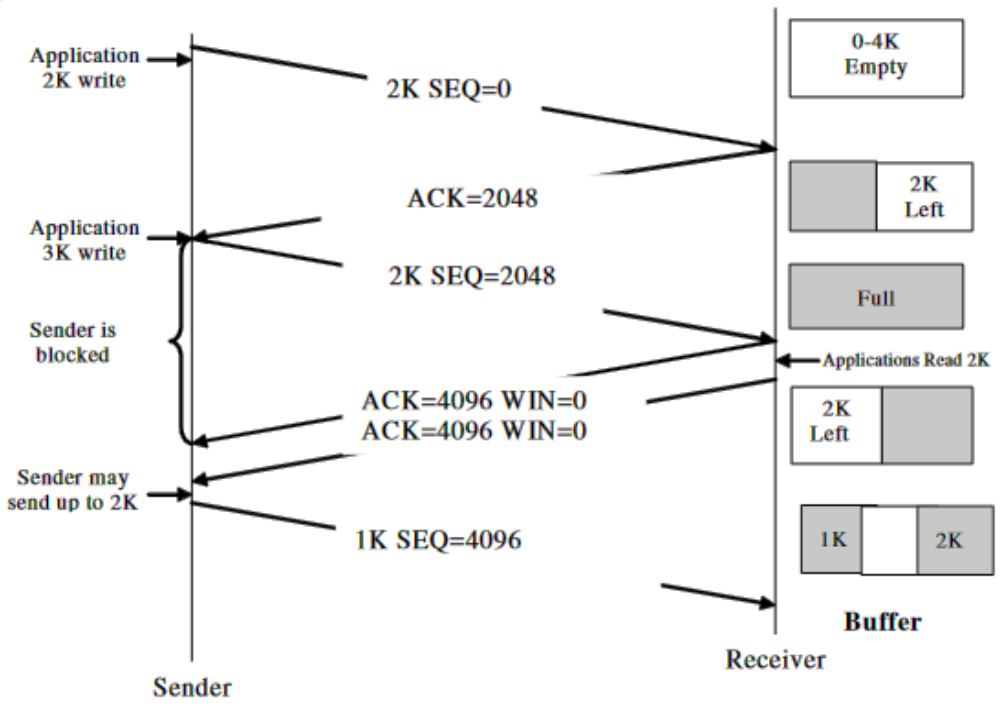

**Gambar 11.8 Data Stream TCP**

Segmen TCP dengan bit FIN yang disetel ke 0 dikirim oleh salah satu host untuk melepaskan koneksi ketika host tersebut selesai mengirimkan data. Dengan pengakuan FIN, koneksi point-to-point dari sisi transmisi ditutup. Namun, data mungkin terus mengalir ke arah lain tanpa batas waktu. Ketika kedua arah dimatikan, sambungan dilepaskan. Untuk menghindari penundaan yang tidak perlu dalam menerima pengakuan, digunakan pengatur waktu. Ketika respons terhadap FIN tidak datang dalam dua masa pakai paket maksimum, pengirim FIN melepaskan koneksi. Akhirnya, pembawa acara lainnya menyadari bahwa sepertinya tidak ada lagi yang mendengarkannya dan pembawa acara tersebut juga time out. Prosedur yang diikuti untuk melepaskan dan membuat sambungan direpresentasikan sebagai berikut:

| No. | Pernyataan | Keterangan |
|---|---|---|
| 1 | TERTUTUP | Menunjukkan tidak ada koneksi yang aktif atau tertunda. |
| 2 | MENDENGARKAN | Server sedang menunggu panggilan masuk. |
| 3 | SYN DITERIMA | Permintaan koneksi telah tiba; menunggu pengakuan. |
| 4 | SYN DIKIRIM | Aplikasi atau proses sudah mulai membuka koneksi. |
| 5 | DIDIRIKAN | Menunjukkan status transfer data normal. |
| 6 | SIRIP TUNGGU 1 | Proses atau aplikasi telah selesai. |
| 7 | SIRIP TUNGGU 2 | Tuan rumah setuju untuk melepaskan koneksi tersebut. |
| 8 | WAKTU TUNGGU | Menandakan menunggu hingga semua paket mati. |
| 9 | PENUTUPAN | Menunjukkan bahwa kedua host telah berusaha menutup secara bersamaan. |
| 10 | TUTUP TUNGGU | Salah satu host telah memulai rilis. |
| 11 | ACK TERAKHIR | Menandakan menunggu hingga semua paket mati. |

**Kebijakan Transmisi TCP**

Manajemen jendela di TCP tidak berhubungan langsung dengan pengakuan. Ketika jendela diatur ke 0, mesin host di ujung pengirim biasanya tidak mengirim segmen. Kita dapat mempertimbangkan contoh di mana host penerima memiliki buffer 4096-byte dan host pengirim mengirimkan segmen 2048-byte. Segmen 2048-byte diterima dengan benar dan host penerima mengakui segmen tersebut. Namun, buffer tersisa dengan hanya 2048 ruang buffer dan host di sisi penerima mengumumkan jendela 2048 byte dimulai dari byte berikutnya yang diharapkan. Sekarang host di pihak pengirim mengirimkan 2048 byte lagi, yang diakui dan jendela yang diiklankan adalah 0. Host di pihak pengirim harus berhenti sampai proses aplikasi pada host di pihak penerima telah menghapus beberapa data dari buffer sehingga TCP dapat mengiklankan jendela yang lebih besar. Hal ini diamati jika jendelanya nol, host di sisi pengirim mungkin tidak mengirimkan segmen. Ada dua pengecualian. Salah satunya terkait data mendesak yang mungkin dikirimkan. Contoh data yang mendesak adalah mengaktifkan mesin host untuk menyelesaikan proses yang berjalan pada mesin host jarak jauh. Gambar 11.9 mengilustrasikan konsep ini.

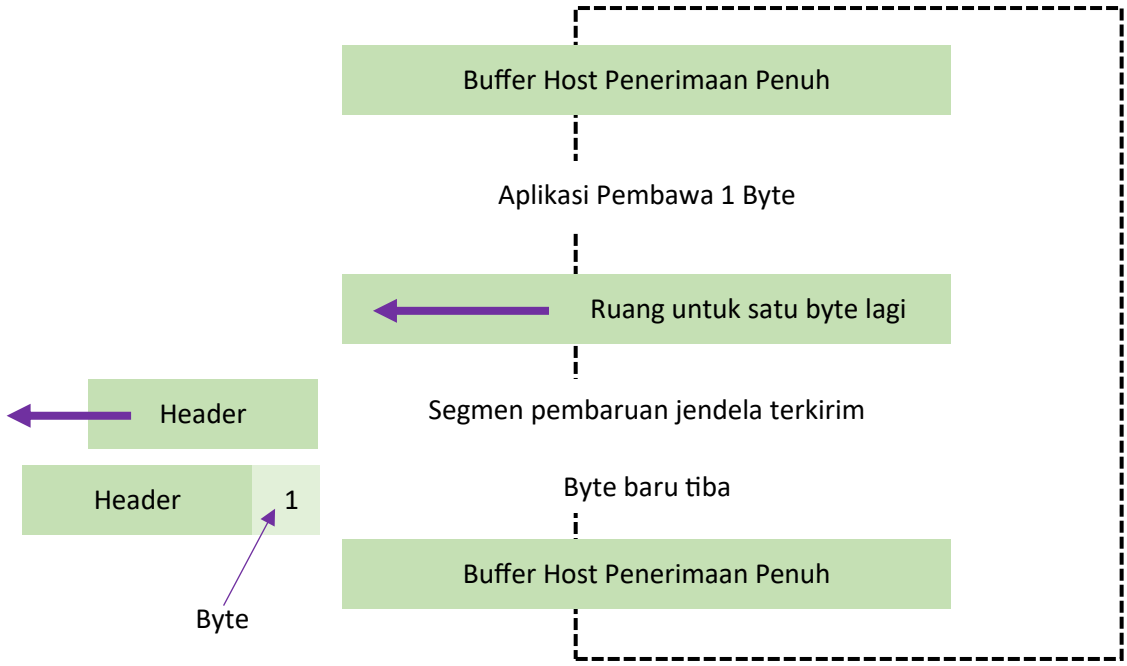



**Gambar 11.9 Jendela Manajemen dalam TCP**

Pengecualian lainnya adalah mesin host pada saat pengiriman dapat mengirimkan segmen 1-byte untuk membuat penerima mengumumkan kembali byte berikutnya yang diharapkan dan ukuran jendela. Hal ini cukup penting untuk mencegah kebuntuan jika pengumuman jendela hilang. Pengirim tidak diharuskan mengirimkan data segera ketika muncul dari aplikasi demikian pula mesin host jarak jauh tidak diharuskan mengirimkan pengakuan sesegera mungkin. Misalnya, pertimbangkan koneksi telnet ke editor interaktif yang bereaksi terhadap setiap penekanan tombol.

Dalam kasus terburuk, jika sebuah karakter tiba di perangkat lunak TCP, segmen TCP 21-byte diberikan kepada IP untuk dikirim sebagai datagram 41-byte. Pada mesin host jarak jauh di sisi penerima, TCP mengembalikan pengakuan 40-byte (header TCP 20-byte + header IP 20-byte). Jika editor bereaksi terhadap karakter tersebut, ia akan menggemakannya sebagai paket 41-byte, yang diakui dengan paket 40-byte. Jadi, 162 byte dan empat segmen dikirim untuk setiap karakter yang diketik. Ada sejumlah masalah yang dapat menurunkan kinerja TCP. Salah satunya adalah sindrom jendela konyol di mana ketika data dikirimkan dalam blok besar, namun aplikasi pada mesin host di sisi penerima membaca data satu byte pada satu waktu. Hal ini diilustrasikan pada Gambar 11.9.

Buffer TCP di sisi penerima penuh dan host pengirim mengetahui hal ini karena ukuran jendela disetel ke nol. Prosesnya membaca satu byte. TCP meneruskan pembaruan jendela salah satunya. Host pengirim mengakui dan mengirimkan satu byte. Buffer menjadi penuh sehingga host penerima mengakui byte dan menetapkan ukuran jendela ke nol.




**Gambar 11.10 Jendela Sindrome Silly**

**Kontrol Kemacetan TCP**

Semua algoritma TCP Internet didasarkan pada waktu habis yang sebagian besar disebabkan oleh kemacetan karena jaringan dan kapasitas host penerima. Paket yang hilang karena gangguan pada saluran transmisi jarang terjadi saat ini. Setiap host pengirim memiliki dua jendela. Salah satunya adalah jendela host penerima yang menunjukkan kapasitas host penerima dan yang lainnya adalah jendela kongesti yang menunjukkan kapasitas jaringan. Jumlah byte yang akan dikirimkan harus minimal 2 jendela.

Awalnya jendela kemacetan adalah MTU yang ditingkatkan menjadi kapasitas ganda pada setiap burst yang berhasil dikirim karena pengakuan diterima sebelum batas waktu diteruskan. Peningkatan eksponensial ini disebut sebagai permulaan yang lambat yang berlanjut hingga ambang batas yang awalnya 64K tercapai. Selanjutnya kenaikannya linear

sebesar 1 MTU. Jika batas waktu habis, ambang batas disetel ke setengah jendela kemacetan saat ini dan permulaan yang lambat diulangi. Ketika paket pemadaman sumber ICMP masuk, paket tersebut diperlakukan dengan cara yang sama seperti batas waktu.

**Manajemen Pengatur Waktu TCP**

Pengatur waktu transmisi ulang bermaksud untuk menangani variasi besar waktu bolak-balik yang terjadi di TCP. Waktu perjalanan pulang pergi M ditentukan untuk setiap segmen dan perkiraan mean dan mean deviasi diperbarui sebagai:

$$\text{Round Trip Time (RTT)} = \beta\text{RTT} + (1-\beta)\text{M}$$
$$\text{D} = \beta\text{D} + (1-\beta)|\text{RTT} - \text{M}|$$

dengan $\beta$ parameter penghalusan, biasanya 7/8. Batas waktu kemudian diatur ke: RTT + 4 D Algoritme Karn tidak memperbarui RTT dan D untuk segmen yang ditransmisikan ulang. Sebagai alternatif, batas waktu digandakan pada setiap kegagalan hingga segmen selesai untuk pertama kalinya. Saat menerima ukuran jendela sama dengan 0, pengatur waktu persistensi digunakan untuk mencegah hilangnya pembaruan jendela berikutnya. Keepalive timer juga digunakan dimana jika koneksi idle dalam waktu yang lama, timeout menyebabkan paket dikirimkan untuk memeriksa apakah pihak lain masih hidup. Jika paket gagal merespons, koneksi dihentikan. Namun fitur ini tidak disarankan karena menambah overhead dan dapat mengakhiri koneksi yang sehat karena masalah jaringan sementara. Pengatur waktu terakhir adalah yang digunakan dalam status TIMED WAIT saat penutupan, berjalan selama dua kali masa pakai paket maksimum untuk memastikan bahwa ketika koneksi ditutup; semua paket yang dibuatnya telah mati.

**Ringkasan**

- Lapisan empat model referensi OSI adalah lapisan transport yang menyediakan transfer data transparan antara mesin sumber dan tujuan menggunakan layanan lapisan jaringan seperti IP di bawahnya untuk memindahkan PDU data antara dua mesin yang berkomunikasi.
- Lapisan transport adalah lapisan sumber-ke-tujuan atau lapisan ujung-ke-akhir yang sesungguhnya. Protokol lapisan Transport OSI (ISO-TP) mengelola kontrol ujung ke ujung dan pemeriksaan kesalahan untuk memastikan pertukaran data yang lengkap. Ini menyediakan komunikasi “peer to peer”, dengan entitas transport mesin tujuan (remote peer).
- Lapisan transport menyediakan layanan yang dapat diandalkan selain layanan yang tidak dapat diandalkan yang disediakan oleh lapisan jaringan. Negosiasi opsi di antara parameter kualitas layanan yang berbeda menghasilkan layanan transportasi yang efisien, andal, dan hemat biaya bagi aplikasi pengguna.
- Kontrol aliran mengatur transmisi data antar perangkat sehingga perangkat pengirim tidak mengirimkan lebih banyak data daripada yang dapat diproses oleh perangkat

penerima. Multiplexing memungkinkan data dari beberapa aplikasi dikirim ke satu tautan fisik.

- Sirkuit virtual dibuat, dipelihara, dan diakhiri oleh lapisan transport. Pemeriksaan kesalahan melibatkan pembuatan berbagai mekanisme untuk mendeteksi kesalahan transmisi, sedangkan pemulihan kesalahan melibatkan pengambilan tindakan, seperti meminta data dikirim ulang, untuk mengatasi kesalahan yang terjadi.
- Transportasi primitif adalah cara yang efektif untuk bertukar data di atas lapisan jaringan. Layanan yang disediakan pada lapisan transport tampaknya serupa dengan layanan pada lapisan data link. Namun, mereka berbeda dalam banyak hal dimana lapisan data link menyediakan koneksi antara dua router menggunakan saluran fisik sedangkan lapisan transport menggunakan subnet.
- TCP adalah protokol dalam rangkaian TCP/IP yang menyediakan transmisi data yang andal. Aplikasi yang memerlukan protokol transport untuk menyediakan pengiriman data yang andal menggunakan TCP karena protokol tersebut memverifikasi bahwa data dikirimkan melalui jaringan secara akurat dan dalam urutan yang benar.
- UDP adalah protokol tanpa koneksi yang tidak dapat diandalkan yang mengurangi beban proses pada CPU. Namun permasalahan kinerja, yang tidak memiliki model ilmiah untuk mendukungnya, didukung oleh pengalaman dan contoh. Mereka berupaya untuk mengatasi masalah kinerja dalam jaringan komputer, mengukur kinerja jaringan, merancang sistem untuk kinerja yang lebih baik, pemrosesan TPDU yang cepat, dan protokol untuk jaringan berkinerja tinggi di masa depan.

**Latihan Soal**

Berikan satu kata untuk pernyataan berikut:

1. Ini adalah jumlah waktu ketika pengakuan diterima dari mesin tujuan yang diminta koneksinya. Tentu saja, semakin sedikit penundaannya, semakin baik layanannya.
2. Karena kemacetan dalam jaringan, kurangnya ketersediaan ruang dalam tabel, beberapa masalah internal dll, menyebabkan koneksi tidak diatur dalam penundaan pendirian.
3. Lapisan transport untuk membuat dan melepaskan koneksi di seluruh jaringan mencakup mekanisme penamaan sehingga suatu proses pada satu mesin dapat menunjukkan dengan siapa proses tersebut ingin berkomunikasi.
4. Ketika lapisan transport menerima pesan besar dari lapisan sesi, pesan tersebut dipecah menjadi unit-unit yang lebih kecil tergantung pada kebutuhan.
5. Kelompok kerja IETF telah mengusulkan model layanan terintegrasi (IS) berdasarkan kebijakan bandwidth keluar untuk sumber daya yang dapat diprediksi dalam jaringan.
6. Kerangka kebijakan yang menjelaskan kualitas aliran data tertentu dalam hal bandwidth, penggunaan buffer, prioritas, penggunaan CPU, dll.
7. Merupakan kemampuan lapisan transport untuk mengakhiri koneksi secara spontan jika terjadi kemacetan.

Isilah bagian yang kosong:

1. TCP adalah contoh..... , protokol transport yang andal.
2. Contoh protokol connectionless adalah..... Keuntungannya adalah overhead yang rendah.
3. Protokol..... mengatur koneksi sebelum mengirimkan informasi ke host.
4. Keuntungan dari..... protokol lebih dapat diandalkan dan melacak pengiriman pesan.
5. Tiga kesalahan yang mungkin dialami dan diperbaiki oleh layanan TCP adalah frame yang hilang; bingkai tiba rusak dan..... bingkai.

Uraian

1. Apa perbedaan lapisan transport dengan lapisan data link ketika layanan yang disediakan pada kedua lapisan tersebut hampir serupa?
2. Mengapa lapisan transport diperlukan ketika lapisan jaringan dan transport menyediakan layanan tanpa koneksi dan berorientasi koneksi?
3. Apa sajakah parameter kualitas layanan yang berbeda pada lapisan transport?
4. Mengapa UDP digunakan ketika UDP menyediakan layanan connectionless yang tidak dapat diandalkan pada lapisan transport?
5. Apa tujuan pengendalian aliran?
6. Jelaskan TCP dan kelebihan utamanya dibandingkan UDP.

# BAB 12
# LAPISAN APLIKASI

**Pendahuluan**

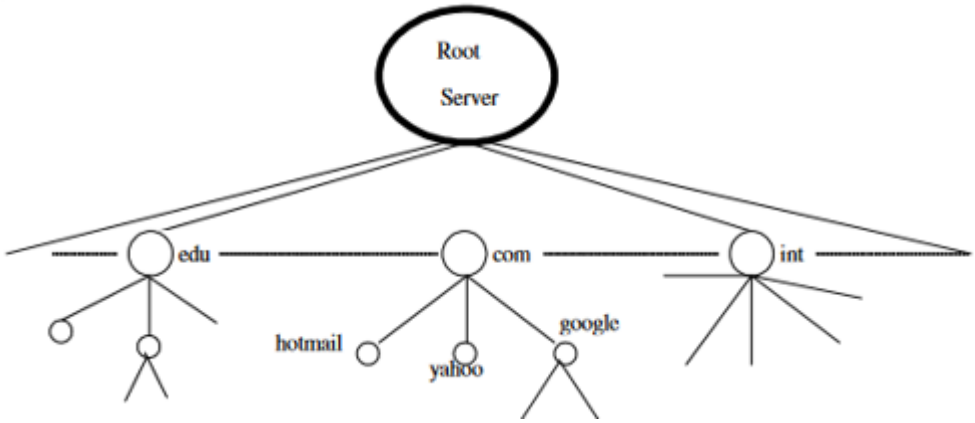
Tiga lapisan teratas yaitu lapisan sesi, presentasi dan aplikasi dianggap sebagai lapisan pengguna atau aplikasi model OSI. Mereka diimplementasikan dalam perangkat lunak. Di sebagian besar protokol, fungsi lapisan-lapisan ini dikonvergensi menjadi satu lapisan yang disebut lapisan aplikasi. TCP adalah salah satu contoh dari jenis protokol tersebut. Lapisan aplikasi, lapisan tertinggi model OSI berinteraksi dengan aplikasi perangkat lunak, yang memungkinkan mesin sumber dan tujuan berkomunikasi dengan baik. Ini menyediakan layanan berbeda, yang dijelaskan di sini.

## 12.1 SISTEM NAMA DOMAIN (DNS)

Sekarang kita memiliki dua jenis alamat IP dalam bentuk angka desimal dan teks untuk host yang sama. Anda tahu bahwa daftar semua alamat IP dikelola secara terpusat oleh ICANN dalam bentuk direktori database terdistribusi. Ada beberapa server terdistribusi, yang memelihara daftar alamat IP ini. Alasan di balik server terdistribusi sangat logis dan sederhana. Ini membantu dalam manajemen bencana dan mengalihkan beban lalu lintas dalam bentuk permintaan dari klien ke server DNS lain yang terletak di situs berbeda. Server DNS memelihara database baik dalam bentuk tekstual maupun notasi desimal. Misalnya, server DNS mempertahankan alamat situs Google sebagai www.google.com dan 216.23.9.53.99. Dengan cara ini, DNS digunakan untuk menyediakan pemetaan alamat host-ke-IP dari host jarak jauh ke host lokal dan sebaliknya. Sekarang sudah cukup jelas bahwa DNS memelihara database terdistribusi untuk memetakan antara nama host dan alamat IP.

Setiap kali klien meminta layanan dari suatu situs, maka kedua situs tersebut menjalankan protokol DNS untuk mengakses database terdistribusi yang tidak lain adalah Sistem Nama Domain. Oleh karena itu, DNS menyediakan protokol yang memungkinkan klien dan server berkomunikasi satu sama lain. DNS memungkinkan sistem untuk menggunakan penyelesai, yang menyelesaikan nama host ke alamat IP yang dapat dimengerti oleh server. Anda mungkin sekarang berpikir tentang bagaimana DNS mampu menyediakan terjemahan cepat teks alamat IP dalam sepersekian detik dari direktori yang berisi miliaran alamat tersebut. Hal ini dapat dimungkinkan dengan menggunakan konsep Domain, yang menggunakan pengaturan hierarki terjemahan alamat teks.

Anda dapat melihat dari Gambar 12.1 bahwa di tingkat atas adalah server root, yang memiliki label null. Di bawahnya ada domain level lain atau domain seperti com, edu, int dan seterusnya yang dikelompokkan menjadi satu. Di bawah ini subdomain atau grup berbeda telah dibuat. Tabel 12.1 menunjukkan beberapa nama domain yang umum muncul dengan situsnya masing-masing. DNS dapat mengakomodasi hampir semua jenis organisasi dengan memungkinkan setiap kelompok memilih antara hierarki penamaan geografis atau organisasi.




**Gambar 12.1 Hirarki DNS**

Seperti yang kita ketahui bahwa server yang memelihara alamat tersebar dan memiliki lokasi di seluruh dunia. Kemudian muncul pertanyaan tentang bagaimana alamat teks disusun dalam susunan hierarki. Anda dapat merujuk Gambar 12.1 di atas dan Tabel 12.1. Hirarki direpresentasikan ke dalam zona dan setiap zona merupakan hierarki dari satu atau lebih node tanpa tumpang tindih. Setiap zona diwakili oleh sebuah server dan tentunya dengan satu server cadangan. Server root seperti yang ditunjukkan pada Gambar 12.1 hanya satu, yang hanya bersifat indikatif; mungkin ada beberapa server root di beberapa lokasi di dunia. Setiap root mengetahui lokasi setiap server DNS dari domain tertentu.

**Tabel 12.1 Domain Internet**

| Domain | Situs Indikatif |
|---|---|
| Com | Lembaga komerial |
| Edu | Institusi pendidikan |
| Org | Organisasi non profit |
| Net | Penyedia layanan jaringan |
| Gov | Departemen pemerintahan |
| Mil | Militer |
| Biz | Bisnis |
| Country Code | Misalnya in untuk india, US untuk USA, AU untuk Australia, JP untuk Jepang dan seterusnya |

Prosesnya sekarang sangat sederhana untuk dipahami. Saat Anda perlu terhubung dengan situs tertentu, Anda terlebih dahulu mengirimkan permintaan Anda ke host lokal Anda. Jika host lokal Anda dapat menyediakan terjemahannya, permintaan Anda selesai. Jika tidak, host lokal Anda kemudian mengirimkan permintaan Anda satu tingkat di atas hierarki. Jika server pada satu tingkat di atas mampu menangani hal yang sama, Anda mendapatkan situs web yang Anda inginkan di desktop melalui server lokal Anda. Jika tidak, maka server satu tingkat di atas server lokal Anda akan mengirimkan permintaan Anda lagi ke server lain

atau memberi tahu server lokal Anda bahwa permintaan Anda gagal dan memberikan alamat server lain untuk memproses permintaan Anda. Proses ini berlanjut hingga ditemukan server yang mengetahui alamatnya, jika tidak, permintaan akan disaring hingga ke server root. Tergantung pada alamat domain, server root meneruskan permintaan ke salah satu server domain yang diwakili pada tingkat hierarki berikutnya. Proses ini berlanjut dan informasi alamat teks dikembalikan ke server Root dan kemudian kembali ke server lokal Anda.

## 12.2 SURAT ELEKTRONIK

Surat elektronik adalah salah satu layanan jaringan yang paling populer. Penggunaan surat elektronik, atau email mungkin dapat disebut sebagai alasan utama popularitas Internet. Menjamurnya kafe cyber dapat disebabkan oleh email atau World Wide Web. E-mail menyediakan sarana komunikasi yang efisien dan cepat dengan kerabat, teman atau kolega di seluruh dunia. Anda tidak hanya dapat berkomunikasi dengan satu orang dalam satu waktu atau ribuan orang tetapi Anda juga dapat menerima dan mengirim file dan informasi lainnya dalam waktu singkat. Dalam komunikasi email, penerima atau penerima pesan yang dituju tidak diharuskan berada di desktop mereka pada saat pesan diterima oleh komputer mereka. Ini berfungsi seperti surat pos. Dalam surat pos, tukang pos memasukkan pesan pengirim ke kotak surat Anda dan ketika Anda kembali dari pekerjaan, Anda mengakses kotak surat Anda untuk mengambil pesan tersebut. Oleh karena itu, kami dapat menganggapnya sebagai pengganti surat pos. Namun, ia memiliki lebih banyak fitur unggulan dibandingkan surat pos. Email memiliki dua bagian:

- **Agen Pengguna**: Ini adalah antarmuka pengguna ke sistem email. Sistem agen pengguna memungkinkan untuk menyediakan cara untuk melihat, mengedit, dan membalas pesan, dll. Sistem ini juga mengakses pesan yang disimpan di kotak surat sistem. Agen pengguna memungkinkan pengguna menggunakan editor teks untuk membuat file yang diserahkan agen pengguna ke agen transfer pesan.
- **Agen Transfer Pesan** (MTA): Ini adalah paket perangkat lunak yang mengangkut pesan yang dibuat oleh pengguna ke kotak surat tujuan, mungkin di mesin jarak jauh. MTA harus melakukan pekerjaan yang lebih kompleks dibandingkan aplikasi lain:
    1. MTA menangani kegagalan sementara ketika mesin tujuan tidak tersedia untuk sementara; itu menyimpan pesan di mesin lokal untuk pengiriman nanti. Jadi, Agen Pengguna biasanya hanya menyimpan pesan ke dalam tempat penyi7mpanan.
    2. MTA membedakan penerima lokal dan penerima jarak jauh.
    3. MTA perlu mengirimkan salinan pesan ke beberapa mesin.
    4. MTA harus mengizinkan pencampuran teks, suara, dan video dalam pesan dan menambahkan dokumen dan file ke pesan.

Seperti dibahas di atas, alamat email terdiri dari komponen-komponen berikut:

- **Nama kotak surat**: Kotak surat dikaitkan dengan satu id login dalam server surat untuk menyimpan email pengguna. Oleh karena itu, nama spesifik diberikan ke kotak surat yang terkait dengan setiap ID.

- **Nama simbolis**: Mengacu pada nama layanan, bukan pengguna tertentu. Misalnya, postmaster secara universal dikenal sebagai alamat untuk masalah surat pos. Dalam sistem email, nama simbolis adalah alias untuk kotak surat tertentu.
- **Nama grup** (peledak email): Merujuk pada alias untuk sekumpulan penerima. MTA berkonsultasi dengan database internal untuk menentukan alamat email.

Ada sejumlah paket email yang tersedia. Beberapa di antaranya gratis seperti email Goggle, Yahoo mail, hotmail, dll, sementara ada juga yang berbayar. Semuanya juga tidak sama tetapi sebagian besar perangkat lunak email memiliki beberapa fungsi dasar yang umum. Ini adalah:

- Mengirim dan menerima pesan email
- Simpan pesan Anda dalam sebuah file
- Mencetak pesan email
- Meneruskan pesan email ke penerima lain
- Membalas pesan email
- Melampirkan file ke pesan email

Untuk mengirim pesan kita perlu mengetikkan terlebih dahulu alamat penerima yang dituju. Alamat email memiliki kemiripan dengan nomor telepon sehubungan dengan identifikasi orang, organisasi, atau lokasi geografis. Demikian pula alamat email, nomor telepon, yang biasanya memiliki kode area, memiliki aturan penggunaan. Biasanya, alamat email memiliki tiga bagian:

1. Identitas atau nama pengguna
2. Tanda “at” (@)
3. Nama domain, yang pada dasarnya menentukan alamat server email pengguna. Ini adalah bagian paling kanan dari alamat dan mengikuti konvensi penamaan tertentu. Anda sekarang dapat memahami alamat email dengan bantuan contoh berikut:- Contoh - services@jalandhar.in

Bagian paling kiri sebelum @ (tanda at) adalah identitas atau nama pengguna dan bagian paling kanan setelah @ adalah server yang menunjukkan India. Ada beberapa konvensi penamaan seperti edu, com, org dll yang masing-masing digunakan untuk pendidikan, komersial, organisasi.

Simple Mail Transfer Protocol adalah standar de facto penyedia layanan surat elektronik (email). Hal ini dimaksudkan untuk transfer pesan email melalui jaringan. Protokolnya sendiri sederhana karena menggunakan jasa TCP dimana sebagian besar kerja kerasnya ditangani oleh protokol tingkat rendah. SMTP menggunakan transport TCP untuk pengiriman pesan email yang andal. Untuk tujuan ini MTA membuka koneksi TCP ke lokasi tujuan dan mengirimkan pesan ke tujuan di lokasi ini. MTA jarak jauh di server email lokasi jarak jauh menyimpan pesan dalam penyimpanannya dan mengembalikan pengakuan setelah pesan berhasil disimpan. Setelah itu, pengirim menghapus salinannya. Ketika alamat tujuan tidak tersedia, MTA mencoba mengirim pesan lagi nanti. Jika peristiwa pesan tidak dapat dikirimkan pada hari tertentu, MTA akan mengembalikan kesalahan kepada pengguna.

Singkatnya, ketika ada email keluar, klien SMTP akan terhubung ke server SMTP dan mengirimkan email ke server jauh. Ini menggunakan protokol sederhana dan berbasis teks

untuk satu atau lebih tujuan pesan. Server SMTP juga memungkinkan layanan telnet. SMTP dapat dianggap sebagai pelengkap UUCP. Mesin yang terhubung bersama dapat mentransfer email dengan baik menggunakan UUCP tetapi tidak dengan mesin yang terhubung melalui jaringan sepanjang waktu.

SMTP juga berkaitan dengan transfer email dari satu MTA ke MTA lainnya. Protokol SMTP cukup sederhana. Ia menggunakan model respons kueri dan hanya beberapa jenis pesan yang ditentukan. Pekerjaan kompleks lainnya ditangani oleh TCP. Perintah SMTP terdiri dari string ASCII yang dapat dibaca manusia. Koneksi TCP tunggal digunakan untuk memproses serangkaian pertukaran pesan antara sepasang host secara serial. SMTP tidak pernah mengautentikasi pengirim. Awalnya, SMTP diimplementasikan menggunakan Sendmail sebagai agen transfer email dalam model server klien. Selanjutnya, standar untuk file biner disertakan selain standar berbasis teks ASCII murni. Standar Multiguna Internet Mail Extensions (MIME) digunakan untuk menyandikan file biner untuk ditransfer melalui SMTP, yang kini telah menjadi standar dengan versinya yang bervariasi. SMTP bersama dengan protokol Post Office Protocol (POP3) atau Internet Message Access Protocol (IMAP) memungkinkan pengambilan email dari server email.

Surat Internet memiliki keunggulan penting dibandingkan sistem surat lainnya, misalnya uucp atau bitnet karena sistem surat Internet menyediakan sistem pengiriman end-to-end yang andal. Berbeda dengan sistem email lainnya, dalam sistem email Internet, semua alamat email memiliki bentuk yang sama: lokal- bagian@nama-domain.

**Protokol Transfer Surat Sederhana (SMTP)**

Surat elektronik (Email) dianggap sebagai aplikasi TCP/IP yang paling banyak digunakan. Protokol email Internet memungkinkan mesin klien untuk bertukar email dan pesan antara host TCP/IP. Tiga protokol standar diterapkan untuk menyediakan aplikasi email tersebut. SMTP adalah salah satunya. Ketiga standar tersebut diberikan di bawah ini:

1. **SMTP**: Ini adalah standar untuk pertukaran email antara dua komputer (STD 11/RFC 821), yang menentukan protokol yang digunakan untuk mengirim email antara host TCP/IP.
2. **Mail**: Ini adalah standar (STD 11) yang mendefinisikan format pesan email, sintaksis bidang header email, sekumpulan bidang header dan interpretasinya, serta tentang sekumpulan tipe dokumen selain ASCII teks biasa yang akan digunakan dalam badan surat.
3. **DNS-MX**: Ini adalah standar untuk perutean email menggunakan Sistem Nama Domain (RFC 974).

SMTP, protokol lapisan aplikasi, digunakan untuk mengirim pesan email melalui Internet. Ia menggunakan TCP sebagai protokol transport untuk mengirim email ke penukar email tujuan, yang disebut server email. Mesin klien mengirim email ke penukar email atau email dikirim dari penukar email ke penukar email lain. Email yang dikirimkan menggunakan SMTP biasanya dikirimkan dari satu penukar surat ke penukar surat lainnya secara langsung. E-mail tidak pernah dirancang untuk diberikan secara instan namun sering muncul.

Catatan Mail Exchanger tidak lain hanyalah program aplikasi perangkat lunak untuk mendukung protokol SMTP. Penukar Surat seperti sendmail atau Microsoft Exchange menunggu datagram IP yang tiba di antarmuka jaringan dengan nomor port TCP 25. Ketika sebuah pesan tiba, penukar surat memeriksa untuk mengetahui apakah itu untuk salah satu penggunanya dan memindahkannya sesuai dengan itu. surat ke kotak surat pengguna. Data yang dikirim menggunakan SMTP adalah data ASCII 7-bit, dengan bit tingkat tinggi yang disetel ke nol dianggap memadai di sebagian besar kasus untuk transmisi pesan teks berbahasa Inggris namun tidak memadai untuk teks non-Inggris atau data non-tekstual. Untuk mengatasi keterbatasan ini, Multiguna Internet Mail Extensions (MIME) mendefinisikan mekanisme untuk pengkodean teks dan data biner sebagai ASCII 7-bit dalam amplop surat dan Ekstensi Layanan SMTP menetapkan mekanisme untuk memperluas kemampuan SMTP melampaui batasan tersebut.

**Bagaimana SMTP Bekerja?**

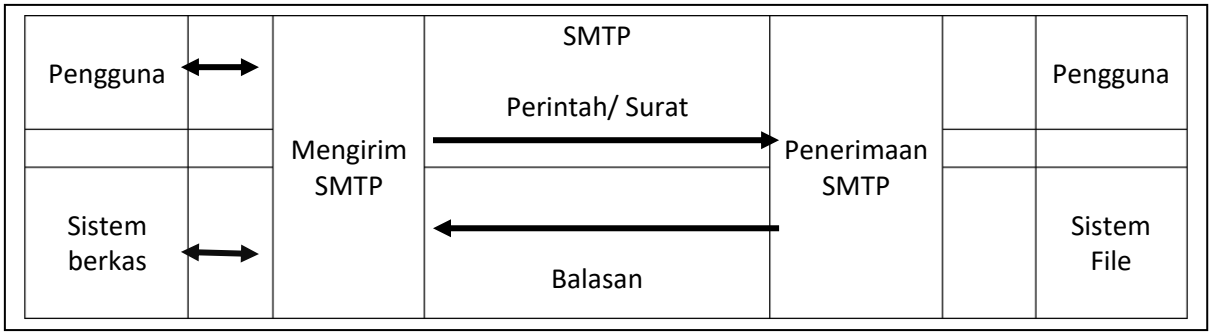
SMTP adalah pengiriman end-to-end di mana mesin klien SMTP menghubungi server SMTP host tujuan secara langsung untuk mengirimkan email. Berbeda dengan prinsip simpan dan teruskan yang mengirimkan konten email ke host tujuan melalui sejumlah node perantara dalam jaringan yang sama, SMTP melanjutkan pengiriman konten email hingga berhasil disalin ke SMTP host. Dalam hal mekanisme penyimpanan dan penerusan, keberhasilan transmisi dari pengirim hanya menunjukkan bahwa konten email telah mencapai hop perantara pertama. Ada beberapa contoh ketika surat dipertukarkan antara sistem surat TCP/IP SMTP dan sistem surat yang digunakan secara lokal. Aplikasi semacam ini disebut sebagai gateway email atau jembatan email. Namun, SMTP hanya menjamin pengiriman ke host gateway email, bukan ke host tujuan sebenarnya, yang terletak di luar jaringan TCP/IP. Dalam hal gateway email, transmisi ujung-ke-ujung SMTP adalah host-to-gateway, gateway-to-host, atau gateway-to-gateway. SMTP tidak menentukan format email di luar gateway. Setiap pesan SMTP berisi kolom berikut:

- Header atau amplop yang diakhiri dengan garis nol.
- Isi - Segala sesuatu setelah baris null atau kosong adalah isi pesan dengan urutan baris yang berisi karakter ASCII.

Simple Mail Transfer Protocol mendefinisikan protokol klien/server. Mesin SMTP klien memulai sesi dengan mengirimkan pesan SMTP dan server email merespons dengan menerima pesan SMTP ke permintaan sesi.

**Pertukaran Surat**

Perancangan SMTP didasarkan pada model komunikasi yang diilustrasikan pada Gambar 12.2. Setelah permintaan email mesin klien, SMTP pengirim menetapkan koneksi dua arah dengan SMTP penerima. SMTP penerima mungkin merupakan mesin tujuan atau mesin perantara (gateway email). SMTP pengirim akan memulai perintah yang dibalas oleh SMTP penerima.




**Gambar 12.2 Komunikasi SMTP**

1. SMTP mesin klien menetapkan koneksi TCP dengan SMTP mesin tujuan dan kemudian menunggu server mengirim pesan layanan siap atau pesan layanan tidak tersedia.
2. HELO (HELO adalah singkatan dari hello) dikirim dan mesin penerima akan mengidentifikasi dirinya dengan mengirimkan kembali nama domainnya. SMTP mesin klien menggunakan ini untuk memverifikasi apakah mesin tersebut mencapai SMTP tujuan yang benar. Jika SMTP mesin klien mendukung Ekstensi Layanan SMTP, perintah EHLO akan menggantikan perintah HELO. SMTP mesin tujuan yang tidak mendukung ekstensi layanan merespons dengan kesalahan Sintaks 500, pesan perintah tidak dikenal. SMTP mesin klien kemudian mencoba lagi dengan HELO, atau jika mesin klien tidak dapat mengirimkan pesan tanpa satu atau lebih ekstensi layanan, mesin tersebut harus mengirimkan pesan QUIT. Jika SMTP penerima mendukung ekstensi layanan, ia merespons dengan pesan multi-baris 250 OK yang berisi daftar ekstensi layanan yang didukungnya.
3. Mesin klien sekarang memulai transaksi email dengan mengirimkan perintah MAIL ke mesin tujuan. Perintah ini memiliki jalur terbalik yang digunakan untuk melaporkan kesalahan. Perlu dicatat bahwa jalur lebih dari sekadar pasangan nama domain kotak surat@host pengguna. Selain itu, ia memiliki daftar host perutean.
4. Langkah selanjutnya dari pertukaran surat yang sebenarnya menyediakan SMTP server dengan tujuan pesan; pesannya mungkin sampai ke lebih dari satu penerima. Hal ini dilakukan dengan mengirimkan satu atau lebih perintah RCPT TO:<forward-path>. Masing-masing dari mereka akan menerima balasan 250 OK ketika tujuannya diketahui oleh server atau 550. Tidak ada pengguna seperti itu di sini ketika tidak diketahui oleh server.
5. Ketika semua perintah RCPT terkirim, pengirim meneruskan perintah DATA untuk memberitahu mesin tujuan bahwa isi pesan mengikuti. Server membalas dengan 354 Mulai input email, akhiri dengan <CRLF>.<CRLF>. Perlu dicatat bahwa urutan akhir yang digunakan mesin klien untuk menghentikan data pesan.
6. Mesin klien sekarang mengirimkan data baris demi baris yang diakhiri dengan urutan 5 karakter Baris <CRLF>.<CRLF> di mana mesin tujuan mengakui dengan 250 OK atau pesan kesalahan yang sesuai ketika ada yang tidak beres.
7. Sekarang, ada beberapa tindakan yang mungkin dilakukan:

- Mesin tujuan tidak memiliki pesan lagi untuk dikirimkan, maka akan mengakhiri koneksi dengan perintah QUIT. Perintah ini dijawab dengan balasan saluran transmisi penutupan Layanan 221.
- Mesin tujuan tidak mempunyai pesan lagi untuk dikirim, namun siap menerima pesan (jika ada) dari sisi lain. Ini akan mengeluarkan perintah TURN. Kedua SMTP sekarang berganti peran sebagai pengirim/penerima dan mesin klien yang sebelumnya merupakan mesin tujuan kini mengirimkan pesan dengan memulai langkah 3 di atas.
- Mesin klien ingin mengirimkan pesan lain dan cukup mengikuti langkah 3 untuk mengirimkan perintah MAIL baru.

## 12.3 WEB DI SELURUH DUNIA

Anda pasti sangat familiar dengan istilah World Wide Web, yang juga dikenal sebagai web atau WWW atau W3 dan sejauh ini telah memantapkan dirinya sebagai bagian paling populer di Internet. Ini adalah tambang informasi yang luar biasa, begitu Anda mulai mencari apa pun mulai dari dokumen, gambar, hingga perangkat lunak, semuanya tampak tak terbatas. Ini memberi Anda dokumen, file suara, melihat gambar, animasi, dan video, berbicara dan mendengar suara, dan melihat program yang dijalankan di hampir semua perangkat lunak di dunia. Oleh karena itu, ini memfasilitasi komunikasi yang kaya dan beragam dengan memungkinkan Anda mengakses dan berinteraksi dengan teks, grafik, animasi, foto, audio dan video. Kini menjadi sangat mudah bagi Anda untuk memahami cara kerja web dan apa itu web. Implementasinya didasarkan pada sistem server klien dan menggunakan komputer pribadi Anda sebagai klien, perangkat lunak browser web, koneksi ke penyedia layanan Internet, server, router dan switch untuk mengarahkan arus informasi. Anda mungkin mengetahui semua istilah yang digunakan dalam pembentukan web kecuali web browser.

Browser adalah perangkat lunak yang digunakan komputer Anda untuk melihat dokumen WWW dan mengakses Internet. Program browser yang ada di komputer Anda memfasilitasi Anda dengan keunggulan pemformatan teks, tautan hypertext, gambar, suara, gerakan, dan fitur lainnya. Internet Explorer dan Netscape adalah beberapa browser yang banyak digunakan. Browser memiliki sub program yang disebut plug-in untuk menangani dokumen yang Anda temukan di Web. Mungkin juga plug-in lain yang disimpan di tempat lain di komputer Anda.Web sangat mudah digunakan. Kapan pun Anda ingin mengunjungi situs web apa pun, misalnya situs web lembaga Anda, Anda cukup memasukkan alamat atau URL situs web tersebut di browser web Anda untuk meneruskan permintaan Anda ke server web lembaga tersebut untuk menyediakan halaman web yang Anda maksud. Server web lembaga tersebut kemudian mengirimkan permintaan Anda di Internet untuk menemukan situs web yang dituju. Setelah diperoleh, server web mengembalikan data yang sama ke komputer Anda di mana browser yang dimuat dengan plug-in berbeda menafsirkan data, menampilkannya di layar komputer Anda. Halaman web yang dimaksud, yang sekarang tersedia di desktop Anda, mungkin memiliki link yang dapat diklik. Jika Anda mengkliknya, Anda dapat mengunjungi

halaman lain. Dengan cara ini, informasi yang tersebar di seluruh dunia dapat dihubungkan satu sama lain.

Sekarang menjadi penting untuk menjelaskan bagaimana halaman web yang berbeda dengan format teks dan standar yang berbeda dapat dihubungkan ke halaman web tertentu. Kekuatan pengikat yang menyatukan Web adalah hypertext dan hyperlink. Hyperlink memungkinkan file elektronik di Web dihubungkan sehingga Anda dapat berpindah dengan mudah di antara file-file tersebut menggunakan protokol hypertext. Seperti yang telah Anda pelajari bahwa browser web yang memungkinkan Anda mengakses Web juga membedakan antara halaman web dan jenis data lainnya di Internet karena halaman web ditulis dalam bahasa komputer yang disebut Hypertext Markup Language atau HTML.

- **Hypertext**: Pengoperasian www didasarkan pada hypertext yang digunakan untuk berinteraksi dengan pengguna web atau browser web. Seperti teks biasa, hypertext dapat disimpan, dibaca, dicari atau diedit. Berbeda dengan teks biasa, hypertext berisi koneksi dalam teks ke dokumen lain. Tautan hiperteks digunakan untuk membuat hyperlink yang selanjutnya dapat membuat jaringan koneksi virtual yang kompleks. Hypertext memungkinkan pengguna web untuk maju atau mundur, mendapatkan lebih banyak detail tentang topik saat ini, mengubah arah dan bernavigasi dengan cara apa pun yang diinginkan pengguna web saat menjelajahi halaman web daripada mengikuti teks secara liner seperti buku. Hal ini dimungkinkan karena hypertext memiliki teks dengan pointer ke teks lain.
- **Hypermedi**a: Ini adalah hypertext dengan beberapa perbedaan. Dokumen hypermedia tidak hanya menyediakan tautan ke bagian teks lain, namun juga menyediakan tautan ke bentuk media lain seperti suara, gambar, dan film. Dengan kata lain, hypermedia digunakan untuk menggabungkan hypertext dan multimedia.

Perhatian Hypermedia dan hypertext memiliki konsep yang mirip namun berbeda. Hypermedia dianggap sebagai superset dari hypertext.

**Fungsi WWW**

World Wide Web merupakan perangkat lunak yang bekerja dalam arsitektur client-server dimana web browser merupakan web client dan web server yang melayani permintaan yang diajukan oleh web client disebut server. Kliennya adalah browser seperti Internet Explorer, Netscape Navigator atau Mozilla. Browser digunakan untuk berinteraksi dengan server menggunakan serangkaian instruksi yang disebut protokol. Protokol-protokol ini memfasilitasi transfer data yang akurat melalui permintaan dari browser dan tanggapan dari server. Banyak protokol yang ada di Internet untuk komunikasi antara beberapa host. World Wide Web adalah bagian dari Internet dan menempatkan semua protokol ini dalam satu kelompok. Itu mungkin HTTP, FTP, Telnet, email dll. www menggunakan protokol tanpa koneksi.

Model server klien menggunakan arsitektur terdistribusi di mana program klien dapat berjalan pada mesin yang benar-benar terpisah dari server, mungkin di ruangan lain atau bahkan di negara lain. Dalam hal ini, tugas penyimpanan dokumen diserahkan kepada server dan tugas presentasi dokumen diserahkan kepada klien sehingga setiap program dapat

berkembang secara independen satu sama lain. Klien web dipanggil dan pengguna web memilih hyperlink di bagian hypertext yang menghubungkan ke dokumen lain. Browser web menggunakan alamat yang terkait dengan hyperlink tersebut untuk terhubung ke server web pada alamat jaringan tertentu dan meminta dokumen.

Server merespons kembali dengan mengirimkan teks dan media lain apa pun di dalam teks tersebut ke browser klien, yang ditampilkan browser di layar pengguna. World Wide Web melibatkan ribuan transaksi virtual per jam di seluruh dunia dan dengan demikian menciptakan jaringan arus informasi. Server web dilengkapi dengan kemampuan enkripsi dan otentikasi klien sehingga mereka dapat mengirim dan menerima data yang aman. Protokol yang digunakan oleh klien web dan server web untuk berkomunikasi satu sama lain disebut HTTP. Halaman web yang dikembalikan menggunakan bahasa pemrograman yang dikenal sebagai Hypertext Markup Language (HTML).

**Arsitektur Peramban**

Browser web terdiri dari tiga bagian. Mereka adalah pengontrol, program klien, dan penerjemah.

1. ***Pengontrol***: Pengontrol memperoleh masukan dari keyboard atau mouse untuk mengakses halaman web dengan bantuan program klien. Setelah mengakses halaman web, pengontrol menggunakan salah satu penerjemah untuk menampilkan halaman web di layar host.
2. ***Program Klien***: Mereka digunakan untuk membuat sesi TCP dengan server web atau server proxy. Program klien menggunakan HTTP, FTP, Gopher atau Telnet.
3. ***Interpreter***: Mereka digunakan untuk menampilkan halaman web di layar pengguna web. Interpreter yang digunakan untuk menerjemahkan halaman web di layar klien adalah HTML, CGI atau JAVA. Mereka bergantung pada jenis dokumen. HTML, yang merupakan bahasa markup dan memungkinkan browser mengubah format halaman web, digunakan untuk membuat skrip halaman web. HTML juga memungkinkan untuk menyimpan instruksi dengan teks sehingga browser mana pun dapat membaca instruksi dan memformat teks sesuai dengan mesin host yang digunakan. Dokumen di World Wide Web diklasifikasikan menjadi tiga jenis. Yaitu dokumen statis, dinamis dan aktif.
4. ***Halaman Web Statis***: Ini adalah dokumen konten tetap dan selalu memberikan informasi yang sama sebagai respons terhadap semua permintaan pengunduhan dari semua pengguna web. Dokumen statis disimpan di server web untuk diakses oleh klien web. Klien web saat meminta halaman web mendapat salinannya. Isi file ditentukan saat dibuat dan bukan saat digunakan. Namun, halaman web dapat dimodifikasi di server tetapi pengguna web tidak mempunyai hak untuk mengubahnya. Dengan demikian, halaman web statis menampilkan informasi yang sama untuk semua pengguna web dari semua konteks dan menyediakan link hypertext untuk melakukan navigasi melalui dokumen statis. Kelebihan menggunakan halaman web statis adalah bersifat cachet Friendly dimana satu salinan dapat ditampilkan kepada banyak orang dan memberikan kemudahan untuk memasangnya dengan cepat bahkan oleh orang

yang tidak mempunyai banyak pengalaman. Namun, pemeliharaannya menjadi sulit ketika situs menjadi besar dan sulit untuk tetap konsisten dan mutakhir.

5. ***Dokumen aktif***: Program yang berjalan di sisi klien dikenal sebagai dokumen aktif. Setiap kali klien web meminta dokumen aktif, server web menyediakan salinan dokumen dalam bentuk kode byte. Dokumen sekarang siap dijalankan di mesin klien web. Karena dokumen aktif disajikan dalam bentuk biner maka dapat diterapkan kompresi dan dekompresi di sisi server dan klien untuk mengurangi kebutuhan bandwidth dan throughput.
6. ***Halaman Web Dinamis***: Mereka menyediakan navigasi web interaktif dan memungkinkan untuk mengubah konten seperti teks, gambar, bidang formulir, dll. pada halaman web berdasarkan konteks atau kondisi yang berbeda. Halaman web dinamis menggunakan dua jenis interaktivitas:
    1. Skrip sisi klien: Digunakan untuk mengubah perilaku antarmuka dalam halaman web tertentu berdasarkan tindakan mouse atau keyboard atau pada peristiwa waktu tertentu. Perilaku dinamis terjadi dalam presentasi. Teknologi presentasi seperti JavaScript atau ActionScript untuk HTML dinamis (DHTML) dan Flash untuk jenis media presentasi digunakan. Skrip sisi klien juga memungkinkan penggunaan skrip jarak jauh di mana halaman DHTML meminta informasi tambahan dari server. Konten dihasilkan di mesin klien web di mana browser web mengambil halaman dari server dan memproses kode yang tertanam di halaman web sehingga konten yang diambil dapat ditampilkan kepada pengguna web. Di halaman dinamis sisi klien, beberapa browser web tidak mendukung bahasa tersebut atau tidak mendukung beberapa perintah bahasa skrip.
    2. Skrip sisi server: Digunakan untuk mengubah sumber halaman web yang diminta antar halaman untuk menyesuaikan urutan atau memuat ulang halaman web yang dikirimkan ke browser. Respons server didasarkan pada kondisi tertentu seperti data dalam bentuk HTML yang diposting, parameter dalam URL, jenis browser yang digunakan, perjalanan waktu atau database atau status server. Halaman web dinamis skrip sisi server dirancang dengan bantuan bahasa sisi server seperti PHP, Perl, ASP, JSP, dll.

       Kedua teknik di atas juga dapat digunakan secara bersamaan untuk mengembangkan halaman web dinamis. Keuntungan halaman web dinamis adalah memungkinkan pembaruan halaman web dengan mudah dan pemuatan halaman web lebih cepat. Dalam halaman web dinamis, konten dan desain ditempatkan secara terpisah sehingga memungkinkan modifikasi yang sering dilakukan pada halaman web termasuk pembaruan teks dan gambar.

**Bahasa Markup Hiperteks (HTML)**

HTML adalah bahasa standar yang digunakan oleh WWW untuk membuat dan mengenali dokumen hypermedia. Halaman web ditulis dalam kode HTML dan file HTML disimpan dengan akhiran ".html". Dokumen HTML adalah file ASCII 7-bit standar dengan kode format yang berisi informasi tentang tata letak, hyperlink, dll. Dan pengguna dapat

mengontrol elemen visual seperti font, ukuran font, spasi paragraf, dll tanpa mengubah informasi asli. Perangkat lunak konversi digunakan untuk menerjemahkan dokumen dari format lain ke dalam HTML. Dokumen dalam bahasa apa pun dapat disajikan di web dengan mengubahnya menjadi format HTML dengan bantuan sejumlah perangkat lunak yang tersedia dengan mudah. Ada filter yang tersedia di web untuk mengonversi file dalam RTF (Rich Text Format), WordPerfect dan FrameMaker serta arsip email dan dokumen hanya teks. Standar HTML digunakan untuk mendukung pembuatan dan tata letak dokumen hypermedia dasar.

Namun HTML terbatas dalam menangani banyak teknik tata letak kompleks yang ditemukan dalam penerbitan dokumen tradisional. Ini dapat mendukung formulir interaktif, "hot spot" yang ditentukan dalam gambar, tata letak dan opsi dan gaya pemformatan yang lebih fleksibel, tabel yang diformat, dll. HTML+ memungkinkan pengguna untuk menyertakan hyperlink email untuk mengirim email secara otomatis saat memilih email. -alamat email dalam sepotong hypertext akan membuka program email, siap mengirim email ke alamat itu. Karakteristik HTML sebagai bahasa markup adalah memungkinkan pengguna untuk menyematkan instruksi pemformatan ke dalam file itu sendiri, yang disimpan bersama teks sehingga browser mana pun dapat membaca file itu sendiri.

**Uniform Resource Locator (URL)**

WWW tidak mungkin terjadi tanpa Uniform Resource Locator (URL). Mereka digunakan untuk mewakili tautan hypermedia dan tautan ke layanan jaringan dalam dokumen HTML. File atau layanan apa pun di Internet dapat disajikan dengan URL. Bagian pertama URL yang muncul sebelum dua garis miring digunakan untuk menentukan metode akses atau protokol yang diikuti untuk komunikasi antara browser dan server web. Bagian kedua yang muncul setelah dua garis miring mewakili alamat mesin host tempat data atau layanan dicari. Bagian lain setelah bagian kedua dapat menentukan nama file, port yang akan disambungkan, atau teks yang akan dicari dalam database. Semua bagian alamat untuk mendapatkan file atau layanan dari mesin host di URL ditampilkan sebagai satu baris tak terputus tanpa spasi dan lokasi mesin host atau situs web yang menjalankan server www biasanya diberi nama dengan www di bagian tersebut, awal alamat jaringan. Dalam mengakses layanan web, browser web memungkinkan pengguna untuk menentukan URL dan terhubung ke dokumen atau layanan tersebut. Ketika pengguna terhubung dengan layanan web, pengguna dengan memilih hypertext dalam dokumen HTML mengirimkan permintaan untuk membuka URL. Dengan demikian, hyperlink digunakan tidak hanya untuk menyediakan teks dan media lain dalam dokumen yang sama tetapi juga untuk menyediakan layanan jaringan lainnya. Browser web bukan sekadar klien web. Mereka adalah klien FTP, Gopher dan telnet berfitur lengkap.

**Antarmuka Gerbang Umum**

*Common Gateway Interface* (CGI) digunakan sebagai protokol standar untuk menghubungkan perangkat lunak aplikasi eksternal dengan server web di mana server web merespons permintaan yang dikirim oleh browser web. Dengan kata lain, ini dapat dipahami sebagai koneksi antara server web dan halaman web. Permintaannya mungkin berupa file yang disimpan di disk server web atau perintah yang dapat dieksekusi dan mungkin argumen. CGI digunakan untuk memberikan respons terhadap jenis permintaan kedua yaitu permintaan

perintah yang dapat dieksekusi. Oleh karena itu, CGI bersifat inklusif terhadap server web dan digunakan untuk berkomunikasi dengan program lain yang berjalan di server web. CGI memungkinkan pengguna web untuk mengajukan pertanyaan dan menjalankan aplikasi secara interaktif.

CGI digunakan untuk membuat halaman web berdasarkan interaksi pengguna web di mana pengguna web dapat membaca halaman acak di situs web, membuat halaman khusus berdasarkan input formulir, dan menghasilkan halaman berdasarkan database. Beberapa aplikasi CGI adalah pemrosesan formulir interaktif, pemrograman gateway, dll. Gateway juga dikenal sebagai gateway web dan merupakan program atau skrip untuk mengakses informasi yang tidak dapat dibaca langsung oleh klien web.

Dalam bentuknya yang paling sederhana, server web menerima permintaan dari klien web dan merespons kembali ke klien web dengan halaman web yang diminta melalui program HTTP tanpa memproses data klien web. Terkadang klien web memerlukan pemrosesan data di sisi server web. Dalam banyak kasus, server web juga tidak mengizinkan penyediaan data kata demi kata. Kasus seperti ini meminta klien web untuk mengirimkan formulir HTML yang diisi untuk mendapatkan data dari server web. Oleh karena itu untuk memulai pemrosesan dan manipulasi data di sisi server web, diperlukan program lain dan mekanisme untuk meneruskan data ke program lain. Program sekunder yang memungkinkan pemrosesan data di server web dikenal sebagai program gateway. Sesuai dengan namanya, mereka bertindak sebagai pintu gerbang antara web dan sumber daya lain di mesin server HTTP seperti database. Program gateway juga digunakan untuk mengembalikan data yang diproses ke klien web.

Biasanya, program dan skrip CGI berada di direktori khusus yang disebut cgi-bin. Ketika pengguna web membuka URL yang terkait dengan program CGI, klien web mengirimkan permintaan ke server web untuk meminta file tersebut. Menyadari bahwa ini adalah program CGI, server web menjalankan program tersebut alih-alih mengembalikan konten file dengan tepat. Ketika program CGI mulai berjalan, program tersebut akan membuat dan mengeluarkan dokumen baru atau memberikan URL ke dokumen yang sudah ada. Setelah itu, program CGI mengirimkan data yang baru dibuat baik secara langsung ke web client atau secara tidak langsung melalui web server. Ketika output terdiri dari header HTTP lengkap, data dikirim langsung ke klien web tanpa modifikasi server web. Alternatifnya, output dikirim ke server web sebagai aliran data dan server web kemudian menambahkan informasi header lengkap dan menggunakan protokol HTTP untuk mentransfer data ke klien.

Header terdiri dari rincian seperti jenis protokol komunikasi, tanggal dan waktu respons, nama dan versi server, serta revisi protokol MIME. MIME adalah spesifikasi Ekstensi Email Internet Serbaguna yang digunakan untuk mengirim berbagai jenis data melalui email. Secara singkat pendekatan dasar CGI dapat dikelompokkan menjadi dua kategori. Mereka mengirim data ke program gateway dan mengembalikan data ke klien web. Kerugian dari Skrip CGI adalah menghasilkan banyak beban pada server web dan program yang ditulis dengan buruk cenderung jatuh ke dalam perulangan tanpa akhir sehingga mengorbankan waktu prosesor server web. Perulangan tanpa akhir ini berlanjut hingga administrator sistem masuk

dan mematikan skrip yang salah. Alat skrip berbasis browser menggunakan prosesor secara lokal dan bukan server Web itu sendiri sehingga kurang intensif pada server Web.

**Java**

Java adalah bahasa pemrograman generasi ketiga tingkat tinggi untuk menulis aplikasi komputer. Java berbagi banyak sintaks C tetapi berbeda dari bahasa C. Keunikan bahasa Java adalah menyediakan program khusus yang disebut applet. Applet dapat diunduh dari Internet dan dapat dimainkan dengan aman di browser web. Java adalah bahasa platform independen untuk pengembangan aplikasi. Disebut demikian karena program Java menghasilkan format khusus yang disebut kode byte yang ditulis dalam heksadesimal byte demi byte, yang terlihat seperti kode bahasa mesin dan sama persis di setiap platform. Namun, program Java yang dikompilasi menjadi kode byte memerlukan penerjemah untuk mengeksekusinya pada platform apa pun. Java menyediakan alokasi dan de-alokasi memori otomatis untuk menjadikannya bahasa yang sederhana dan bebas bug. Beberapa fitur bahasa Java diberikan sebagai berikut:

- Java adalah pemrograman Berorientasi Objek sehingga lebih sederhana dan mudah untuk membaca program. Ini memberikan penggunaan kembali kode yang lebih efisien.
- Java adalah bahasa platform independen yang mana program Java tidak pernah benar-benar dijalankan secara asli pada mesin host. Sebaliknya, program asli khusus yang disebut penerjemah Java membaca kode byte dan mengeksekusi instruksi mesin asli yang sesuai.
- Java dianggap sebagai eksekusi kode yang aman dan terjamin di seluruh jaringan, meskipun sumber kode tersebut tidak tepercaya dan mungkin berbahaya.
- Java adalah bahasa berkinerja tinggi di mana kode byte Java dikompilasi dengan cepat ke kode sementara C++ menggunakan kompiler just-in-time. Kompiler arsitektur mesin asli untuk Java digunakan untuk menghasilkan kode yang dapat dieksekusi yang tidak memerlukan penerjemah terpisah.
- Java bersifat multi-thread dan satu program Java dapat mengeksekusi banyak thread berbeda secara mandiri dan terus-menerus.
- Java adalah sampah yang dikumpulkan di mana memori dialokasikan sesuai kebutuhan dan diambil kembali oleh pengumpul sampah ketika tidak lagi diperlukan.

## 12.4 MULTIMEDIA

Seperti namanya, multimedia adalah seperangkat lebih dari satu elemen media yang digunakan untuk menghasilkan cara komunikasi yang konkrit dan lebih terstruktur. Dengan kata lain multimedia adalah penggunaan data secara simultan dari berbagai sumber. Sumber-sumber ini dalam multimedia dikenal sebagai elemen media. Dengan perkembangan dan perubahan teknologi informasi yang sangat cepat, Multimedia telah menjadi bagian penting dalam dunia komputer. Pentingnya hal ini telah disadari di hampir semua lapisan masyarakat, baik itu pendidikan, bioskop, periklanan, fashion dan sebagainya.

Sepanjang tahun 1960an, 1970an dan 1980an, komputer telah dibatasi untuk menangani dua jenis data utama – kata dan angka. Namun teknologi informasi yang mutakhir memperkenalkan sistem yang lebih cepat yang mampu menangani grafik, audio, animasi dan video. Dan seluruh dunia terkejut dengan kekuatan multimedia. Multimedia adalah cawan suci jaringan. Hal ini membawa tantangan teknis yang sangat besar dalam menyediakan video (interaktif) sesuai permintaan ke setiap rumah dan keuntungan yang sama besarnya. Secara harfiah, multimedia hanyalah dua media atau lebih. Secara umum, istilah multimedia berarti gabungan dua atau lebih media yang berkesinambungan. Dalam praktiknya, kedua media tersebut biasanya berupa audio dan video.

**Elemen Multimedia**

Ada banyak jenis komponen multimedia. Ini adalah audio, video, gambar, animasi, dll.

1. **Teks**: Penyertaan informasi tekstual dalam multimedia merupakan langkah dasar menuju pengembangan perangkat lunak multimedia. Teks dapat berupa jenis apa pun, dapat berupa kata, satu baris, atau paragraf. Data tekstual untuk multimedia dapat dikembangkan menggunakan editor teks apa pun. Namun untuk memberikan efek khusus diperlukan software grafis yang mendukung pekerjaan tersebut. Bahkan seseorang dapat menggunakan perangkat lunak pengolah kata paling populer untuk membuat data tekstual untuk dimasukkan dalam multimedia. Teks dapat memiliki jenis, ukuran, warna dan gaya yang berbeda untuk memenuhi kebutuhan profesional perangkat lunak multimedia.
2. **Grafik:** Elemen lain yang menarik dalam multimedia adalah grafis. Faktanya, dengan mempertimbangkan sifat manusia, suatu subjek lebih dijelaskan dengan semacam representasi gambar/grafis, dibandingkan dengan potongan besar teks. Hal ini juga membantu mengembangkan layar multimedia yang bersih, sedangkan penggunaan teks dalam jumlah besar di layar membuat presentasi menjadi membosankan.
3. **Animasi**: Gambar bergerak mempunyai efek yang sangat kuat pada penglihatan tepi manusia. Berikut adalah beberapa poin untuk popularitasnya.
   (a) Animasi adalah sekumpulan keadaan statis, yang saling berhubungan dengan transisi.
   (b) Menunjukkan dimensi dalam transisi
   (c) Mengilustrasikan perubahan seiring berjalannya waktu
   (d) Menggandakan tampilan
   (e) Memperkaya representasi grafis
   (f) memvisualisasikan struktur tiga dimensi
4. **Audio**: Representasi, pemrosesan, penyimpanan dan transmisi sinyal audio adalah bagian utama dari studi sistem multimedia. Rentang frekuensi telinga manusia berkisar antara 20 Hz hingga 20K Hz. Telinga sangat sensitif terhadap variasi suara yang hanya berlangsung beberapa milidetik. Sebaliknya, mata tidak memperhatikan perubahan tingkat cahaya yang hanya berlangsung beberapa milidetik. Jadi, jitter yang hanya beberapa milidetik selama transmisi multimedia lebih mempengaruhi kualitas suara yang dirasakan dibandingkan kualitas gambar yang dirasakan.

5. **Video**: Mata manusia memiliki sifat yang ketika sebuah gambar dipantulkan ke retina, gambar tersebut dipertahankan selama beberapa milidetik sebelum membusuk. Jika rangkaian gambar di-flash pada 50 gambar atau lebih/detik, mata tidak menyadari bahwa ia sedang melihat gambar terpisah. Semua sistem TV memanfaatkan properti ini untuk menghasilkan gambar bergerak.
   Saat ini, video dapat digunakan untuk:
   a. Mempromosikan acara televisi, film, atau media non-komputer lainnya yang biasanya menggunakan trailer dalam iklannya.
   b. Memberikan kesan kepada pengguna tentang kepribadian pembicara.
   c. Menampilkan benda-benda yang bergerak. Misalnya, klip dari film. Demo produk produk fisik juga cocok untuk video.

**Penggunaan Multimedia**

Menempatkan media dalam perspektif dalam proses pembelajaran merupakan peran penting guru dan profesional perpustakaan. Berikut ini adalah kemungkinan bidang penerapan multimedia:

- Dapat digunakan sebagai penguat
- Dapat digunakan untuk memperjelas atau melambangkan suatu konsep
- Menciptakan sikap positif individu terhadap apa yang dipelajarinya dan proses pembelajaran itu sendiri dapat ditingkatkan.
- Isi suatu topik dapat dipilih dan diatur dengan lebih cermat
- Proses belajar mengajar menjadi lebih menarik dan interaktif
- Penyampaian pengajaran dapat lebih terstandarisasi.
- Lamanya waktu yang diperlukan untuk pengajaran dapat dikurangi.
- Instruksi dapat diberikan kapan dan dimana diinginkan atau diperlukan.

**Ringkasan**

- Lapisan paling atas dari model OSI menyediakan sejumlah layanan kepada pengguna menggunakan protokol TCP/IP. Antarmuka Socket digunakan untuk menyediakan pendekatan standar yang terdokumentasi dengan baik untuk mengakses sumber daya jaringan kernel.
- Aplikasi TCP/IP beroperasi pada lapisan aplikasi atau proses hierarki TCP/IP dan membagi aplikasi menjadi komponen server dan klien.
- Sistem Nama Domain (DNS) menyediakan terjemahan cepat teks alamat IP dalam sepersekian detik dari direktori yang berisi miliaran alamat tersebut. Hal ini dapat dimungkinkan dengan menggunakan konsep Domain, yang menggunakan pengaturan hierarki terjemahan alamat teks. Server yang memelihara alamat didistribusikan dan memiliki lokasi di seluruh dunia.
- Surat elektronik adalah salah satu layanan jaringan paling populer dan menggunakan agen pengguna dan agen transfer pesan untuk mengangkut pesan yang dibuat oleh pengguna ke kotak surat tujuan, mungkin pada mesin jarak jauh. Aplikasi multimedia telah meramaikan kehidupan di halaman web sehingga menjadikannya interaktif.

Konvergensi berbagai media seperti teks, gambar, video dan suara menjadi satu media telah memberikan kontribusi yang sangat besar bagi pertumbuhan Internet dan www.

- Penerapan paket multimedia dapat ditemukan di semua lapisan masyarakat. Dengan kemajuan dan inovasi dalam alat presentasi multimedia, aplikasi multimedia telah memberikan kesan realitas virtual kepada pengguna akhirnya.
- Simple Mail Transfer Protocol (SMTP) digunakan untuk mentransfer email dari satu sistem komputer ke sistem komputer lain yang terhubung ke jaringan yang sama atau jaringan berbeda dan menggunakan pengiriman end-to-end di mana mesin klien SMTP menghubungi server SMTP host tujuan secara langsung untuk mengirimkan surat.
- HTTP menggunakan layanan transport TCP melalui soket untuk mentransfer data. Klien HTTP memulai koneksi TCP dengan menggunakan soket pada port 80 ke server HTTP. Setelah menerima koneksi dari klien, server merespons kembali permintaan klien dengan halaman HTML dan objeknya. Dengan demikian, halaman HTML dan objek lainnya dipertukarkan antara browser klien dan server web. Setelah melayani permintaan klien, koneksi TCP diakhiri.
- Multimedia tidak lain adalah pengolahan dan penyajian informasi secara lebih terstruktur dan mudah dipahami dengan menggunakan lebih dari satu media seperti teks, grafik, animasi, audio dan video.

**Latihan Soal**

Isilah bagian yang kosong:

1. Perintah SMTP terdiri dari string..... yang dapat dibaca manusia.
2. Kotak surat dikaitkan dengan satu id login dalam..... untuk menyimpan email pengguna.
3. .....mengacu pada alias untuk sekumpulan penerima.
4. Server DNS memelihara database baik dalam bentuk tekstual maupun notasi .....
5. .....dapat mengakomodasi hampir semua jenis organisasi dengan memungkinkan setiap kelompok memilih antara hierarki penamaan geografis atau organisasi.
6. .....adalah jenis protokol push sedangkan POP3 dan IMAP adalah protokol tarik.

Nyatakan apakah pernyataan berikut ini benar atau salah:

1. Browser adalah perangkat lunak yang digunakan komputer Anda untuk melihat dokumen WWW dan mengakses Internet.
2. Hyperlink memungkinkan file elektronik di Web dihubungkan sehingga Anda dapat berpindah dengan mudah di antara file-file tersebut menggunakan protokol FTP.
3. Dokumen hypermedia tidak hanya menyediakan tautan ke bagian teks lain, namun juga menyediakan tautan ke bentuk media lain seperti suara, gambar, dan film.
4. www menggunakan protokol berorientasi koneksi.
5. Protokol yang digunakan oleh klien web dan server web untuk berkomunikasi satu sama lain disebut HTTP.
6. Dokumen di World Wide Web diklasifikasikan menjadi lima jenis.

7. Halaman web statis menampilkan informasi yang sama untuk semua pengguna web dari semua konteks dan menyediakan link hypertext untuk melakukan navigasi.
8. Halaman web dinamis menggunakan tiga jenis interaktivitas.
9. Halaman web dinamis skrip sisi server dirancang dengan bantuan bahasa sisi server seperti PHP, Perl, ASP, JSP, dll.

Uraian

1. Tulis catatan singkat tentang DNS.
2. Apa itu koneksi HTTP dan apa perbedaannya?
3. Apa saja jenis identifikasi server pengguna? Jelaskan secara singkat.
4. Apa perbedaan www dengan Internet? Menjelaskan.
5. Bagaimana cara kerja SMTP dalam mentransfer email dari satu sistem komputer ke sistem komputer lain yang terhubung ke jaringan berbeda?
6. Apa itu server web? Bagaimana cara kerjanya?
7. Jelaskan perbedaan dan persamaan antara URL dan alamat email.
8. Jelaskan bagaimana email disimpan dan dikirimkan oleh server POP dan SMTP.
9. Jelaskan konsep multimedia? Apa saja macam-macam komponen multimedia?

# BAB 13
# LAPISAN SESI DAN LAPISAN PRESENTASI

**Pendahuluan**

Tiga lapisan teratas yaitu lapisan sesi, presentasi dan aplikasi dianggap sebagai lapisan pengguna atau aplikasi model OSI. Mereka diimplementasikan dalam perangkat lunak. Di sebagian besar protokol, fungsi lapisan-lapisan ini dikonvergensi menjadi satu lapisan yang disebut lapisan aplikasi. TCP adalah salah satu contoh dari jenis protokol tersebut.

Lapisan sesi terletak di atas lapisan transport dan dimaksudkan untuk memberikan layanan nilai tambah pada layanan lapisan transport yang mendasarinya. Lapisan sesi membuat, mengelola dan melepaskan sesi komunikasi antara entitas lapisan presentasi di mesin sumber dan tujuan. Protokol lapisan sesi mengelola sesi komunikasi termasuk membuat permintaan layanan sesi komunikasi dan respons layanan, keamanan dan otentikasi. Mereka terjadi antara aplikasi yang terletak di mesin sumber dan tujuan dalam jaringan. Protocol Data Unit (PDU) adalah data pada lapisan ini. Lapisan ini merespons permintaan layanan dari lapisan presentasi dan mengeluarkan permintaan layanan ke lapisan transport.

Lapisan presentasi memelihara dan memelihara makna informasi yang dikirimkan melalui jaringan. Ini mengkodekan data dengan berbagai cara, misalnya kompresi atau enkripsi data. Demikian pula, mesin penerima akan mengubah pengkodean kembali ke bentuk aslinya. Lapisan aplikasi, lapisan tertinggi model OSI berinteraksi dengan aplikasi perangkat lunak yang memungkinkan mesin sumber dan tujuan berkomunikasi dengan baik.

## 13.1 LAPISAN SESI MASALAH DESAIN

Lapisan sesi adalah lapisan tertipis dengan jumlah protokol paling sedikit dalam model OSI. Lapisan sesi bertujuan untuk membangun, memelihara dan menyinkronkan dialog antara lapisan atas yang berkomunikasi. Komunikasi dapat terjadi antara pengguna atau aplikasi.
Fungsi lapisan sesi adalah sebagai berikut:

- Sesi untuk mengangkut komunikasi: Untuk mengoordinasikan koneksi dan melepaskan koneksi dialog antara aplikasi yang berkomunikasi.
- Manajemen Dialog: Untuk mengoordinasikan siapa yang mengirim, kapan.
- Manajemen Aktivitas: Untuk memastikan transfer data selesai sebelum sesi ditutup.
- Sinkronisasi: Untuk menyediakan titik sinkronisasi untuk transfer data.
- Komunikasi Sesi ke Transportasi: Lapisan sesi membantu mengoordinasikan koneksi dan pelepasan koneksi dialog antara aplikasi yang berkomunikasi, ia berkomunikasi dengan lapisan transport. Komunikasinya bisa satu ke satu, banyak ke satu, dan satu ke banyak. Dalam satu ke satu, satu koneksi lapisan sesi dibuat untuk setiap koneksi lapisan transport. Dalam banyak ke satu, beberapa koneksi lapisan sesi dibagikan dengan layanan dari satu koneksi lapisan transport. Komunikasi koneksi satu ke banyak

diatur ketika satu koneksi lapisan sesi memanggil banyak koneksi lapisan transport untuk menangani layanan.

- Manajemen Dialog: Lapisan sesi bertujuan untuk memutuskan giliran siapa yang berbicara. Beberapa aplikasi beroperasi dalam mode setengah dupleks. Half duplex menyediakan komunikasi alternatif dua sisi antara mengirim dan menerima pesan dan tidak pernah mengirim data secara bersamaan. Manajemen dialog diimplementasikan melalui penggunaan token data yang dikirimkan bolak-balik untuk memberikan hak kepada pengguna untuk mengirimkan hanya ketika ia memiliki token tersebut.
- Manajemen Aktivitas: Lapisan sesi memungkinkan pengguna untuk membatasi data menjadi unit logis yang disebut aktivitas. Setiap aktivitas diperlakukan sebagai aktivitas terpisah dan independen dari aktivitas sebelum dan sesudah aktivitas tersebut. Aktivitas digunakan untuk membatasi file transfer multi-file. Aktivitas digunakan untuk karantina, mengumpulkan semua data pertukaran multi-pesan sebelum memprosesnya. Aplikasi penerima mulai memproses data hanya setelah semua data tiba. Hal ini memastikan bahwa semua atau tidak satupun dari serangkaian operasi dilakukan. Misalnya, transaksi bank mungkin melibatkan penguncian catatan, memperbarui nilai, dan kemudian membuka kunci catatan. Ketika aplikasi memproses operasi pertama, namun tidak dapat menerima operasi yang tersisa karena kegagalan klien atau jaringan. Catatan akan tetap terkunci selamanya. Karantina memecahkan masalah ini.

Penanganan pengecualian: Ini adalah mekanisme tujuan umum untuk melaporkan kesalahan.

## 13.2 LAPISAN SESI SINKRONISASI

Seringkali selama transmisi data, beberapa jenis kesalahan mungkin muncul karena berbagai alasan, oleh karena itu lapisan sesi bertujuan untuk menyinkronkan transmisi data sehingga penerima menerima unit data sesuai keinginan dan bukan dalam bentuk yang terdistorsi. Ini memerlukan sinkronisasi.

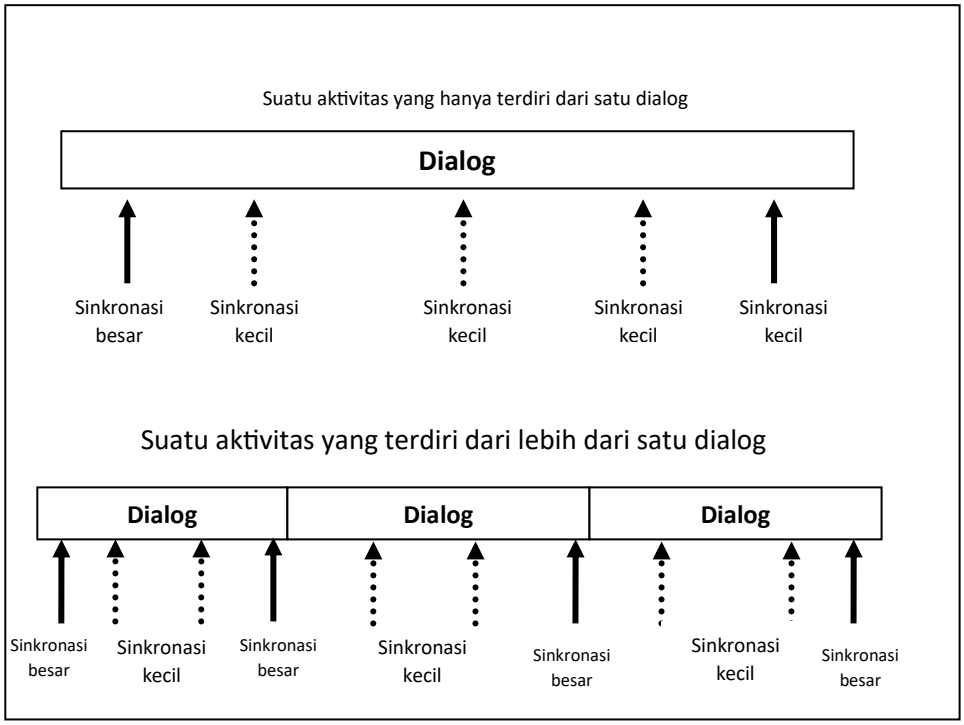
Misalnya, jika Anda melakukan transfer file selama satu jam antara dua mesin, dan kerusakan jaringan terjadi kira-kira setiap 30 menit, Anda mungkin tidak akan pernah dapat menyelesaikan transfer file. Setelah setiap transfer dibatalkan, Anda harus memulai dari awal lagi. Untuk menghindari masalah ini, Anda dapat memperlakukan seluruh transfer file sebagai aktivitas tunggal dengan titik pemeriksaan dimasukkan ke dalam aliran data. Dengan begitu, jika terjadi kerusakan, lapisan sesi dapat melakukan sinkronisasi ke pos pemeriksaan sebelumnya. Pos pemeriksaan ini disebut titik sinkronisasi.

Ada dua jenis titik sinkronisasi: titik sinkronisasi mayor dan minor. Titik sinkronisasi mayor yang disisipkan oleh pihak yang berkomunikasi harus diakui oleh pihak komunikasi lainnya, sedangkan titik sinkronisasi minor tidak diakui. Bagian sesi yang berada di antara dua titik sinkronisasi utama disebut unit dialog. Operasi pengelolaan keseluruhan aktivitas disebut manajemen aktivitas. Suatu aktivitas dapat terdiri dari satu atau lebih unit dialog.

Sinkronisasi dilakukan dengan menggunakan nomor urut. Protokol lapisan sesi menyediakan titik sinkronisasi mayor dan minor. Titik sinkronisasi utama membagi pesan

menjadi serangkaian dialog. Setiap titik sinkronisasi utama diketahui sebelum sesi dilanjutkan. Ketika kesalahan terjadi, data hanya dipulihkan hingga titik besar terakhir. Aktivitas lapisan sesi dibagi menjadi satu dialog atau beberapa dialog yang dipisahkan oleh titik sinkronisasi utama. Jika melakukan sinkronisasi ulang, seseorang hanya akan kembali ke titik sinkronisasi utama sebelumnya. Selain itu, titik sinkronisasi utama dikenali dengan bantuan pesan eksplisit sehingga membuat penggunaannya menjadi mahal.

Titik sinkronisasi kecil hanyalah penanda dan disisipkan di tengah dialog. Mereka, tergantung pada aplikasinya, mungkin memerlukan pengakuan atau tidak. Ini adalah zona keamanan untuk memulihkan data dari satu atau lebih titik sinkronisasi kecil dalam dialog ketika terjadi kesalahan. Catatan Perlu dicatat secara hati-hati bahwa titik-titik sinkronisasi utama perlu diketahui sehingga kendali dapat memulai transmisi ulang data dari titik titik-titik sinkronisasi besar terakhir tepat sebelum titik terjadinya kesalahan. Titik sinkronisasi kecil digunakan sebagai selimut keamanan dan oleh karena itu tidak perlu diketahui. Ketika kesalahan terjadi, kontrol kembali ke satu atau lebih titik sinkronisasi kecil untuk mengirimkan ulang data.




**Gambar 13.1 Konsep titik sinkronisasi dengan jelas.**

## 13.3 LAPISAN PRESENTASI

Lapisan presentasi dalam model jaringan berkaitan dengan sintaksis dan semantik informasi yang dipertukarkan antara dua sistem. Lapisan presentasi menentukan bagaimana komputer mewakili format data seperti ASCII, GIF, dll dan mengimplementasikan fungsi pengkodean dan konversi untuk data lapisan aplikasi untuk memastikan bahwa data yang dikirim dari lapisan aplikasi mesin sumber akan dapat dibaca oleh lapisan aplikasi mesin tujuan. Metode pengkodean dan konversi lapisan presentasi menyediakan format

representasi data umum, konversi format representasi karakter, teknik kompresi data umum, dan teknik enkripsi data umum.

Format representasi data umum yang mungkin melibatkan penggunaan format gambar, suara, dan video standar memungkinkan pertukaran data aplikasi antara berbagai jenis sistem komputer dari mesin sumber ke mesin tujuan. Mesin yang bertukar data mungkin menggunakan representasi teks dan data yang berbeda seperti EBCDIC dan ASCII. Teknik kompresi data memungkinkan data terkompresi di mesin sumber didekompresi dengan benar di mesin tujuan. Demikian pula, teknik enkripsi data memungkinkan data yang dienkripsi di mesin sumber dapat didekripsi dengan benar di mesin tujuan. Dengan demikian, lapisan presentasi membuat lapisan aplikasi bebas dari tanggung jawab perbedaan sintaksis dalam representasi data dalam mesin sumber dan tujuan atau sistem pengguna akhir.

## 13.4 LAPISAN PRESENTASI MASALAH DESAIN

Lapisan presentasi berhubungan dengan penerjemahan, enkripsi/dekripsi, otentikasi dan kompresi yang dijelaskan sebagai berikut:

- **Terjemahan**: Ini mengubah struktur data kompleks yang digunakan oleh aplikasi string, bilangan bulat, struktur, dll. menjadi aliran byte yang dapat ditransmisikan melalui jaringan. Pesan tersebut direpresentasikan sedemikian rupa sehingga mesin yang berkomunikasi menyetujui format data yang dipertukarkan. Misalnya, kumpulan karakter ASCII atau EBCDIC.

Terjemahannya mungkin langsung atau tidak langsung. Dalam metode penerjemahan langsung, kode ASCII diterjemahkan sebagai EBCDIC di mesin tujuan. Dalam metode tidak langsung, kode ASCII terlebih dahulu diterjemahkan ke format standar pada mesin sumber itu sendiri sebelum dikirimkan. Mesin tujuan mengubahnya menjadi kode EBCDIC. Metode langsung tidak diinginkan karena alasan yang jelas karena mesin tujuan harus berurusan dengan beberapa komputer dalam jaringan dan oleh karena itu diperlukan tabel konversi untuk format data yang berbeda. Metode tidak langsung yang menyertakan Notasi Sintaks Abstrak 1 (ASN.1) direkomendasikan oleh OSI. Metode ini menangani pemformatan, keragaman sifat data seperti teks, program, dll., dan keragaman format penyimpanan data.

**Notasi Sintaks Abstrak**

Notasi Sintaks Abstrak (ASN.1) adalah standar OSI yang menangani masalah representasi, pengkodean, transmisi, dan decoding struktur data. Ini memiliki dua bagian seperti yang diberikan di bawah ini:

1. Sintaks abstrak yang menggambarkan struktur data dengan cara yang jelas. Sintaksnya memungkinkan pengguna untuk menggunakan bilangan bulat, string karakter, dan struktur, bukan bit dan byte.
2. Sintaks transfer yang menjelaskan pengkodean aliran bit objek data ASN.1. Data dan bidang tambahan dikirim untuk menjelaskan jenis data. Di mesin tujuan, operasi sebaliknya diterapkan untuk mengkonversi dari format ASN.1 ke representasi internal mesin tujuan.

Terdapat pendekatan alternatif terhadap representasi data namun memiliki kelemahan. Dalam satu pendekatan, mesin sumber mengubah data ke dalam format yang diharapkan oleh mesin tujuan sehingga mesin tujuan tidak perlu melakukan decoding apa pun. Kerugian dari pendekatan ini adalah setiap mesin sumber perlu mengetahui cara menyandikan data untuk setiap mesin tujuan yang mungkin. Dalam pendekatan lain, ASN.1 mengubah semuanya menjadi bentuk umum yang serupa dengan representasi standar jaringan TCP/IP. Namun kelemahan metode ini adalah komunikasi antara dua mesin identik menghasilkan konversi yang tidak perlu. Bentuk sintaksis abstrak ASN.1 mirip dengan bahasa pemrograman tingkat tinggi lainnya. ASN.1 terdiri dari tipe primitif dan tipe kompleks yang dibangun berdasarkan tipe primitif.

- **Enkripsi/Dekripsi**: Ini berkaitan dengan masalah keamanan dan privasi. Enkripsi digunakan untuk mengacak data sehingga hanya orang yang berwenang yang dapat menguraikan data percakapan. Dekripsi membalikkan proses enkripsi untuk menerjemahkan pesan kembali ke bentuk aslinya. Untuk mengenkripsi data, pengirim di mesin sumber menggunakan algoritma enkripsi dan kunci untuk mengubah teks biasa (pesan asli) menjadi teks tersandi (pesan terenkripsi). Di mesin tujuan, proses sebaliknya terjadi. Penerima memiliki kunci dan algoritma dekripsi untuk menerjemahkan kembali ciphertext menjadi plaintext asli.

  Metode enkripsi dan dekripsi ada dua jenis. Itu adalah metode konvensional dan kunci publik. Pada metode konvensional, kunci enkripsi dan dekripsinya sama dan rahasia. Kerugian dari metode konvensional adalah bahwa algoritma dekripsi selalu merupakan kebalikan dari algoritma enkripsi dan oleh karena itu siapapun yang mengetahui algoritma enkripsi akan dapat menyimpulkan algoritma dekripsi dan dengan demikian kerahasiaan dan privasi pesan terancam. Dalam pendekatan enkripsi kunci publik, setiap pengguna memiliki kunci dan algoritma yang sama untuk enkripsi pesan. Namun, algoritma dekripsi dan kuncinya dirahasiakan. Dengan demikian, pesan tersebut dapat dienkripsi oleh siapa saja; namun, itu dapat didekripsi oleh orang yang berwenang. Algoritma dekripsi dirancang sedemikian rupa sehingga tidak dapat disimpulkan dari kebalikan dari algoritma enkripsi. Selain itu, kunci enkripsi dan dekripsi yang berbeda mempersulit dekripsi pesan oleh orang yang tidak berwenang.
- **Otentikasi**: Ini memverifikasi anteseden dari pihak jarak jauh sebagai pihak yang sebenarnya dan bukan penipu. Artinya pesan tersebut diterima dari orang asli, bukan dari penipu. Tanda tangan digital adalah salah satu dari beberapa pendekatan otentikasi yang menggunakan metode enkripsi kunci publik.
- **Kompresi Data**: Ini memampatkan data untuk mengurangi jumlah data yang dikirimkan sehingga menghemat bandwidth dan uang. Ada tiga metode umum untuk kompresi data. Setiap metode mempertimbangkan bahwa aliran data dapat diubah menjadi representasi yang lebih kompak. Aliran data kompak ini direkonstruksi kembali menjadi data asli di mesin tujuan.
- **Kumpulan Simbol Terhingga**: Dianggap bahwa perpustakaan dengan banyak kantor cabang di mana transaksi hari-hari sebelumnya dikirimkan ke setiap cabang lain

setelah penutupan. Transaksi terdiri dari buku yang sudah diperiksa dan dikembalikan. Pertukaran informasi dapat dilakukan dengan cara berikut:

1. Nama buku, penulisnya, nomor salinan, dll beserta jenis transaksi yang dikirimkan.
2. Perpustakaan perlu memelihara meja kantor yang memberikan nomor ID unik untuk setiap buku di setiap cabang. Transaksi kemudian mengacu pada nomor ID buku, bukan judulnya. Karena ID buku berukuran kecil dan berisi beberapa byte, maka lebih sedikit data yang akan dikirimkan.

Catatan: Dapat dicatat dari uraian di atas bahwa teknik di atas digunakan di seluruh pemrograman dan pointer serta subskrip array sering dipertukarkan untuk menghindari biaya transfer data dalam jumlah besar antar subrutin. Diasumsikan juga bahwa semua objek muncul dengan frekuensi yang sama dan himpunan objek, dalam hal ini buku, adalah berhingga. Saat teks diperiksa, segera diketahui bahwa beberapa kata lebih sering muncul dibandingkan kata lain.

Dengan mengambil contoh dari hal ini, jumlah bit yang diperlukan untuk mewakili suatu dokumen dapat dikurangi dengan menggunakan skema pengkodean yang menggunakan kata-kata kode kecil untuk mewakili kata-kata umum dan kata-kata kode yang lebih panjang untuk mewakili kata-kata yang jarang muncul.

- Pengkodean Huffman: Pengkodean Huffman digunakan untuk mengkodekan simbol-simbol sesuai dengan frekuensi penggunaannya yang dijelaskan sebagai berikut:
  1. Satu set node, satu node per simbol dengan nilai node yang ditentukan oleh probabilitas kemunculannya dalam data dibuat.
  2. Ditemukan dua node yang memiliki nilai terkecil. Mereka dihapus dari himpunan dan sebuah node baru yang memiliki dua node yang dihapus sebagai anak dibuat. Node baru kemudian diberi nilai yang sama dengan jumlah nilai turunannya. Node baru ditambahkan kembali ke kumpulan node.
  3. Langkah 2 diulangi hingga hanya tersisa satu node. Ini menghasilkan sebuah pohon, yang nilai probabilitasnya adalah satu.
  4. Pengkodean setiap simbol dilakukan yaitu jalur dari root ke simbol. Kode 0 digunakan untuk anak kiri dan 1 untuk anak kanan. Dengan demikian, panjang pengkodean setiap simbol sebanding dengan probabilitas relatif kemunculannya.

  Tahukah kamu? Kerugian dari pengkodean Huffman adalah simbol-simbol memiliki panjang yang berbeda-beda sehingga menjadi relatif mahal untuk didekode. Selain itu, kesalahan satu bit saja akan merusak keseluruhan pesan.
- Pengkodean Tergantung Konteks: Ini mengakui bahwa probabilitas kemunculan simbol tertentu berikutnya bergantung pada simbol sebelumnya. Misalnya, probabilitas bahwa P langsung mengikuti M adalah sekitar 4 kali lebih kecil dari probabilitas Q mengikuti M. Kelemahan metode probabilitas bersyarat adalah bertambahnya ruang tabel. Setiap simbol memerlukan tabelnya sendiri untuk memberikan kode simbol-simbol tersebut segera setelahnya. Namun, pendekatan ini memiliki keunggulan dibandingkan pengkodean Huffman. Semua simbol memiliki panjang yang tetap dan

oleh karena itu membuat pengkodean dan penguraian kode menggunakan pencarian tabel menjadi sangat efisien. Ia juga lebih kebal terhadap kesalahan transmisi.

❖ Pengkodean Panjang Proses: Pengkodean panjang proses adalah alternatif untuk menyandikan data yang berisi simbol berulang. Mari kita asumsikan string biner 0 dan 1. Jangka panjang 0 ditangani dengan menggunakan simbol k-bit yang menunjukkan berapa banyak 0 bit yang terjadi antara 1 berturut-turut. Kata kode dari semua contoh berikut:
`000100001010011000000000000000000000000001000000011` (48 bit) terdiri dari run dengan panjang `3, 4, 1, 2, 0, 23, 7 dan 0`. Menggunakan simbol 4-bit, dikodekan sebagai:
`0011 0100 0001 0010 0000 1111 0100 0111, untuk 32 bit dan penghematan 16/48 = 33%.`
Menggunakan simbol 3-bit, akan dikodekan sebagai: `011 100 001 010 000 111 111 111 010 111 000 selama 33 bit.`

**Ringkasan**

- Lapisan sesi terletak di atas lapisan transport dan dimaksudkan untuk memberikan layanan bernilai tambah pada layanan lapisan transport yang mendasarinya. Lapisan sesi membuat, mengelola dan melepaskan sesi komunikasi antara entitas lapisan presentasi di mesin sumber dan tujuan.
- Lapisan sesi mengimplementasikan mekanisme untuk mengelola dialog antara proses aplikasi pengguna akhir. Ini memfasilitasi dalam membuat operasi duplex atau half-duplex untuk mengimplementasikan prosedur check-pointing, penundaan, terminasi, dan restart.
- Titik sinkronisasi yang diperkenalkan sebagai titik referensi dalam aliran kontrol data dan kesalahan di lapisan sesi.
- Titik sinkronisasi utama membagi pesan menjadi serangkaian dialog. Setiap titik sinkronisasi utama diketahui sebelum sesi dilanjutkan. Ketika kesalahan terjadi, data hanya dipulihkan hingga titik besar terakhir.
- Titik sinkronisasi kecil hanyalah penanda dan disisipkan di tengah-tengah dialog. Mereka, tergantung pada aplikasinya, mungkin memerlukan pengakuan atau tidak. Ini adalah zona keamanan untuk memulihkan data dari satu atau lebih titik sinkronisasi kecil dalam dialog ketika terjadi kesalahan.
- Lapisan presentasi berhubungan dengan penerjemahan, enkripsi/dekripsi, otentikasi dan kompresi.
- Enkripsi digunakan untuk mengacak data sehingga hanya orang yang berwenang yang dapat menguraikan data suatu percakapan. Dekripsi membalikkan proses enkripsi untuk menerjemahkan pesan kembali ke bentuk aslinya.

**Latihan Soal**

Isilah bagian yang kosong:

1. Lapisan..... terletak di atas lapisan transport dan dimaksudkan untuk memberikan layanan bernilai tambah pada layanan lapisan transport yang mendasarinya.
2. Lapisan..... memelihara dan memelihara makna informasi yang dikirimkan melalui jaringan.
3. Lapisan..... adalah lapisan tertipis dengan jumlah protokol paling sedikit dalam model OSI.
4. Lapisan sesi memungkinkan pengguna untuk membatasi data menjadi unit logis yang disebut ……
5. Ada..... jenis titik sinkronisasi.
6. Sinkronisasi dilakukan dengan menggunakan..... angka.

Isi bagian yang kosong:

1. Enkripsi/dekripsi dilakukan pada lapisan.....
2. Lapisan..... bertanggung jawab untuk membangun, memelihara, menyinkronkan dan mengakhiri dialog.
3. Lapisan ……. memutus sesi secara tiba-tiba, sedangkan lapisan ..... menyediakan penutupan yang baik.
4. .....poin memulihkan data yang telah terkirim tetapi belum digunakan.
5. .....adalah fungsi utama dari lapisan presentasi.

Uraian

1. Jelaskan secara singkat fungsi lapisan presentasi.
2. Apa perbedaan antara titik sinkronisasi minor dan titik sinkronisasi mayor?
3. Apa saja elemen lapisan presentasi?
4. Jelaskan proses sinkronisasi sehubungan dengan lapisan sesi.
5. Bedakan antara lapisan sesi dan lapisan presentasi.

# BAB 14
# KEAMANAN JARINGAN

**Pendahuluan**

Selama beberapa tahun terakhir, dunia menjadi saling terhubung dengan cara yang tidak terbayangkan sebelumnya. Perusahaan kecil dan besar hadir di WWW dan kantor mereka yang tersebar di seluruh dunia memiliki kolaborasi antar kantor setiap hari. Oleh karena itu, semua interkoneksi ini sangat bergantung pada kemampuan kita untuk melindungi jaringan yang menciptakan koneksi tersebut. Keamanan jaringan adalah topik yang luas dengan pendekatan berlapis-lapis. Hal ini dapat diatasi pada lapisan data link, lapisan jaringan, dan lapisan aplikasi. Masalah yang dimaksud adalah: intrusi dan enkripsi paket, paket IP dan tabel perutean dengan versi pembaruannya, dan bug tingkat host yang terjadi masing-masing pada lapisan data link, lapisan jaringan, dan aplikasi.

Protokol TCP/IP digunakan secara global terlepas dari sifat organisasinya, apakah itu termasuk dalam kategori organisasi umum atau organisasi sensitif keamanan tertentu. Berita atau informasi mengenai peretasan suatu situs web atau portal oleh pihak yang tidak diinginkan sudah menjadi hal yang lumrah saat ini. Hal ini menunjukkan bahwa protokol TCP/IP rentan terhadap intersepsi. Hal ini menimbulkan kebutuhan untuk memastikan keamanan menyeluruh untuk jaringan dalam suatu organisasi. Tugas administrator jaringan harus diperluas untuk mencakup keamanan jaringan secara keseluruhan. Dia harus memastikan bahwa seluruh bagian jaringan ini terlindungi secara memadai dan tindakan keamanan yang memadai telah diterapkan dalam jaringan TCP/IP. Dia harus menyadari kebijakan keamanan yang efektif. Ia juga harus mampu menentukan area risiko utama yang mungkin dihadapi jaringan. Pada dasarnya, area risiko utama ini bervariasi dari satu jaringan ke jaringan lain tergantung pada fungsi organisasi. Oleh karena itu terdapat berbagai aspek terkait keamanan, yang mempunyai implikasi langsung bagi administrator jaringan serta sarana untuk memantau langkah-langkah keamanan yang diterapkan secara efektif dan untuk mengatasi masalah pelanggaran keamanan jika hal itu terjadi.

## 14.1 KEAMANAN JARINGAN

Tujuan utama jaringan adalah untuk berbagi informasi di antara penggunanya yang berada secara lokal atau jarak jauh. Oleh karena itu, ada kemungkinan pengguna yang tidak diinginkan dapat meretas jaringan dan terbukti berbahaya bagi kesehatan jaringan atau pengguna. Ada beberapa poin dasar, yang harus diikuti oleh administrator jaringan untuk memberikan jaringan keamanan yang memadai selain keamanan khusus jaringan seperti dalam kasus e-commerce, dll. Hal ini diberikan di bawah ini:

- Jaringan dirancang untuk berbagi informasi. Oleh karena itu, jaringan harus dikonfigurasi dengan jelas untuk mengidentifikasi informasi yang dapat dibagikan dan informasi yang tidak dapat dibagikan.
- Jaringan juga harus menjelaskan dengan jelas kepada siapa informasi yang dapat dibagikan dapat dibagikan.

- ❖ Dengan meningkatnya keamanan sistem, harga pengelolaannya juga akan meningkat; oleh karena itu tingkat kompromi antara keamanan dan harga harus ditetapkan sesuai dengan persyaratan kebijakan sistem keamanan jaringan. Hal ini sangat bergantung pada tingkat keamanan yang diperlukan untuk diterapkan dalam jaringan, persyaratan keamanan secara keseluruhan, dan penerapan efektif tingkat keamanan yang dipilih.
- ❖ Pembagian tanggung jawab mengenai keamanan jaringan harus didefinisikan dengan jelas antara pengguna dan administrator sistem.
- ❖ Persyaratan keamanan harus dirinci dalam kebijakan keamanan jaringan organisasi yang menunjukkan data berharga dan biaya terkait bagi bisnis.
- ❖ Setelah mendefinisikan kebijakan keamanan jaringan secara rinci dan mengidentifikasi tanggung jawab yang jelas dalam organisasi, administrator sistem harus bertanggung jawab untuk memastikan bahwa kebijakan keamanan diterapkan secara efektif pada lingkungan perusahaan, termasuk infrastruktur jaringan yang ada.

**Tingkat Keamanan**

Tingkat keamanan berisi masalah terkait keamanan dalam bentuk komponen atau modular. Setiap level berisi masalah keamanan spesifik, yang dipecah menjadi beberapa divisi berbeda. Masing-masing divisi atau klasifikasi memberikan representasi tingkat keamanan yang ditentukan dalam kategori umum berikut:

- ➢ Identifikasi dan otentikasi pengguna
- ➢ Kemampuan untuk memantau dan mengaudit aktivitas sistem
- ➢ Penyediaan akses diskresi
- ➢ Pengendalian penggunaan kembali sumber daya
- ➢ Mengidentifikasi area spesifik yang mungkin menjadi sasaran serangan
- ➢ Penyediaan tindakan penanggulangan yang sesuai
- ➢ Tingkat kepercayaan sistem, termasuk arsitektur sistem, desain, implementasi, transportasi, dan kepercayaan dari host lain.

Tahukah kamu? Evolusi tingkat keamanan dapat dilihat dalam berbagai bentuk, yang disumbangkan oleh Departemen Pertahanan AS. Langkah pertama ke arah ini adalah penjabaran Kriteria Evaluasi Sistem Komputer Terpercaya pada bulan Desember 1985 yang populer dengan nama Buku Oranye. Sebagai kelanjutan dari tingkat keamanan Buku Oranye ini, tingkat keamanan lain yang dikenal sebagai Interpretasi Jaringan Tepercaya dari Kriteria Evaluasi Sistem Komputer Tepercaya atau Buku Merah dijelaskan pada bulan Juli 1987.

Tingkat keamanan berisi masalah terkait keamanan dalam bentuk komponen atau modular. Setiap level berisi masalah keamanan spesifik, yang dipecah menjadi beberapa divisi berbeda. Masing-masing divisi atau klasifikasi memberikan representasi tingkat keamanan yang ditentukan dalam kategori umum berikut:

- ☞ Identifikasi dan otentikasi pengguna
- ☞ Kemampuan untuk memantau dan mengaudit aktivitas sistem
- ☞ Penyediaan akses diskresi
- ☞ Pengendalian penggunaan kembali sumber daya
- ☞ Mengidentifikasi area spesifik yang mungkin menjadi sasaran serangan

- ☞ Penyediaan tindakan penanggulangan yang sesuai
- ☞ Tingkat kepercayaan sistem, termasuk arsitektur sistem, desain, implementasi, transportasi, dan kepercayaan dari host lain.

## 14.2 KEAMANAN DATA

Keamanan data berkaitan dengan perlindungan data yang terdapat dalam suatu file atau banyak file di komputer baik secara mandiri maupun dalam jaringan dari intersepsi yang tidak sah dengan memberikan semacam keamanan.

Dalam sistem pos, kartu pos sebagai pembawa informasi terbuka untuk semua orang. Itu tidak memiliki langkah-langkah keamanan apa pun. Amplop digunakan untuk menyembunyikan informasi dari orang lain. Artinya amplop di sini berfungsi sebagai alat pengaman. Oleh karena itu, kartu pos dan amplop memiliki tujuan berbeda dalam hal keamanan. Kedua kasus khusus ini memulai tindakan serupa untuk menyelesaikan masalah terkait keamanan dalam komunikasi data. Email terbuka untuk semua orang sebagai kartu pos. Mengikuti contoh amplop dalam sistem pos akan memungkinkan pengguna mengamankan setidaknya sebagian data mereka.

Perlindungan akses yang diberikan oleh kata sandi masuk bukanlah sistem bukti penuh dan ini dapat dengan mudah dilewati. Metode yang dilewati termasuk mem-boot dari disket atau menghubungkan hard drive yang dicuri sebagai hard drive sekunder ke komputer lain. Dengan cara ini, data penting apa pun dapat diakses dengan mudah. Akibatnya, enkripsi informasi tampaknya menjadi satu-satunya cara efektif untuk melindungi data agar tidak masuk atau disadap oleh orang yang tidak berwenang. Enkripsi harus dikembangkan dengan filosofi untuk menjamin keamanan data yang andal dan hampir tidak mungkin untuk mendekripsi data tanpa kata sandi yang tepat atau pengguna yang tepat. Kelemahan utama enkripsi berbasis kata sandi mencakup hilangnya kata sandi atau pendaftaran kata sandi yang salah karena kesalahan ejaan atau kesalahan manusia lainnya. Dalam hal ini, memulihkan data menjadi sangat mustahil. Ada aturan lain untuk menghindari situasi seperti itu.

## 14.3 ANCAMAN KEAMANAN

Akses tidak valid ke host dapat dicegah sampai batas tertentu dalam kasus host konvensional ke terminal karena jumlah terminal yang terhubung terbatas. Situasinya sangat berbeda dalam kasus Internet dimana Internet memungkinkan akses dari terminal mana pun yang terhubung pada jaringan. Oleh karena itu hal ini memerlukan langkah-langkah keamanan yang tepat. Di bawah ini adalah daftar beberapa ancaman yang sering terjadi di jaringan:

1. **Virus dan Worm**: Istilah virus merujuk secara khusus pada malware yang memasukkan kode berbahaya ke dalam dokumen atau program yang ada. Ia menyebar dengan berbagai cara. Namun virus masih dianggap sebagai jenis ancaman keamanan jaringan yang paling umum. Hampir 90 persen virus menyebar melalui lampiran di email. Namun, tindakan pengguna yang berhati-hati dapat mencegah penyebaran virus karena virus memerlukan tindakan pengguna untuk memasukkan dirinya ke dalam komputer. Oleh karena itu disarankan agar jangan pernah membuka lampiran email,

yang tidak diharapkan, meskipun pengirimnya tampaknya dikenal. Namun, tindakan pencegahan ini tidak akan banyak membantu menghentikan worm menginfeksi jaringan karena worm tidak memerlukan file host dan dapat menyebar dengan sendirinya. Ketika mereka menginfeksi komputer, mereka sering membuat salinannya dengan cepat dan menginfeksi seluruh jaringan dalam beberapa jam. Untuk menghindari serangan virus dan worm, sebaiknya gunakan software anti virus versi terbaru.

2. **Trojan Horses**: Serangan malware ini menyamar sebagai sesuatu yang tidak bersalah seperti permainan komputer atau halaman hasil pencarian. Setelah terinstal di komputer, kuda Troya dapat mengunduh dan menginstal keylogger ke komputer yang terinfeksi untuk mencatat setiap penekanan tombol oleh pengguna komputer, sehingga mencuri rincian penting dari pengguna. Mereka biasanya menyembunyikan diri dalam perangkat lunak gratis yang dapat diunduh di sebuah situs web. Pengguna harus berhenti mengunduh freeware. Seringkali terlihat bahwa organisasi memblokir perangkat lunak unduhan gratis untuk mencegah serangan kuda Troya. Kadang-kadang, komputer yang terinfeksi Trojan Horse perlu diformat ulang, oleh karena itu, disarankan agar langkah-langkah pencegahan perlu diterapkan secara efektif daripada menyembuhkan sistem komputer yang terinfeksi.
3. **Spam**: Spam mencakup 70 hingga 84 persen email harian yang dikirim ke seluruh dunia yang menuntut kebutuhan sumber daya TI yang semakin meningkat untuk menyaring ancaman yang menjengkelkan dan berpotensi berbahaya ini. Email spam terdiri dari email yang tidak diminta yang mempromosikan produk dan serangan spam terkoordinasi yang menghabiskan begitu banyak bandwidth di jaringan sehingga menyebabkan kerusakan. Spam mungkin menggunakan teknik spam “layanan berita”, yang menggunakan judul berita sah untuk mengelabui penerima agar membuka email spam. Filter email yang baik digunakan untuk menyaring spam. Dan banyak hal yang lolos dapat dihindari dengan menjauhi email. Harus ada pemeriksaan untuk penandatanganan layanan online atau freebie apa pun. Sistem penamaan untuk membuat akun email tidak boleh mudah ditebak karena semakin banyak pelaku spam yang menelusuri daftar nama umum untuk mengumpulkan email menjadi spam.
4. **Phishing:** Email dengan judul seperti, “URGENT: Perbarui Status Akun” adalah upaya pelaku spam untuk “memphis” rincian akun. Phishing mengacu pada email spam untuk mengelabui penerima agar mengeklik tautan ke situs web yang tidak aman dan memberikan rincian yang menganggap situs web tersebut asli. Biasanya, upaya phishing dilakukan untuk mencuri informasi akun situs e-commerce seperti bank, eBay, atau situs web lembaga keuangan biasa. Email phishing menipu pengguna untuk mengklik link, yang akan membawa pengguna ke halaman di mana pengguna diminta memasukkan kembali semua detail akunnya termasuk nomor kartu kredit dan/atau kata sandi. Situs web ini bukanlah situs sebenarnya, meskipun tampilannya mirip. Untuk melindungi jaringan, pengguna harus berhati-hati dan tidak suka membuka dan memberikan rincian penting yang diminta oleh lembaga keuangan mana pun. Mereka

harus memastikan integritasnya sebelum memberikan rincian tersebut. Lembaga keuangan juga harus mendidik karyawannya tentang cara paling umum yang dilakukan peretas untuk mencoba melakukan phishing terhadap informasi akun.

5. **Packet Sniffers**: Packet sniffer adalah teknik yang digunakan untuk menangkap aliran data melalui jaringan untuk mendapatkan data sensitif seperti nama pengguna, kata sandi, nomor kartu kredit, dll. Jadi, packet sniffer adalah bentuk ancaman yang lebih berbahaya terhadap keamanan jaringan. Pengendus paket memantau dan mencatat rincian yang datang dari dan pergi ke komputer melalui jaringan yang disusupi. Untuk mendapatkan akses ke suatu jaringan, packet sniffer menggunakan honeypots. Itu hanyalah titik akses wifi tidak aman yang dibuat peretas untuk menjebak pengguna yang menggunakannya. Membuat pengguna sadar akan ancaman packet sniffer adalah kebijakan pencegahan terbaik. Pengguna harus berhati-hati untuk tidak mengakses Internet melalui koneksi yang tidak aman. Kegagalan dalam teknik packet sniffer akan menyebabkan kompromi dengan data jaringan yang sensitif. Selain itu, pengguna harus menggunakan berbagai nama masuk dan kata sandi yang berbeda untuk mengakses berbagai tingkat keamanan jaringan. Hal ini membantu ketika informasi login disusupi, kerusakan setidaknya dapat dibatasi cakupannya.
6. **Situs Web Berkode Berbahaya**: Situs Web berkode berbahaya membuat situs web yang dapat dipetakan yang memungkinkan pengguna memberikan donasi dan dengan demikian mencuri informasi pribadi yang penting. Situs web berkode berbahaya juga digunakan untuk memasuki jaringan untuk memasang keylogger. Informasi mengenai beberapa lembaga amal harus diperoleh dari situs bersertifikat keamanan.
7. **Serangan Kata Sandi**: 'Serangan Kata Sandi' mencakup sejumlah teknik yang digunakan oleh peretas untuk mencuri kata sandi. Beberapa dari mereka terdaftar di bawah ini:
   - Brute force: Ini adalah metode di mana seorang peretas mencoba menebak kata sandi dengan berulang kali memasukkan kombinasi kata dan frasa baru yang dikumpulkan dari kamus untuk mencuri kata sandi. Mengembangkan nama pengguna dan kata sandi yang sulit ditebak dapat mencegahnya.
   - Packet sniffer : Sudah dibahas diatas.
   - IP-spoofing: Seperti honeypots, IP spoofing melibatkan intersepsi paket data oleh komputer yang berhasil berpura-pura menjadi server/sumber daya tepercaya.
8. **Komputer Zombie dan Botnet**: Komputer 'Zombie' adalah komputer yang ditangkap oleh pelaku spam yang telah menginfeksi komputer yang terhubung ke jaringan dengan malware sehingga bertindak sebagai alat pelaku spam dengan mengirimkan ribuan email dari pemiliknya secara diam-diam. alamat email. Dengan demikian, komputer pengguna yang tidak bersalah mengirimkan ribuan pesan spam tanpa sepengetahuan pengguna. Para pelaku spam mengatur komputer zombie menjadi kelompok-kelompok kecil yang disebut 'botnet'. ‘Botnet’ ini kemudian mengirimkan spam termasuk upaya phishing, virus, dan worm. Botnet biasanya mengirimkan serangan spam dan phishing.

9. **Serangan Denial-of-Service** (DoS): Serangan Denial-of-Service (DoS) adalah metode serangan untuk menolak akses ke halaman web situs web atau jaringan kepada pengguna yang sah.

## 14.4 ENKRIPSI DATA

Enkripsi adalah suatu teknik untuk menyembunyikan data dari orang yang tidak berkepentingan dengan cara menyandikan data agar tidak dapat dilihat dan diubah. Proses enkripsi data melibatkan pengubahan data menjadi data terenkripsi yang disebut ciphertext menggunakan rumus matematika yang disebut algoritma. Algoritme ini menghasilkan kunci dan kemudian merangkum pesan dengan kunci ini. Dua jenis enkripsi seperti asimetris dan simetris sedang populer. Lapisan presentasi berhubungan dengan penerjemahan, enkripsi/dekripsi, otentikasi dan kompresi, yang dijelaskan sebagai berikut:

**Terjemahan**

Ini mengubah struktur data kompleks yang digunakan oleh string aplikasi, bilangan bulat, struktur, dll. menjadi aliran byte yang dapat ditransmisikan melalui jaringan. Pesan tersebut direpresentasikan sedemikian rupa sehingga mesin yang berkomunikasi menyetujui format data yang dipertukarkan. Misalnya, kumpulan karakter ASCII atau EBCDIC.

Terjemahannya mungkin langsung atau tidak langsung. Dalam metode penerjemahan langsung, kode ASCII diterjemahkan sebagai EBCDIC di mesin tujuan. Dalam metode tidak langsung, kode ASCII terlebih dahulu diterjemahkan ke format standar pada mesin sumber itu sendiri sebelum dikirimkan. Mesin tujuan mengubahnya menjadi kode EBCDIC. Metode langsung tidak diinginkan dengan alasan yang jelas karena mesin tujuan harus berurusan dengan beberapa komputer dalam jaringan dan oleh karena itu diharuskan memiliki tabel konversi untuk format data yang berbeda. Metode tidak langsung yang menyertakan Notasi Sintaks Abstrak 1 (ASN.1) direkomendasikan oleh OSI. Metode ini menangani pemformatan, keragaman sifat data seperti teks, program, dll., dan keragaman format penyimpanan data.

**Enkripsi/Dekripsi**

Ini berkaitan dengan masalah keamanan dan privasi. Enkripsi digunakan untuk mengacak data sehingga hanya orang yang berwenang yang dapat menguraikan data percakapan. Dekripsi membalikkan proses enkripsi untuk menerjemahkan pesan kembali ke bentuk aslinya. Untuk mengenkripsi data, pengirim di mesin sumber menggunakan algoritma enkripsi dan kunci untuk mengubah teks biasa (pesan asli) menjadi teks tersandi (pesan terenkripsi). Di mesin tujuan, proses sebaliknya terjadi. Penerima memiliki kunci dan algoritma dekripsi untuk menerjemahkan kembali ciphertext menjadi plaintext asli.

Otentikasi mengacu pada menjaga rahasia dua orang aman dari orang ketiga. Namun, non-penyangkalan memerlukan pembuktian bahwa pengirim pun tidak dapat menyampaikan pesan tersebut. Untuk menerapkan masalah keamanan seperti yang diberikan di atas, teknik yang disebut kriptografi diterapkan. Enkripsi terdiri dari dua jenis:

1. **Enkripsi Asimetris**: Dua kunci yang berhubungan secara matematis yaitu kunci publik dan kunci privat dihasilkan untuk mengenkripsi dan mendekripsi pesan. Enkripsi asimetris dianggap lebih aman dibandingkan enkripsi simetris. Enkripsi kunci asimetris

yang melibatkan pasangan kunci sebagai kunci publik dan privat melibatkan enam langkah utama:

(a) Plaintext: Plaintext adalah pesan teks yang algoritmanya diterapkan.
(b) Algoritma Enkripsi: Menyediakan operasi matematika untuk melakukan substitusi dan transformasi ke teks biasa.
(c) Kunci Publik dan Pribadi: Merupakan sepasang kunci yang digunakan untuk enkripsi dan dekripsi pesan.
(d) Ciphertext: Penerapan algoritma pada plaintext menghasilkan pesan terenkripsi atau acak.
(e) Algoritma Dekripsi: Algoritma ini diterapkan untuk menghasilkan ciphertext dan kunci yang cocok untuk menghasilkan plaintext.

Proses enkripsi mengubah pesan teks menjadi kode hash dengan menggunakan rumus matematika. Kode hash ini kemudian dienkripsi dengan bantuan kunci pribadi pengirim. Kunci pribadi dihasilkan dengan bantuan algoritma. Kode hash terenkripsi dan pesan dienkripsi lagi menggunakan kunci pribadi pengirim. Selanjutnya, pengirim mengenkripsi kunci rahasia tersebut dengan kunci publik penerima, sehingga hanya penerima yang dapat mendekripsinya dengan kunci pribadinya.

Dalam proses dekripsi, penerima menggunakan kunci pribadinya yang panjang dengan kunci rahasianya untuk menguraikan kode hash terenkripsi dan pesan terenkripsi. Penerima kemudian menggunakan kunci publik pengirim untuk mendekripsi kode hash dan memverifikasi identitas pengirim. Penerima menghasilkan kode hash dari pesan tersebut. Jika kode hash yang dihasilkan sama dengan kode hash yang diteruskan oleh pengirim, maka ini memverifikasi bahwa pesan tersebut tidak diubah dalam perjalanan.

2. **Enkripsi Simetris**: Enkripsi simetris juga disebut sebagai enkripsi konvensional atau enkripsi kunci tunggal yang didasarkan pada kunci rahasia, yang dibagikan oleh kedua pihak yang berkomunikasi. Pihak pengirim mengenkripsi teks biasa untuk menyandikan pesan teks menggunakan kunci rahasia. Pihak penerima saat menerima pesan teks sandi menggunakan kunci rahasia yang sama untuk mendekripsinya menjadi teks biasa. Contoh enkripsi simetris adalah algoritma RSA. Metode enkripsi simetris memiliki lima bagian utama berikut:

   (a) Plaintext: Ini adalah pesan teks yang akan dikirim dimana suatu algoritma diterapkan.
   (b) Algoritma Enkripsi: Memungkinkan operasi matematika untuk melakukan substitusi dan transformasi ke teks biasa.
   (c) Kunci Rahasia: Mereka merupakan bagian dari algoritma untuk enkripsi dan dekripsi pesan.
   (d) Ciphertext: Ini adalah pesan terenkripsi yang dihasilkan dengan menerapkan algoritma pada pesan plaintext menggunakan kunci rahasia.
   (e) Algoritma Dekripsi: Ini adalah algoritma enkripsi yang mendekripsi teks sandi menjadi teks biasa dengan menggunakan teks sandi dan kunci rahasia.

Dalam penerapan enkripsi simetris, pengirim dan penerima diharuskan bertukar kunci rahasia secara aman dengan bantuan algoritma enkripsi yang kuat.

**Otentikasi**

Ini memverifikasi bahwa pendahulu dari pihak terpencil adalah pihak yang sebenarnya dan bukan penipu. Artinya pesan tersebut diterima dari orang asli, bukan dari penipu. Tanda tangan digital adalah salah satu dari beberapa pendekatan otentikasi yang menggunakan metode enkripsi kunci publik.

**Kompresi Data**

Ini memampatkan data untuk mengurangi jumlah data yang dikirimkan sehingga menghemat bandwidth dan uang. Ada tiga metode umum untuk kompresi data. Setiap metode mempertimbangkan bahwa aliran data dapat diubah menjadi representasi yang lebih kompak. Aliran data kompak ini direkonstruksi kembali menjadi data asli di mesin tujuan.

**Kumpulan Simbol yang Terbatas**

Perpustakaan dianggap memiliki banyak kantor cabang di mana transaksi hari-hari sebelumnya dikirimkan ke setiap cabang lain setelah penutupan. Transaksi terdiri dari buku yang sudah diperiksa dan dikembalikan. Pertukaran informasi dapat dilakukan dengan cara berikut:

1. Nama buku, penulisnya, nomor salinan, dll beserta jenis transaksi yang dikirimkan.
2. Perpustakaan perlu memelihara meja kantor yang memberikan nomor ID unik untuk setiap buku di setiap cabang. Transaksi kemudian mengacu pada nomor ID buku, bukan judulnya. Karena ID buku berukuran kecil dan berisi beberapa byte, maka lebih sedikit data yang akan dikirimkan.

Catatan Deskripsi di atas bahwa teknik di atas digunakan di seluruh pemrograman dan pointer serta subskrip array sering dipertukarkan untuk menghindari biaya transfer data dalam jumlah besar antar subrutin. Diasumsikan juga bahwa semua objek muncul dengan frekuensi yang sama dan himpunan objek, dalam hal ini buku, adalah berhingga. Saat teks diperiksa, segera diketahui bahwa beberapa kata lebih sering muncul dibandingkan kata lain. Dengan mengambil contoh dari hal ini, jumlah bit yang diperlukan untuk mewakili suatu dokumen dapat dikurangi dengan menggunakan skema pengkodean yang menggunakan kata-kata kode kecil untuk mewakili kata-kata umum dan kata-kata kode yang lebih panjang untuk mewakili kata-kata yang jarang muncul.

## 14.5 KRIPTOGRAFI

Sandi substitusi dan transposisi adalah dua kategori sandi yang digunakan dalam kriptografi klasik. Substitusi dan transposisi berbeda dalam cara penanganan potongan pesan melalui proses enkripsi.

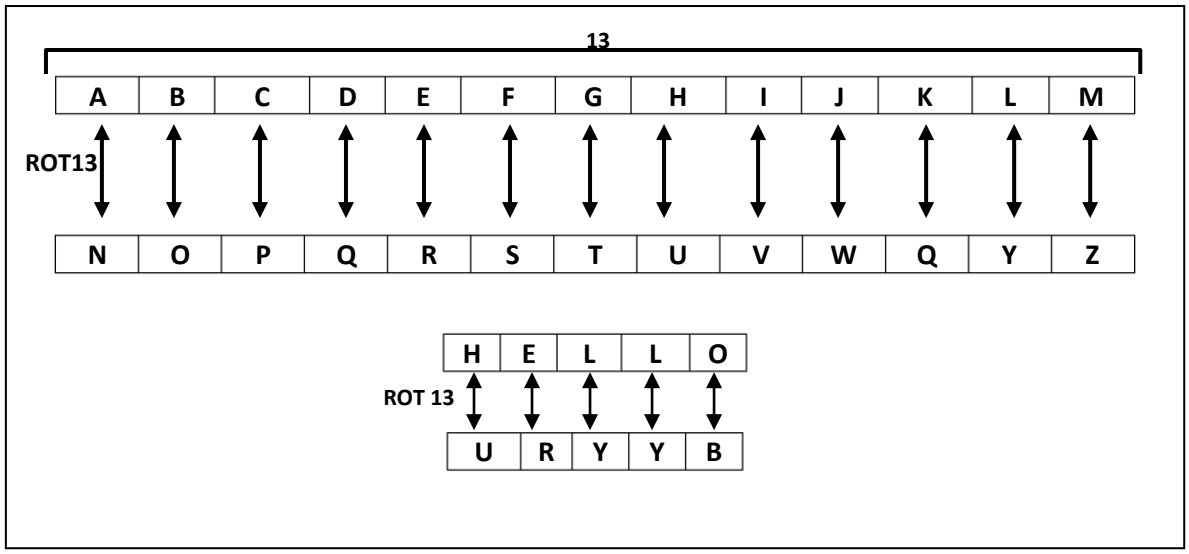
**Sandi Substitusi**

Dalam kriptografi, sandi substitusi adalah metode enkripsi dimana unit teks biasa diganti dengan teks sandi menurut sistem reguler; “satuannya” bisa berupa huruf tunggal (yang paling umum), huruf berpasangan, huruf kembar tiga, huruf campuran di atas, dan sebagainya. Penerima menguraikan teks dengan melakukan substitusi terbalik.

Sandi substitusi dapat dibandingkan dengan sandi transposisi. Dalam sandi transposisi, unit-unit teks biasa disusun ulang dalam urutan yang berbeda dan biasanya cukup rumit, namun unit-unit itu sendiri tidak diubah. Sebaliknya, dalam sandi substitusi, unit-unit teks biasa dipertahankan dalam urutan yang sama dalam teks sandi, namun unit-unit itu sendiri diubah.

Ada beberapa jenis sandi substitusi. Jika sandi beroperasi pada satu huruf, maka disebut sandi substitusi sederhana; sandi yang beroperasi pada kelompok huruf yang lebih besar disebut poligrafik. Sandi monoalfabetik menggunakan substitusi tetap pada seluruh pesan, sedangkan sandi polialfabetik menggunakan sejumlah substitusi pada waktu yang berbeda dalam pesan, di mana satu unit dari teks biasa dipetakan ke salah satu dari beberapa kemungkinan dalam teks tersandi dan sebaliknya.

**Substitusi Sederhana**




**Gambar 14.1 contoh kriptografi subtitusi sederhana**

ROT13 adalah sandi Caesar, sejenis sandi substitusi. Di ROT13, alfabet diputar 13 langkah. Substitusi pada satu huruf—substitusi sederhana—dapat ditunjukkan dengan menuliskan alfabet dalam urutan tertentu untuk mewakili substitusi tersebut. Ini disebut alfabet substitusi. Alfabet sandi dapat digeser atau dibalik (masing-masing membuat sandi Caesar dan Atbash) atau diacak dengan cara yang lebih kompleks, dalam hal ini disebut alfabet campuran atau alfabet gila. Secara tradisional, alfabet campuran dibuat dengan menuliskan kata kunci terlebih dahulu, menghilangkan huruf berulang di dalamnya, lalu menulis semua huruf yang tersisa dalam alfabet.

**Contoh**

Dengan menggunakan sistem ini, kata kunci “zebra” memberi kita huruf berikut:

Alfabet teks biasa: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabet teks sandi: ZEBRASCDFGHIJKLMNOPQTUVWXY

Pesan untuk melarikan diri sekaligus. kita ketahuan!

sandi ke SIAA ZQ LKBA. VA ZOA RFPBLUAOAR!

Secara tradisional, teks sandi ditulis dalam blok dengan panjang tetap, tanpa tanda baca dan spasi; hal ini dilakukan untuk membantu menghindari kesalahan transmisi dan menyamarkan batasan kata dari teks biasa. Blok ini disebut “grup”, dan terkadang “jumlah grup” (yaitu jumlah grup) diberikan sebagai pemeriksaan tambahan. Lima kelompok surat bersifat tradisional, berasal dari saat pesan dikirim melalui telegraf:

SIAAZ QLKBA VAZOA RFPBL UAOAR

Jika panjang pesan tidak habis dibagi lima, pesan tersebut dapat diisi di bagian akhir dengan “nulls”. Ini bisa berupa karakter apa saja yang didekripsi menjadi omong kosong, sehingga penerima dapat dengan mudah mengenalinya dan membuangnya.

Alfabet ciphertext terkadang berbeda dengan alfabet plaintext; misalnya, pada sandi kandang babi, teks sandi terdiri dari sekumpulan simbol yang berasal dari kisi-kisi. Misalnya:


Namun fitur-fitur tersebut tidak banyak berpengaruh pada keamanan suatu skema – paling tidak, rangkaian simbol aneh apa pun dapat ditranskripsikan kembali ke dalam alfabet A-Z dan ditangani seperti biasa. Dalam daftar dan katalog untuk orang penjualan terkadang enkripsi yang sangat sederhana digunakan untuk mengganti angka numerik dengan huruf.

Digit biasa: 1234567890

Alfabet teks sandi: LABA

**Keamanan untuk Sandi Substitusi Sederhana**

Kerugian dari metode kekacauan ini adalah huruf-huruf terakhir dalam alfabet (yang sebagian besar berfrekuensi rendah) cenderung berada di akhir. Cara yang lebih kuat untuk menyusun alfabet campuran adalah dengan melakukan transposisi kolom pada alfabet biasa menggunakan kata kunci, tetapi hal ini jarang dilakukan.

Meskipun jumlah kunci yang mungkin sangat besar (26!H” 288.4, atau sekitar 88 bit), sandi ini tidak terlalu kuat dan mudah dipecah. Asalkan pesannya memiliki panjang yang masuk akal, kriptanalis dapat menyimpulkan kemungkinan arti dari simbol-simbol yang paling umum dengan menganalisis distribusi frekuensi ciphertext—analisis frekuensi. Hal ini memungkinkan pembentukan kata-kata parsial, yang dapat diisi sementara, sehingga semakin memperluas solusi (parsial) (lihat analisis frekuensi untuk demonstrasinya). Dalam beberapa kasus, kata yang mendasarinya juga dapat ditentukan dari pola hurufnya; misalnya, draw, osseous, dan kata-kata dengan keduanya sebagai akar kata adalah satu-satunya kata bahasa Inggris yang umum dengan pola ABBCADB. Banyak orang memecahkan sandi tersebut untuk rekreasi, seperti teka-teki kriptogram di koran.

**Sandi Transposisi**

Dalam kriptografi, sandi transposisi adalah sebuah metode enkripsi di mana posisi yang dipegang oleh unit-unit teks biasa (yang biasanya berupa karakter atau kelompok karakter) digeser menurut sistem yang teratur, sehingga teks tersandi merupakan permutasi dari teks

biasa. Artinya, urutan unitnya diubah. Secara matematis digunakan fungsi bijektif pada posisi karakter untuk mengenkripsi dan fungsi invers untuk mendekripsi.
Berikut beberapa implementasinya:

Sandi transposisi mengenkripsi teks biasa dengan memindahkan potongan-potongan kecil pesan. Anagram adalah sandi transposisi primitif. Tabel ini menunjukkan "VOYAGER" dienkripsi dengan sandi transposisi primitif di mana setiap dua huruf ditukar satu sama lain:

| V | O | Y | A | G | E | R |
|---|---|---|---|---|---|---|
| O | V | A | Y | E | G | R |

**Sandi Substitusi dan Transposisi di Zaman Modern**

Kriptanalisis modern membuat sandi substitusi dan transposisi sederhana menjadi usang. Namun, teknik ini tetap berguna untuk memahami kriptografi dan cara kerja sandi modern yang lebih kompleks.

**Ringkasan**

- Data pada jaringan tidak bersifat rahasia dan oleh karena itu harus dijaga keamanannya dari orang-orang yang tidak diinginkan yang duduk di belakang mesin yang terhubung pada jaringan.
- Niat jahat mungkin termasuk menjatuhkan server yang melekat pada jaringan, menggunakan informasi pribadi orang seperti nomor kartu kredit untuk kegiatan penipuan dan menyabot organisasi utama dengan mengakses situs web mereka. Oleh karena itu bertujuan untuk mengamankan data dan mencegah dari menguping dari mendengarkan dan mencuri data. Data pengguna di komputer juga dilindungi dengan memberikan akses terbatas kata sandi ke data dan sumber daya sehingga hanya orang yang berwenang untuk menggunakannya. Aspek keamanan juga melibatkan mengidentifikasi penjahat dan menggagalkan upaya mereka untuk menyebabkan kerusakan pada jaringan di antara sumber daya lainnya.
- Otentikasi melibatkan memverifikasi anteseden orang yang telah meminta layanan dari mesin jarak jauh atau akses ke mesin jarak jauh baik melalui fisik maupun dengan mengirim email sebelum mengizinkannya melakukannya. Otentikasi melibatkan proses untuk mengautentikasi identitas seseorang ke mesin jarak jauh.
- Integritas melibatkan kebenaran pesan yang diterima oleh mesin jarak jauh. Dengan kata lain, pesan tersebut memang sama tanpa perubahan apa pun yang dikirimkan oleh mesin sumber. Dalam hal ini, metode kode redundansi siklik tidak akan cukup karena penyusup dalam sistem atau saluran komunikasi mungkin dengan sengaja mengubah pesan. Keamanan harus memastikan bahwa tidak seorang pun di sepanjang rute dapat mengubah pesan.
- Kerahasiaan: Memastikan bahwa tidak ada orang yang dapat membaca pesan di perjalanan. Hal ini memerlukan penerapan teknik enkripsi.

- Pesan dienkripsi di ujung pengirim dan didekripsi di ujung penerima untuk mempertahankan privasi dengan bantuan teknik enkripsi dan dekripsi. Kunci rahasia dan teknik kunci publik adalah teknik yang tersedia dengan kelebihan dan kekurangannya.
- Substitusi dan transposisi cipher adalah dua kategori sandi yang digunakan dalam kriptografi klasik. Substitusi dan transposisi berbeda dalam bagaimana potongan pesan ditangani oleh proses enkripsi.

**Latihan Soal**

Isilah bagian yang kosong:

1. Dalam enkripsi kunci rahasia, kunci rahasia digunakan untuk ..... .
2. Dalam enkripsi kunci publik, kunci publik digunakan untuk .....pemijatan.
3. Enkripsi dan dekripsi biasanya menangani ..... suatu jaringan.
4. Dalam enkripsi kunci publik, kunci privat digunakan untuk... mengirim pesan ke teks biasa.
5. .....melibatkan intersepsi paket data oleh komputer yang berhasil berpura-pura menjadi server/sumber daya tepercaya.

Nyatakan apakah pernyataan berikut ini benar atau salah:

1. Cryptanalysis modern membuat substitusi sederhana dan transposisi cipher usang.
2. Menurut jarak unicity dari bahasa Inggris, 20 huruf ciphertext diperlukan untuk memecahkan substitusi sederhana alfabet campuran.
3. Dalam Cipher Substitusi, fungsi BETTIF digunakan pada posisi karakter untuk mengenkripsi dan fungsi terbalik untuk mendekripsi.
4. Secara tradisional, ciphertext ditulis dalam blok panjang tetap, menghilangkan tanda baca dan ruang.
5. ROT13 adalah cipher caesar, jenis cipher transposisi.

Uraian

1. Apa saja kriteria untuk menjaga kerahasiaan informasi ketika dikirim melalui jaringan publik?
2. Bagaimana enkripsi mempengaruhi kinerja jaringan?
3. Ada basis informasi tertentu di Internet yang perlu dicegah oleh orang yang tidak diinginkan. Bagaimana orang yang tidak diinginkan dapat dicegah mengaksesnya?
4. Bagaimana cara kita menjaga komputer kita dan komputer orang lain tetap aman dari peretas? Jelaskan dengan bantuan situasi hipotetis.
5. Apa itu Sandi? Mengapa cipher digunakan untuk pesan berukuran besar?
6. Jelaskan secara singkat dua jenis serangan keamanan, yang dapat ditujukan terhadap sistem komputer yang terhubung ke Internet.
7. Apa perbedaan antara kunci rahasia dan enkripsi kunci publik?
8. Apa itu kriptografi? Apa keuntungan menggunakan teknik ini?
9. Apa yang dimaksud dengan sandi substitusi dan transposisi? Bedakan antara keduanya.

# DAFTAR PUSTAKA


Akyildiz, I. F., Wang, X., 2010, "Wireless Mesh Networks", New York, Wiley-IEEE Press.

Al-Sakib Khan Pathan, M., Mat Kiah, M. L., 2010, "Network Security: Challenges and Solutions", Boca Raton, CRC Press.

Andrews, J. G., 2004, "Computer Networks: A Systems Approach", Boston, Morgan Kaufmann Publishers.

Barrett, D., Silverman, R., Byrnes, R., 2005, "SSH, The Secure Shell: The Definitive Guide", Beijing, O'Reilly Media.

Bejtlich, R., 2005, "The Tao of Network Security Monitoring: Beyond Intrusion Detection", Boston, Addison-Wesley Professional.

Brown, J., 2018, "Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework", Indianapolis, Wiley.

Burns, R., 2007, "Network Security", New York, McGraw-Hill.

Carlin, D., 2005, "Internet Security: A Jumpstart for Systems Administrators and IT Managers", San Francisco, Syngress.

Cisco Systems, Inc., 2013, "Interconnecting Cisco Network Devices, Part 1 (ICND1): CCNA Exam 640-802 and ICND1 Exam 640-822", Indianapolis, Cisco Press.

Cisco Systems, Inc., 2015, "CCNA Routing and Switching Portable Command Guide", Indianapolis, Cisco Press.

Collier, J., 2011, "Introduction to Networking with Network+", Boston, Cengage Learning.

Comer, D. E., 2016, "Computer Networks and Internets", Boston, Pearson.

Dixit, S., 2015, "SDN and NFV Simplified: A Visual Guide to Understanding Software Defined Networks and Network Function Virtualization", Indianapolis, Cisco Press.

Douligeris, C., Serpanos, D. N., 2008, "Network Security: Current Status and Future Directions", Hoboken, Wiley-Interscience.

Doyle, J., Carroll, J., 2005, "Routing TCP/IP, Volume 1", Indianapolis, Cisco Press.

Durica, M., 2011, "Computer Networking: Principles, Protocols and Practice", New York, Saylor Foundation.

Farrel, A., 2009, "GMPLS: Architecture and Applications", Amsterdam, Elsevier.

Forouzan, B. A., 2016, "Data Communications and Networking", New York, McGraw-Hill Education.

Goralski, W., 2005, "LDAP Directories Explained: An Introduction and Analysis", Boston, Addison-Wesley Professional.

Gralla, P., 2002, "How the Internet Works", Indianapolis, Que.

Guowang, M., Xylomenos, G., 2016, "Mobile Networks Architecture", Cambridge, Cambridge University Press.

Hallberg, B., 2009, "Fiber Optics Technician's Manual", Burlington, Newnes.

Harris, C., 2011, "CISSP All-in-One Exam Guide", New York, McGraw-Hill.

Hunt, C., 2013, "TCP/IP Network Administration", Beijing, O'Reilly Media.

Kaeo, M., 2000, "Internet Protocol Version 6 (IPv6) for the IPv4 Administrator", Indianapolis, Cisco Press.

Keshav, S., 2010, "An Engineering Approach to Computer Networking", New York, Addison-Wesley.

Kim, W. S., 2008, "Network Security Technologies and Solutions", Indianapolis, Cisco Press.

Kurose, J. F., Ross, K. W., 2017, "Computer Networking: A Top-Down Approach", Boston, Pearson.

Lammle, T., 2018, "CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125", Indianapolis, Sybex.

Medina, A., 2007, "BGP Design and Implementation", Indianapolis, Cisco Press.

Mock, D., Schmidt, T., 2007, "Pro DNS and BIND", Berkeley, Apress.

Moy, J., 1995, "OSPF: Anatomy of an Internet Routing Protocol", Boston, Addison-Wesley Professional.

Moy, J., 1998, "OSPF: Anatomy of an Internet Routing Protocol", Boston, Addison-Wesley Professional.

Odom, W., 2009, "CCENT/CCNA ICND1 Official Exam Certification Guide", Indianapolis, Cisco Press.

Odunaike, O. A., 2017, "Introduction to Computer Networking and Cybersecurity", Boca Raton, CRC Press.

Pahlavan, K., Krishnamurthy, P., 2002, "Principles of Wireless Networks: A Unified Approach", Upper Saddle River, Prentice Hall.

Perlman, R., 2000, "Interconnections: Bridges, Routers, Switches, and Internetworking Protocols", Boston, Addison-Wesley Professional.

Peterson, L. L., Davie, B. S., 2011, "Computer Networks: A Systems Approach", Amsterdam, Morgan Kaufmann.

Ramaswamy, S., 2010, "Fundamentals of Wireless Communication Engineering Technologies", Hoboken, Wiley.

Ross, K. W., Kurose, J. F., 2009, "Computer Networking: A Top-Down Approach Featuring the Internet", Boston, Pearson.

Russell, D., 2003, "Network Security Essentials: Applications and Standards", Boston, Pearson.

Schwartz, M., 2010, "Broadbandits: Inside the $750 Billion Telecom Heist", New York, Atria Books.

Sidhu, A., 2017, "Software Defined Networking", Cham, Springer International Publishing.

Simon, D., 2013, "Data Warehousing For Dummies", Hoboken, Wiley.

Stallings, W., 2013, "Data and Computer Communications", Upper Saddle River, Pearson Education.

Stamatelatos, M., 2002, "Network Design and Case Studies", Upper Saddle River, Prentice Hall.

Tanenbaum, A. S., 2011, "Computer Networks", Upper Saddle River, Pearson Education.

Tanenbaum, A. S., van Steen, M., 2007, "Distributed Systems: Principles and Paradigms", Upper Saddle River, Prentice Hall.

Tanenbaum, A. S., Wetherall, D. J., 2011, "Computer Networks", Upper Saddle River, Pearson Education.

Yang, D., 2016, "Internet of Things", Boca Raton, CRC Press.

# Teknologi Jaringan Komputer

Dr. Agus Wibowo, M.Kom, M.Si, MM.

## BIO DATA PENULIS

Penulis memiliki berbagai disiplin ilmu yang diperoleh dari Universitas Diponegoro (UNDIP) Semarang. dan dari Universitas Kristen Satya Wacana (UKSW) Salatiga. Disiplin ilmu itu antara lain teknik elektro, komputer, manajemen dan ilmu sosiologi. Penulis memiliki pengalaman kerja pada industri elektronik dan sertifikasi keahlian dalam bidang Jaringan Internet, Telekomunikasi, Artificial Intelligence, Internet Of Things (IoT), Augmented Reality (AR), Technopreneurship, Internet Marketing dan bidang pengolahan dan analisa data (komputer statistik).

Penulis adalah pendiri dari Universitas Sains dan Teknologi Komputer (Universitas STEKOM ) dan juga seorang dosen yang memiliki Jabatan Fungsional Akademik Lektor Kepala (Associate Professor) yang telah menghasilkan puluhan Buku Ajar ber ISBN, HAKI dari beberapa karya cipta dan Hak Paten pada produk IPTEK. Sejak tahun 2023 penulis tercatat sebagai Dosen luar biasa di Fakultas Ekonomi & Bisnis (FEB) Universitas Diponegoro Semarang. Penulis juga terlibat dalam berbagai organisasi profesi dan industri yang terkait dengan dunia usaha dan industri, khususnya dalam pengembangan sumber daya manusia yang unggul untuk memenuhi kebutuhan dunia kerja secara nyata.

YAYASAN PRIMA AGUS TEKNIK

**PENERBIT :**
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Dr. Agus Wibowo, M.Kom, M.Si, MM.

# Teknologi Jaringan Komputer

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8642-14-4 (PDF)
9 786238 642144