



YAYASAN PRIMA AGUS TEKNIK

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

KOMUNIKASI DATA BISNIS dan JARINGAN KOMPUTER



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

KOMUNIKASI DATA BISNIS dan 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 978-623-8642-11-3 (PDF)



9 786238 642113

KOMUNIKASI DATA BISNIS DAN JARINGAN KOMPUTER

Penulis :

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

ISBN : 978-623-8642-11-3

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 Yuniarto, 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. 08122925000

Fax. 024-6710144

Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :

Universitas STEKOM

Jl. Majapahit no 605 Semarang

Telp. 08122925000

Fax. 024-6710144

Email : info@stekom.ac.id

Hak cipta dilindungi undang-undang

Dilarang memperbanyak karya tulis ini dalam bentuk dan dengan cara
apapun tanpa ijin dari penulis

KATA PENGANTAR

Puji Syukur kehadiran Tuhan Yang Maha Esa, atas berkat dan Rahmat-Nya, sehingga penulis dapat menyelesaikan buku yang berjudul "***Komunikasi Data Bisnis Dan Jaringan Komputer***", dengan lancar. Buku ini ditulis untuk menambah wawasan mengenai proses pengiriman dan penerimaan data atau informasi antara dua atau lebih perangkat yang terhubung dalam sebuah jaringan.

Komunikasi data adalah proses pengiriman dan penerimaan data atau informasi melalui dua atau lebih perangkat, seperti komputer, laptop, smartphone, dan lain-lain yang terhubung dalam sebuah jaringan. Proses ini melibatkan pergerakan data elektronik berdasarkan lokasi geografis, media teknologi, dan konten. Komunikasi data menggunakan berbagai teknik dan teknologi untuk mengaktifkan segala bentuk komunikasi elektronik, termasuk telekomunikasi, jaringan komputer, dan radio atau satelit. Dalam proses ini, data dikirim melalui media transportasi antar node, seperti kabel tembaga, fiber optic, atau nirkabel, dan dapat berupa data audio, video, atau audio video. Komunikasi data memiliki lima komponen dasar, yaitu sumber data, media penghantar, sink/penerima, pengirim, dan peralatan switching. Dengan menggunakan sistem ini, pengguna dapat mengirimkan data berjumlah besar secara efisien, mendukung manajemen dan pengelolaan data, serta memudahkan penyebaran informasi.

Bab 1 ini secara singkat membahas dasar-dasar jaringan komputer dan komunikasi data, termasuk terminologi dasar, komponen utama jaringan, tata letak jaringan, konvergensi layanan, arsitektur jaringan, serta model protokol TCP/IP dan OSI. Bab ini juga membandingkan kedua model tersebut, menyoroti perbedaan dan persamaannya dalam pengelolaan komunikasi data di jaringan komputer. Bab 2 ini membahas konsep dasar tentang data dan sinyal dalam jaringan komunikasi. Anda akan mempelajari perbedaan antara data digital dan analog serta sinyal digital dan analog, dengan fokus pada keunggulan data digital dalam keandalan dan efisiensi bandwidth. Bab ini juga mengidentifikasi komponen dasar sinyal seperti amplitudo, frekuensi, dan fase, serta pentingnya bandwidth dalam kecepatan transfer data. Selain itu, pembahasan mencakup kekuatan dan redaman sinyal yang mempengaruhi kualitas transmisi data jarak jauh. Anda juga akan memahami ciri-ciri berbagai jenis transmisi data analog dan digital dengan sinyal yang sesuai, serta teknik dasar pengkodean digital dan modulasi yang digunakan dalam komunikasi digital. Selanjutnya dalam Bab 3 ini mengajarkan tentang berbagai media transmisi dalam jaringan komunikasi. Anda akan mempelajari kabel twisted pair dari berbagai kategori serta perbedaannya dengan kabel berpelindung dan tidak berpelindung. Selain itu, dibahas juga kelebihan dan kelemahan kabel koaksial dan kabel serat optik sebagai alternatif. Bab ini juga menjelaskan sistem gelombang mikro terestrial dan satelit, serta perbedaan antara jenis-jenis satelit. Anda akan memahami dasar-dasar telepon seluler dan evolusi sistem seluler generasi saat ini.

Tujuan dari bab 4 ini adalah untuk memberikan pemahaman yang mendalam tentang berbagai standar antarmuka dalam konteks teknologi komunikasi data. Pembaca akan mampu mengidentifikasi komponen-komponen yang umum terdapat dalam semua standar antarmuka, memahami operasi dasar dari standar antarmuka USB, dan membedakan antara koneksi half-duplex yang mengizinkan transmisi data dalam satu arah pada satu waktu, dengan

full-duplex yang memungkinkan transmisi data dua arah secara bersamaan. Selain itu, pembaca akan dapat mengenali keunggulan dari beberapa standar antarmuka seperti FireWire, Thunderbolt, SCSI, iSCSI, InfiniBand, dan Fibre Channel dalam konteks aplikasi dan kecepatan transfer data. Bab ini juga menguraikan karakteristik antarmuka data link asynchronous, synchronous, dan isochronous, yang mempengaruhi sinkronisasi dan waktu transmisi data. Terakhir, pembaca akan mengidentifikasi ciri khas dari koneksi terminal-ke-mainframe, yang unik karena penggunaan dalam komunikasi besar-besaran dan pengolahan data di pusat data atau sistem terpusat. Dalam bab 5 ini akan memberikan pemahaman mendalam tentang berbagai teknik multiplexing dan kompresi dalam konteks sistem komunikasi dan transfer data. Pembaca akan dapat menjelaskan dan memahami aplikasi, kelebihan, serta kekurangan dari multiplexing pembagian frekuensi dan waktu sinkron, serta karakteristik dasar dari sistem multiplexing seperti T-1, SONET/SDH, statistik pembagian waktu, dan pembagian panjang gelombang. Selain itu, pembaca akan mampu mengidentifikasi karakteristik dari teknik multiplexing lainnya seperti multinada diskrit dan pembagian kode, serta menerapkan teknik-teknik ini dalam situasi bisnis umum.

Bab 6 ini adalah untuk memberikan pemahaman yang mendalam tentang kebisingan dalam jaringan komputer dan teknik pencegahan serta deteksi kesalahan yang diterapkan untuk memastikan integritas data yang tinggi. Pembaca akan mengidentifikasi berbagai jenis kebisingan yang umum terjadi di jaringan komputer dan mempelajari teknik-teknik pencegahan kesalahan seperti redundansi data, paritas sederhana, paritas longitudinal, checksum redundansi siklik, dan checksum aritmatika. Selanjutnya bab 7 memberikan pemahaman yang mendalam tentang jaringan area lokal (LAN) dalam konteks teknologi komunikasi data. Pembaca akan mampu mendefinisikan LAN sebagai jaringan komputer yang mencakup area terbatas seperti kantor, sekolah, atau gedung yang sama. Mereka juga akan mempelajari fungsi utama, aktivitas sehari-hari, dan berbagai area penerapan LAN, termasuk kelebihan dan kekurangannya dalam mendukung komunikasi dan kolaborasi di lingkungan yang terbatas. Dan bab ke 8 memberikan pemahaman yang mendalam tentang infrastruktur dan komponen-komponen yang mendukung jaringan area lokal (LAN). Pembaca diharapkan dapat mengidentifikasi komponen dasar jaringan area lokal nirkabel, termasuk perangkat keras seperti access point dan kartu jaringan nirkabel. Mereka juga akan memahami fungsi utama sistem operasi jaringan yang menjadi basis operasional untuk jaringan LAN, serta fitur dasar dari sistem operasi jaringan seperti Novell NetWare/OES, Windows Server, UNIX, Linux, dan Mac OS X Server.

Bab ke 9 akan membahas pemahaman yang mendalam tentang berbagai jenis jaringan dan konsep fundamental dalam infrastruktur jaringan komunikasi data. Pembaca diharapkan dapat membedakan jaringan area lokal (LAN), jaringan area metropolitan (MAN), dan jaringan area luas (WAN), serta mengidentifikasi karakteristik khusus dari jaringan area metropolitan dan membandingkannya dengan jaringan area luas dan lokal. Selain itu, bab ini menjelaskan berbagai mode operasi jaringan seperti Circuit-Switched, Datagram Packet-Switched, dan Virtual Circuit Packet-Switched, serta bagaimana teknik-teknik ini membentuk struktur jaringan cloud modern. Pembaca juga diajarkan perbedaan antara jaringan berorientasi koneksi (connection-oriented) dan jaringan tanpa koneksi (connectionless), disertai contoh implementasinya. Selanjutnya bab ke 10 akan membahas tentang protokol dan teknologi inti yang membentuk dasar internet dan jaringan komunikasi data saat ini. Pembaca diharapkan

dapat memahami tanggung jawab Internet Protocol (IP) dalam mengelola alamat dan routing data antar jaringan, serta kemampuan untuk mengidentifikasi dan membedakan antara alamat IPv4 dan IPv6 yang digunakan dalam pengalamatan jaringan modern. Selain itu, bab ini membahas peran Protokol Kontrol Transmisi (TCP) dalam memastikan koneksi end-to-end yang andal dan stabil di internet. Pembaca juga diajarkan mengenai hubungan antara TCP/IP dengan protokol lain seperti ICMP, UDP, ARP, DHCP, NAT, dan protokol terowongan, serta bagaimana setiap protokol ini berkontribusi dalam fungsi operasional jaringan.

Dalam bab ke 11 membahas tentang sistem telepon, evolusi industri telekomunikasi, dan teknologi jaringan terkini. Pembaca akan mengidentifikasi elemen dasar sistem telepon, perbedaan sebelum dan sesudah regulasi telekomunikasi, serta karakteristik koneksi internet dan saluran sewaan. Bab ini juga mencakup teknologi moden seperti ATM, MPLS, dan VPN, serta menjelaskan konsep konvergensi dalam industri jaringan. Dengan ini, pembaca diharapkan dapat memahami perkembangan terbaru dalam telekomunikasi dan jaringan komunikasi data. Selanjutnya dalam bab ke 12 ini akan membahas tentang keamanan sistem komputer dan jaringan. Pembaca akan mengenal berbagai bentuk serangan sistem, konsep perlindungan fisik, teknik pengendalian akses, serta evaluasi kelebihan dan kelemahan penggunaan password. Bab ini juga membahas teknik untuk mengamankan data, seperti kriptografi, serta perbedaan antara metode sandi substitusi dan transposisi. Selain itu, pembaca akan mempelajari teknik keamanan komunikasi, termasuk teknik spektrum sebaran, pentingnya firewall, jenis perlindungan yang ditawarkan, dan keuntungan bisnis dari menerapkan kebijakan keamanan yang efektif. Dengan ini, pembaca diharapkan dapat mengimplementasikan strategi keamanan yang sesuai untuk melindungi sistem dan data mereka. Dalam bab 13 yang merupakan bab terakhir buku ini akan membahas mengenai manajemen sistem dan operasi jaringan. Pembaca akan mengidentifikasi Siklus Hidup Pengembangan Sistem, yang meliputi fase-fase kunci dari perencanaan hingga penghentian sistem. Pentingnya membuat peta konektivitas juga ditekankan untuk memvisualisasikan struktur jaringan secara keseluruhan. Perbedaan antara kelayakan teknis, finansial, operasional, dan waktu dijelaskan untuk membantu dalam evaluasi proyek IT. Analisis biaya-manfaat yang mencakup nilai waktu dari uang membantu dalam pengambilan keputusan yang lebih baik. Sulitnya melakukan perencanaan kapasitas dan analisis lalu lintas dijelaskan karena melibatkan prediksi yang kompleks terhadap kebutuhan jaringan di masa depan

Dengan demikian buku ini dibuat supaya dapat bermanfaat bagi para pembaca, dengan tujuan untuk memahami prinsip-prinsip dasarnya, kita dapat membangun jaringan yang lebih efektif dan efisien. Terima Kasih.

Semarang, Juni 2024

Penulis

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

DAFTAR ISI

Halaman Judul	i
Kata Pengantar	ii
Daftar Isi	v
BAB 1 PENGANTAR JARINGAN KOMPUTER DAN KOMUNIKASI DATA	1
1.1. Pendahuluan	2
1.2. Bahasa Jaringan Computer	4
1.3. Gambaran Besar Jaringan	5
1.4. Tata Letak Dasar Jaringan Komunikasi	7
1.5. Konvergensi	15
1.6. Arsitektur Jaringan	16
1.7. Tata Letak Jaringan Beraksi	27
1.8. Suite Protocol TCP/IP Beraksi	28
BAB 2 DASAR-DASAR DATA DAN SINYAL	35
2.1. Pendahuluan	36
2.2. Data Dan Sinyal	38
2.3. Mengubah Data Menjadi Sinyal	47
2.4. Kode Data	63
BAB 3 MEDIA KONDUKTOR DAN NIRKABEL	77
3.1. Pendahuluan	78
3.2. Media Yang Dilakukan	78
3.3. Media Nirkabel	91
3.4. Kriteria Pemilihan Media	112
3.5. Dua Contoh Aksi Media Yang Dilakukan	116
3.6. Contoh Media Nirkabel	119
BAB 4 MEMBUAT KONEKSI	126
4.1. Pendahuluan	126
4.2. Interfacing Komputer Ke Perangkat Peripheral	128
4.3. Koneksi Tautan Data	134
4.4. Koneksi Komputer Terminal Ke Mainframe	139
4.5. Melakukan Koneksi Komputer	141
BAB 5 MEMBUAT KONEKSI EFISIEN MULTIPLEXING DAN KOMPRESI	146
5.1. Pendahuluan	147
5.2. Multiplexing Divisi Frekuensi	147
5.3. Multiplexing Divisi Waktu	150
5.4. Multiplexing Divisi Panjang Gelombang	158
5.5. Multiton Diskrit	160
5.6. Multiplexing Divisi Kode	161
5.7. Perbandingan Teknik Multiplexing	163
5.8. Kompresi	165
5.9. Multiplexing Bisnis	174

BAB 6	KESALAHAN, DETEKSI KESALAHAN, DAN PENGENDALIAN KESALAHAN	181
6.1.	Pendahuluan	182
6.2.	Kebisingan Dan Kesalahan	183
6.3.	Pencegahan Kesalahan	187
6.4.	Deteksi Kesalahan	189
6.5.	Control Kesalahan	196
6.6.	Deteksi Kesalahan Dalam Praktiknya	207
BAB 7	JARINGAN AREA LOKAL – BAGIAN 1	213
7.1.	Pendahuluan	214
7.2.	Fungsi Utama Jaringan Area Lokal	215
7.3.	Keunggulan Dan Kekurangan Jaringan Area Lokal	217
7.4.	Jaringan Area Lokal Pertama: BUS/TREE	219
7.5.	LAN Yang Lebih Modern	222
7.6.	Switch	227
7.7.	Ethernet Kabel	237
7.8.	Format Bingkai Ethernet Kabel	240
BAB 8	JARINGAN AREA LOKAL – BAGIAN II	251
8.1.	Pendahuluan	252
8.2.	Ethernet Nirkabel	253
8.3.	CSMA/CA Nirkabel.....	257
8.4.	Sistem Operasi Jaringan	260
8.5.	Sistem Operasi Jaringan Masa Lalu Dan Sekarang	262
8.6.	Server	272
8.7.	Perangkat Lunak Dukungan Jaringan	276
8.8.	Perjanjian Lisensi Perangkat Lunak	280
8.9.	Perangkat Dukungan LAN	282
8.10.	Penggunaan LAN Dalam Perusahaan	284
8.11.	Jaringan Nirkabel Untuk Rumah	287
BAB 9	PENGANTAR JARINGAN AREA METROPOLITAN DAN JARINGAN AREA LUAS	294
9.1.	Pendahuluan	295
9.2.	Dasar-Dasar Jaringan Wilayah Metropolitan	296
9.3.	Dasar-Dasar Jaringan Area Luas (WAN)	300
9.4.	Rute	309
9.5.	Kecepatan Jaringan	318
9.6.	Smart Phone Berbasis WAN	321
BAB 10	INTERNET	328
10.1.	Pendahuluan	329
10.2.	Protokol Internet	330
10.3.	World Wide Web (www)	349
10.4.	Layanan Internet	353
10.5.	Internet Dan Bisnis	362
10.6.	Mada Depan Internet	364
10.7.	Perusahaan Menciptakan VPN	366

BAB 11	JARINGAN PENGIRIMAN SUARA DAN DATA	373
11.1.	Pendahuluan	374
11.2.	Sistem Telepon Dasar	374
11.3.	Saluran Pelanggan Digital	382
11.4.	Modem Kabel	386
11.5.	T-1 Layanan Leased LINE	388
11.6.	Frame Relay	389
11.7.	Mode Transfer Asynchronous	393
11.8.	MPLS Dan VPN	397
11.9.	Konvergensi	399
11.10.	Sistem Telekomunikasi Perusahaan	403
BAB 12	KEAMANAN JARINGAN	414
12.1.	Pendahuluan	415
12.2.	Serangan Sistem Standar	416
12.3.	Perlindungan Fisik	420
12.4.	Mwngontrol Akses	421
12.5.	Mengamankan Data	427
12.6.	Mengambil Komunikasi	440
12.7.	Masalah Kebijakan Keamanan	448
12.8.	Membuat Keamanan LAN Nirkabel	450
BAB 13	DESAIN DAN MANAJEMEN JARINGAN	457
13.1.	Pendahuluan	458
13.2.	Siklus Hidup Perkembangan Sistem	459
13.3.	Pemodelan Jaringan	461
13.4.	Studi Kelayakan	465
13.5.	Perencanaan Kapasitas	470
13.6.	Menciptakan Garis Dasar	474
13.7.	Keterampilan Administrator Jaringan	477
13.8.	Menghasilkan Statistic Yang Dapat Digunakan	478
13.9.	Alat Diagnostik Jaringan	481
13.10.	Perencanaan Kapasitas Dan Desain Jaringan	485
	Daftar Pustaka	486
	Lampiran Daftar Tarif Internet	489

BAB 1

PENGANTAR JARINGAN KOMPUTER DAN KOMUNIKASI DATA

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Menjelaskan terminologi dasar jaringan komputer
- Kenali masing-masing komponen gambaran besar jaringan komputer
- Kenali tata letak jaringan dasar
- Definisikan istilah "konvergensi" dan jelaskan penerapannya pada jaringan komputer
- Sebutkan alasan penggunaan arsitektur jaringan dan jelaskan bagaimana penerapannya pada sistem jaringan saat ini
- Buat daftar lapisan rangkaian protokol TCP/IP dan jelaskan tugas setiap lapisan
- Buat daftar lapisan model OSI dan jelaskan tugas masing-masing lapisan
- Bandingkan rangkaian protokol TCP/IP dan model OSI, serta buat daftar perbedaan dan persamaannya

MEMBUAT PREDIKSI adalah tugas yang sulit, tidak terkecuali memprediksi masa depan komputasi. Sejarah penuh dengan prediksi terkait komputer yang sangat tidak akurat sehingga saat ini prediksi tersebut lucu. Misalnya saja prediksi berikut:

"Saya pikir ada pasar dunia untuk mungkin lima komputer." Thomas Watson, ketua IBM, 1943

"Saya telah melakukan perjalanan jauh dan luas di negara ini, dan berbicara dengan orang-orang terbaik, dan saya dapat meyakinkan Anda bahwa pemrosesan data adalah sebuah tren yang tidak akan bertahan lama." Editor yang bertanggung jawab atas buku bisnis untuk Prentice Hall, 1957

"Tidak ada alasan siapa pun menginginkan komputer di rumah mereka." Ken Olsen, presiden dan pendiri Digital Equipment Corporation, 1977

"640K seharusnya cukup untuk siapa pun." Bill Gates, 1981

"Kami yakin kedatangan adik PC [PCjr] merupakan perkembangan yang signifikan dan bertahan lama dalam sejarah komputasi seperti yang telah dibuktikan oleh upaya awal IBM dalam komputasi mikro." PC Magazine, Desember 1983 (PCjr berlangsung kurang dari satu tahun.)

Rupanya, tidak peduli seberapa terkenalnya Anda atau seberapa berpengaruhnya posisi Anda, sangatlah mudah untuk membuat prediksi yang sangat buruk. Meskipun demikian, sulit untuk membayangkan bahwa seseorang dapat membuat prediksi yang lebih buruk daripada prediksi di atas. Didukung oleh rasa optimisme yang salah ini, mari kita membuat beberapa perkiraan kita sendiri:

Suatu hari sebelum Anda keluar rumah, Anda akan meraih payung Anda, dan payung akan memberi tahu Anda cuaca seperti apa yang akan terjadi di luar. Sinyal radio akan menghubungkan payung ke layanan cuaca lokal yang akan mengunduh kondisi cuaca terkini untuk kenyamanan Anda.

Suatu hari nanti kamu akan mengendarai mobil, dan jika kamu melaju lebih cepat dari kecepatan yang telah ditentukan, mobil tersebut akan mengirimkan pesan teks kepada orang tuamu untuk memberitahukan mereka tentang “*kebiasaan mengemudi*” kamu.

Suatu hari nanti kita akan memakai komputer—seperti pakaian—dan saat kita berjabat tangan dengan seseorang, data akan ditransfer ke kulit kita, melalui tangan yang berjabat, dan ke “*komputer*” orang lain.

Suatu saat dalam waktu yang tidak lama lagi, Anda akan menyajikan beberapa hot dog dan hamburger di atasnya panggangan dan kemudian masuk ke dalam untuk menonton pertandingan bola. Tiba-tiba, Anda akan mendapat pesan di ponsel Anda: “*Makanan Anda sudah selesai dimasak.*”

Suatu hari nanti Anda akan memiliki aki mobil yang, ketika daya aki menjadi terlalu lemah untuk menghidupkan mobil, akan menghubungi Anda melalui ponsel untuk memberi tahu Anda bahwa Anda memerlukan penggantian atau pengisian daya.

Suatu hari Anda akan berada di kota besar dan menelepon ponsel Anda untuk meminta taksi. Suara di seberang sana hanya akan berkata, “*Tetaplah di tempatmu sekarang. Apakah Anda melihat taksi lewat di jalan? Saat berhenti di depan Anda, masuklah.*”

Suatu hari nanti Anda akan mengemudi di kota besar dan ponsel atau perangkat Global Positioning System (GPS) Anda akan memberi tahu Anda di mana tempat parkir kosong terdekat di jalan tersebut.

Apakah prediksi ini terdengar tidak masuk akal dan penuh dengan teknologi misterius yang hanya dapat dipahami oleh para ilmuwan dan insinyur? Seharusnya tidak demikian, karena itu bukan prediksi. Itu adalah skenario yang terjadi saat ini dengan teknologi yang sudah ada. Terlebih lagi, semua kemajuan tersebut tidak akan mungkin terjadi saat ini jika tidak ada jaringan komputer dan komunikasi data.

1.1 PENDAHULUAN

Dunia jaringan komputer dan komunikasi data merupakan bidang studi yang sangat luas dan semakin signifikan. Dulunya dianggap sebagai domain para insinyur dan teknisi

jaringan, jaringan komputer kini melibatkan manajer bisnis, pemrogram komputer, perancang sistem, manajer kantor, pengguna komputer rumahan, dan masyarakat sehari-hari. Hampir tidak mungkin bagi rata-rata orang di jalan untuk menghabiskan 24 jam tanpa menggunakan jaringan komputer secara langsung atau tidak langsung.

Tanyakan kepada kelompok mana pun, *“Apakah ada yang menggunakan jaringan komputer saat ini?”*, dan lebih dari separuh orang mungkin menjawab, *“Ya.”* Kemudian tanyakan kepada yang lain, *“Bagaimana Anda bisa bekerja, sekolah, atau toko hari ini jika Anda tidak menggunakan jaringan komputer?”* Sebagian besar sistem transportasi menggunakan jaringan komunikasi yang luas untuk memantau arus kendaraan dan kereta api. Jalan tol dan jalan raya memiliki sistem terkomputerisasi untuk mengendalikan sinyal lalu lintas dan membatasi akses selama jam sibuk lalu lintas. Beberapa kota besar memasang perangkat keras yang sesuai di dalam bus kota dan kereta api sehingga lokasi persis setiap bus dan kereta api dapat diketahui. Informasi ini memungkinkan sistem transportasi menjaga jarak antar bus tetap merata dan lebih tepat waktu, serta memungkinkan penumpang mengetahui kapan bus atau kereta berikutnya akan tiba.

Selain itu, semakin banyak orang yang menggunakan perangkat GPS berbasis satelit di mobil mereka untuk memberikan petunjuk arah mengemudi dan menghindari titik rawan lalu lintas. Sistem serupa dapat membuka kunci pintu mobil Anda jika Anda meninggalkan kunci di kunci kontak dan dapat menemukan lokasi mobil Anda di tempat parkir yang ramai—membunyikan klakson dan menyalakan lampu depan jika Anda tidak dapat mengingat di mana Anda parkir.

Namun meskipun saat ini Anda tidak menggunakan angkutan massal atau perangkat GPS di mobil, ada banyak cara lain untuk menggunakan jaringan komputer. Bisnis dapat memesan suku cadang dan inventaris sesuai permintaan dan membuat produk sesuai spesifikasi yang dirancang pelanggan.

Kation secara elektronik, tanpa memerlukan kertas. Gerai ritel online dapat melacak setiap barang yang Anda lihat atau beli. Dengan menggunakan data ini, mereka dapat membuat rekomendasi produk serupa dan memberi tahu Anda di masa mendatang ketika produk baru tersedia. Mesin perbankan 24 jam dapat memverifikasi identitas pengguna dengan mengambil sidik jari pengguna.

Selain itu, televisi kabel terus berkembang, menawarkan program yang luas, pilihan bayar-per-tayang, perekaman video, televisi digital dan musik, dan konektivitas multi-megabit ke Internet. Sistem telepon, jaringan perangkat komunikasi tertua dan terluas, terus menjadi jaringan komputer setiap hari. Jaringan *“telepon”* terkini kini dapat menyalurkan suara, Internet, dan televisi melalui satu sambungan. Sistem telepon seluler mencakup hampir seluruh benua Amerika Utara dan memungkinkan pengguna mengunggah dan mengunduh data ke dan dari Internet, mengirim dan menerima gambar, dan mengunduh video streaming seperti program televisi. Perangkat genggam yang Anda pegang dapat memutar musik, melakukan panggilan telepon, mengambil gambar, menjelajahi Web, dan memungkinkan Anda bermain game sambil menunggu kereta berikutnya.

Selamat datang di dunia jaringan komputer yang menakjubkan! Kecuali Anda telah menghabiskan 24 jam terakhir dalam isolasi total, hampir tidak mungkin untuk tidak menggunakan suatu bentuk jaringan komputer dan komunikasi data. Karena semakin berkembangnya integrasi jaringan komputer dan komunikasi data ke dalam bisnis dan kehidupan, kita tidak dapat menyerahkan bidang studi ini kepada teknisi. Kita semua khususnya mahasiswa sistem informasi, bisnis, dan ilmu komputer perlu memahami konsep dasar. Berbekal pengetahuan ini, kita tidak hanya akan lebih baik dalam berkomunikasi dengan spesialis dan insinyur jaringan, tetapi juga akan menjadi pelajar, manajer, dan karyawan yang lebih baik.

1.2 BAHASA JARINGAN KOMPUTER

Selama bertahun-tahun, banyak istilah dan definisi yang berkaitan dengan jaringan komputer dan komunikasi data telah muncul. Untuk memperoleh wawasan mengenai banyak subbidang studi, dan untuk menjadi akrab dengan penekanan buku teks ini, mari kita periksa istilah-istilah yang lebih umum dan definisinya.

Jaringan komputer adalah interkoneksi komputer dan peralatan komputasi menggunakan kabel atau gelombang radio dan dapat berbagi data dan sumber daya komputasi. Jaringan komputer yang menggunakan gelombang radio disebut nirkabel dan dapat melibatkan siaran radio, gelombang mikro, atau transmisi satelit. Jaringan yang mencakup area beberapa meter di sekitar individu disebut jaringan area pribadi (PAN). Jaringan area pribadi mencakup perangkat seperti komputer laptop, asisten digital pribadi, dan koneksi nirkabel. Jaringan yang ukuran geografisnya sedikit lebih besar mencakup ruangan, lantai dalam gedung, gedung, atau kampus adalah jaringan area lokal (LAN). Jaringan yang melayani wilayah hingga kira-kira 50 kilometer kira-kira seluas kota pada umumnya disebut jaringan wilayah metropolitan (MAN). Jaringan area metropolitan adalah jaringan berkecepatan tinggi yang menghubungkan bisnis dengan bisnis lain dan Internet. Jaringan besar yang mencakup sebagian negara bagian, banyak negara bagian, negara, dan dunia disebut jaringan area luas (WAN). Bab Tujuh dan Delapan berkonsentrasi pada jaringan area lokal, dan Bab Sembilan, Sepuluh, dan Sebelas berkonsentrasi pada jaringan area metropolitan dan jaringan area luas.

Studi tentang jaringan komputer biasanya dimulai dengan pengenalan dua blok bangunan penting: data dan sinyal. Data adalah informasi yang telah diterjemahkan ke dalam bentuk yang lebih kondusif untuk penyimpanan, transmisi, dan penghitungan. Seperti yang akan kita lihat di Bab Dua, sinyal digunakan untuk mengirimkan data. Kami mendefinisikan komunikasi data sebagai transfer data digital atau analog menggunakan sinyal digital atau analog. Setelah dibuat, sinyal analog dan digital ini kemudian ditransmisikan melalui media konduksi atau media nirkabel (keduanya dibahas pada Bab Tiga).

Menghubungkan perangkat ke komputer, atau komputer ke jaringan, memerlukan antarmuka, topik yang dibahas dalam Bab Empat. Karena mengirimkan hanya satu sinyal melalui suatu media pada satu waktu dapat menjadi cara yang tidak efisien dalam menggunakan media transmisi, banyak sistem melakukan multiplexing. Multiplexing adalah

transmisi beberapa sinyal pada satu media. Agar suatu media dapat mengirimkan banyak sinyal secara bersamaan, sinyal-sinyal tersebut harus diubah agar tidak saling mengganggu. Kompresi adalah teknik lain yang dapat memaksimalkan jumlah data yang dikirim melalui suatu media. Kompresi melibatkan pemerasan data ke dalam paket yang lebih kecil, sehingga mengurangi jumlah waktu (serta ruang penyimpanan) yang diperlukan untuk mengirimkan data. Multiplexing dan kompresi dibahas secara rinci di Bab Lima.

Ketika sinyal yang dikirimkan antar perangkat komputasi rusak dan terjadi kesalahan, deteksi kesalahan dan pengendalian kesalahan diperlukan. Topik-topik ini dibahas secara rinci di Bab Enam. Dahulu kala, jaringan suara mengirimkan sinyal telepon, dan jaringan data mengirimkan data komputer. Namun pada akhirnya, perbedaan antara jaringan suara dan jaringan data menghilang. Penggabungan jaringan suara dan data merupakan salah satu contoh konvergensi, sebuah topik penting yang akan dibahas nanti di bab ini dan dikembangkan lebih lanjut di bab berikutnya.

Keamanan komputer (dibahas dalam Bab Dua Belas) semakin menjadi perhatian baik bagi personel pendukung komputer profesional maupun pengguna komputer rumahan yang memiliki koneksi Internet. Manajemen jaringan adalah desain, instalasi, dan dukungan jaringan serta perangkat keras dan perangkat lunaknya. Bab Tiga Belas membahas banyak konsep dasar yang diperlukan untuk mendukung desain dan peningkatan perangkat keras dan perangkat lunak jaringan dengan baik, serta teknik manajemen yang lebih umum digunakan untuk mendukung jaringan.

1.3 GAMBARAN BESAR JARINGAN

Jika Anda dapat membuat satu gambar yang mencoba memberikan gambaran umum tentang jaringan komputer pada umumnya, apa saja yang termasuk dalam gambar ini? Gambar 1-1 menunjukkan gambaran seperti itu, dan mencakup contoh jaringan area lokal, pribadi, dan luas. Perhatikan bahwa gambar ini menunjukkan dua jenis jaringan area lokal (LAN 1 dan LAN 2). Meskipun penjelasan lengkap tentang berbagai komponen yang membentuk jaringan area lokal tidak diperlukan saat ini, penting untuk dicatat bahwa sebagian besar LAN mencakup perangkat keras berikut:

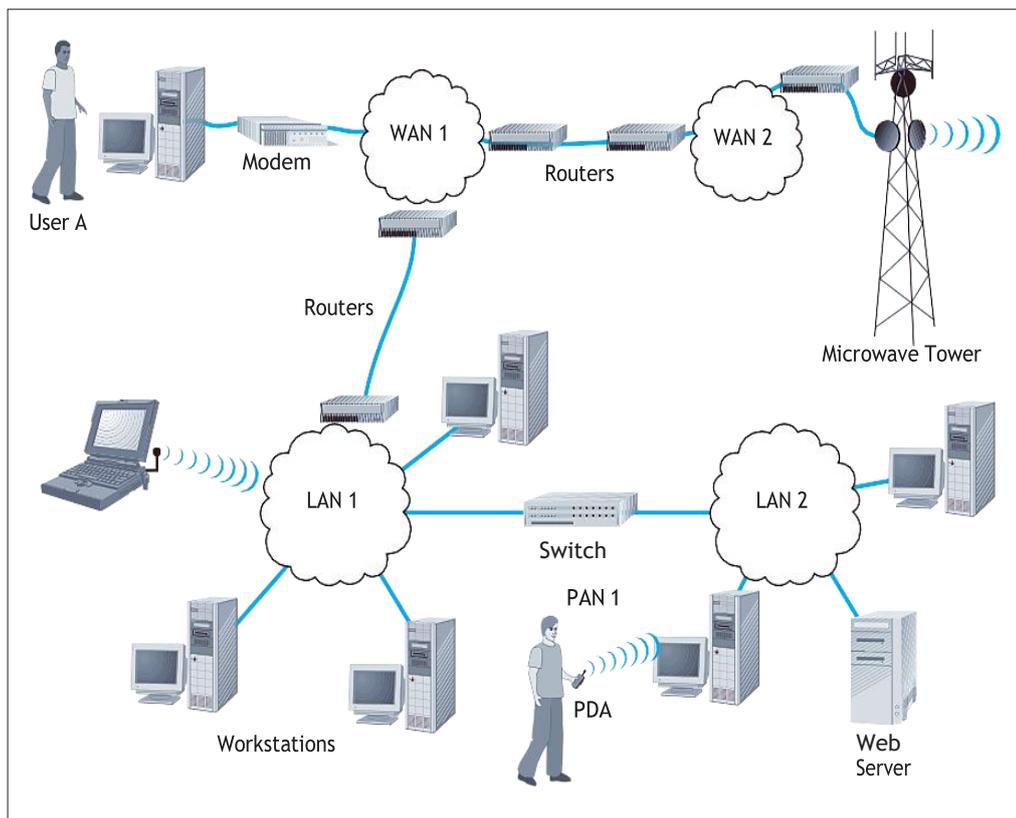
- Workstation, yaitu komputer pribadi/mikrokomputer (desktop, laptop, netbook, perangkat genggam, dll.) tempat tinggal pengguna
- Server, yaitu komputer yang menyimpan perangkat lunak jaringan dan file pengguna bersama atau pribadi
- Sakelar, yang merupakan titik pengumpulan kabel-kabel yang menghubungkan stasiun kerja
- Router, yang merupakan perangkat penghubung antara jaringan area lokal dan jaringan area luas

Ada juga banyak jenis jaringan area luas. Meskipun banyak teknologi berbeda yang digunakan untuk mendukung jaringan area luas, semua jaringan area luas mencakup komponen berikut:

- Node, yaitu perangkat komputasi yang memungkinkan stasiun kerja terhubung ke jaringan dan mengambil keputusan tentang ke mana rute suatu data

- Beberapa jenis saluran transmisi berkecepatan tinggi, yang mengalir dari satu titik ke titik lainnya
- Subjaringan, atau cloud, yang terdiri dari node dan jalur transmisi, dikumpulkan menjadi unit yang kohesif

Untuk melihat bagaimana jaringan area lokal dan jaringan area luas bekerja sama, pertimbangkan Pengguna A (di sudut kiri atas Gambar 1.1), yang ingin mengambil halaman Web dari server Web yang ditunjukkan di sudut kanan bawah. Untuk melakukan hal ini, komputer Pengguna A harus memiliki perangkat keras dan perangkat lunak yang diperlukan untuk berkomunikasi dengan jaringan area luas pertama yang ditemuinya, WAN 1 penyedia layanan Internet Pengguna A. Dengan asumsi bahwa komputer Pengguna A terhubung ke jaringan area luas ini melalui saluran telepon DSL, Pengguna A memerlukan beberapa jenis modem. Selain itu, jika jaringan area luas ini merupakan bagian dari Internet, komputer Pengguna A memerlukan perangkat lunak yang dapat berkomunikasi dengan Internet: TCP/IP (Transmission Control Protocol/Internet Protocol).



Gambar 1.1 Pandangan keseluruhan interkoneksi antara berbagai jenis jaringan

Perhatikan bahwa tidak ada koneksi langsung antara WAN 1, tempat Pengguna A berada, dan LAN 2, tempat server Web berada. Untuk memastikan bahwa permintaan halaman Web Pengguna A mencapai penerima yang dituju (server Web), perangkat lunak Pengguna A melampirkan informasi alamat yang sesuai yang digunakan WAN 1 untuk merutekan permintaan Pengguna A ke router yang menghubungkan WAN 1 ke LAN 1. Setelah permintaan ada di LAN 1, perangkat mirip sakelar yang menghubungkan LAN 1 dan LAN 2

menggunakan informasi alamat untuk meneruskan permintaan ke LAN 2. Informasi alamat tambahan kemudian merutekan permintaan halaman Web Pengguna A ke server Web, yang perangkat lunaknya menerima permintaan tersebut.

Dalam kondisi dan lalu lintas normal, prosedur ini mungkin hanya memakan waktu sepersekian detik. Ketika Anda mulai memahami semua langkah yang terlibat dan banyaknya transformasi yang harus dilakukan oleh permintaan halaman Web sederhana, fakta bahwa hanya dibutuhkan sepersekian detik untuk mengirimkannya sungguh menakjubkan.

1.4 TATA LETAK DASAR JARINGAN KOMUNIKAS

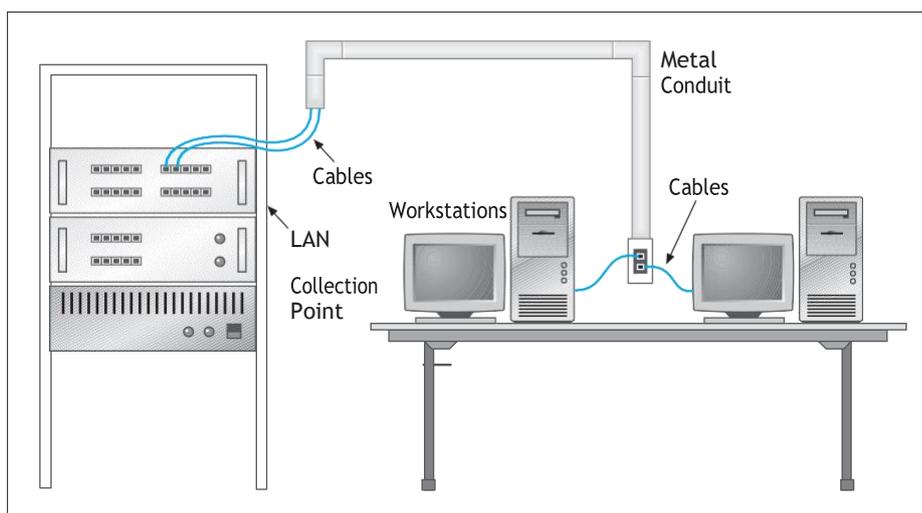
Awal bab ini menjelaskan beberapa aplikasi jaringan komputer dan komunikasi data yang Anda temui dalam kehidupan sehari-hari. Dari pengambilan sampel tersebut, Anda dapat melihat bahwa menetapkan semua jenis pekerjaan dan layanan yang menggunakan jaringan komputer dan komunikasi data akan menghasilkan daftar yang sangat banyak. Sebaliknya, mari kita periksa sistem jaringan dasar dan tata letaknya untuk melihat seberapa luas penggunaan komunikasi data dan jaringan komputer. Tata letak dasar yang akan kita periksa meliputi:

- Jaringan area mikrokomputer-ke-lokal
- Komputer mikro-ke-Internet
- Jaringan area lokal-ke-jaringan area lokal
- Jaringan area pribadi-ke-workstation
- Jaringan area lokal-ke-jaringan area metropolitan
- Jaringan area lokal-ke-jaringan area luas
- Jaringan area luas-ke-jaringan area luas
- Jaringan area sensor-ke-lokal
- Satelit dan gelombang mikro
- Ponsel
- Komputer terminal/mikrokomputer-ke-mainframe

Tata letak jaringan area mikro-ke-lokal

Mungkin tata letak jaringan yang paling umum saat ini, tata letak jaringan area mikro-komputer-ke-lokal ditemukan di hampir setiap lingkungan bisnis dan akademik dan bahkan di banyak rumah. Komputer mikro yang juga dikenal sebagai komputer pribadi, PC, komputer desktop, komputer laptop, notebook, netbook, atau workstation mulai muncul pada akhir tahun 1970an dan awal tahun 1980an. (Demi konsistensi, kita akan menggunakan istilah lama “komputer mikro” untuk menandakan semua jenis komputer yang berbasis mikroprosesor, drive disk, dan memori.) LAN, seperti yang akan kita lihat di Bab Tujuh, adalah alat yang sangat baik untuk menyediakan gerbang ke jaringan, perangkat lunak, dan periferal lain. Di beberapa LAN, kumpulan data yang menyertai perangkat lunak aplikasi berada di komputer pusat yang disebut server. Dengan menggunakan mikrokomputer yang terhubung ke LAN, pengguna akhir dapat meminta dan mengunduh kumpulan data, kemudian menjalankan aplikasi di komputer mereka. Jika pengguna ingin mencetak dokumen pada printer jaringan berkualitas

tinggi, LAN berisi perangkat lunak jaringan yang diperlukan untuk mengarahkan permintaan pencetakan mereka ke printer yang sesuai. Jika pengguna ingin mengakses email mereka dari server email perusahaan, jaringan area lokal menyediakan koneksi yang cepat dan stabil antara stasiun kerja pengguna dan server email. Jika pengguna ingin mengakses Internet, jaringan area lokal menyediakan pintu gerbang yang efektif ke dunia luar. Gambar 1.2 menunjukkan diagram tata letak jaringan area mikro-ke-lokal jenis ini.



Gambar 1.2 Lab komputer mikro, menunjukkan kabel yang keluar dari bagian belakang workstation dan berjalan ke titik pengumpulan LAN

Salah satu bentuk tata letak jaringan area mikro-ke-lokal yang umum dalam dunia bisnis adalah sistem klien/server. Dalam sistem klien/server, pengguna di komputer mikro, atau mesin klien, mengeluarkan permintaan untuk beberapa bentuk data atau layanan. Ini bisa berupa permintaan catatan database dari server database atau permintaan untuk mengambil pesan email dari server email. Permintaan ini berjalan melintasi sistem ke server yang berisi gudang data dan/atau program yang besar. Server mengisi permintaan dan mengembalikan hasilnya ke klien, menampilkan hasilnya di monitor klien.

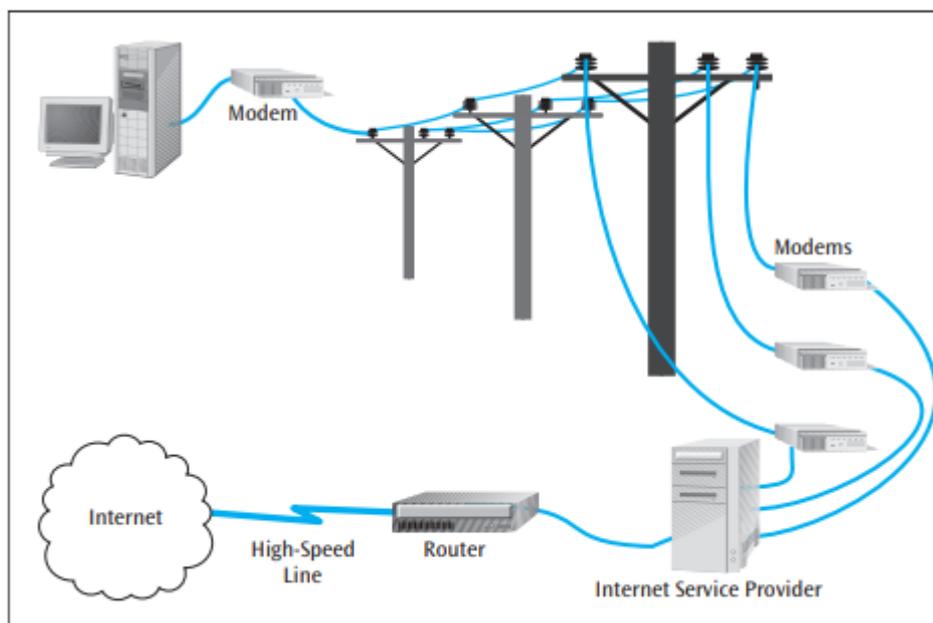
Jenis tata letak jaringan area mikro-ke-lokal yang semakin populer adalah tata letak nirkabel. Seorang pengguna yang duduk di workstation atau laptop menggunakan komunikasi nirkabel untuk mengirim dan menerima data ke dan dari titik akses nirkabel. Jalur akses ini terhubung ke jaringan area lokal dan pada dasarnya berfungsi sebagai “jembatan” antara perangkat pengguna nirkabel dan jaringan kabel. Meskipun pengaturan ini menggunakan transmisi frekuensi radio, kami masih menganggapnya sebagai tata letak jaringan area mikro-komputer-lokal.

Tata letak komputer mikro-ke-Internet

Dengan pertumbuhan Internet yang eksplosif dan keinginan pengguna untuk terhubung ke Internet dari rumah (baik untuk kesenangan atau alasan terkait pekerjaan), tata letak komputer mikro-ke-Internet terus berkembang dengan mantap. Awalnya, sebagian besar pengguna rumahan terhubung ke Internet melalui saluran telepon dial-up dan modem. Pengaturan ini memungkinkan kecepatan transfer data maksimum sekitar 56.000 bit per detik

(56 kbps). (Koneksi sebenarnya tidak mencapai 56 kbps, tapi itulah pembahasan yang akan kita bahas pada Bab Sebelas.) Modem dial-up bukan lagi tata letak yang paling sering digunakan. Saat ini, sebagian besar pengguna rumahan terhubung ke Internet menggunakan saluran pelanggan digital (DSL) atau mengakses Internet melalui layanan modem kabel. Seluruh layanan telekomunikasi ini akan dibahas lebih rinci pada Bab Sebelas. (Dalam membandingkan berbagai kecepatan transfer data layanan dan perangkat, kita akan menggunakan konvensi di mana huruf kecil k sama dengan 1000. Juga sebagai bagian dari konvensi, huruf kecil b akan mengacu pada bit, sedangkan huruf besar B mengacu pada byte.)

Untuk berkomunikasi dengan Internet menggunakan koneksi dial-up, DSL, atau modem kabel, komputer pengguna harus terhubung ke komputer lain yang sudah berkomunikasi dengan Internet. Cara termudah untuk membuat koneksi ini adalah melalui layanan penyedia layanan Internet (ISP). Dalam hal ini, komputer pengguna perlu memiliki perangkat lunak yang diperlukan untuk berkomunikasi dengan Internet. Internet “berbicara” hanya TCP/IP, jadi pengguna harus menggunakan perangkat lunak yang mendukung protokol TCP dan IP. Setelah komputer pengguna berbicara TCP/IP, koneksi ke Internet dapat dibuat. Gambar 1.3 menunjukkan tata letak mikrokomputer-ke-Internet.



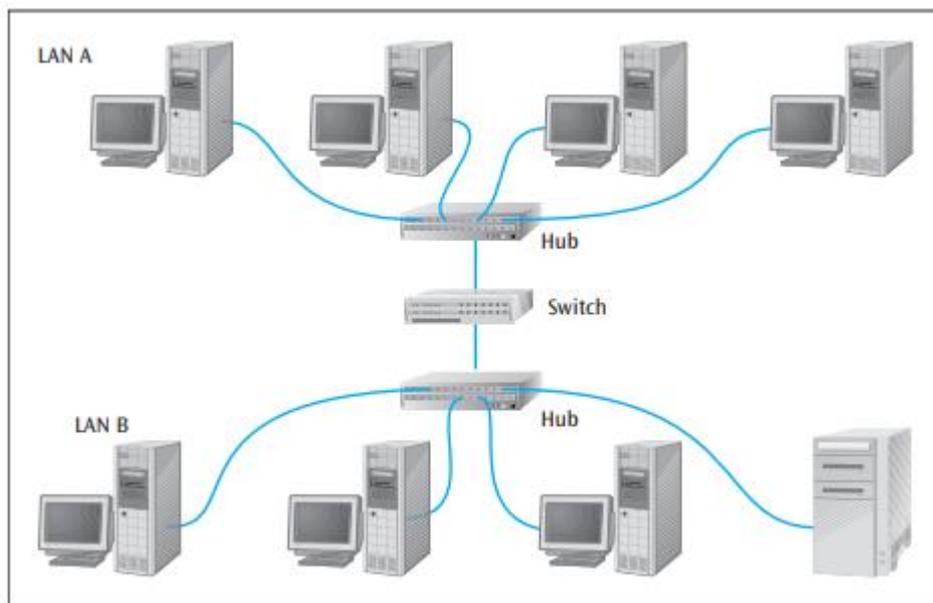
Gambar 1.3 Komputer mikro/workstation mengirimkan data melalui jalur DSL ke penyedia layanan Internet dan ke Internet

Tata letak jaringan area lokal-ke-jaringan area lokal

Karena jaringan area lokal merupakan standar dalam lingkungan bisnis dan akademis, tidak mengherankan jika banyak organisasi memerlukan layanan beberapa jaringan area lokal dan mungkin LAN ini perlu berkomunikasi satu sama lain. Misalnya, sebuah perusahaan mungkin menginginkan jaringan area lokal yang mendukung departemen risetnya berbagi printer laser warna yang mahal dengan jaringan area lokal departemen pemasarannya. Untungnya, dua jaringan area lokal dapat dihubungkan sehingga keduanya dapat berbagi

periferal serta perangkat lunak. Perangkat yang biasanya menghubungkan dua LAN atau lebih adalah switch dan router.

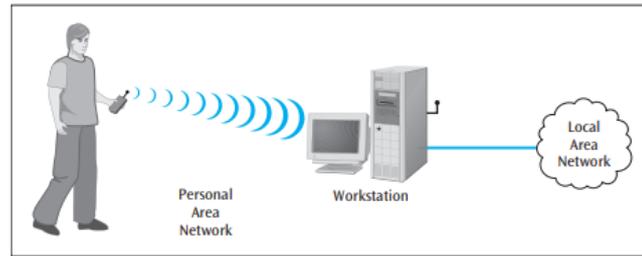
Dalam beberapa kasus, mencegah aliran data antar jaringan area lokal mungkin lebih penting daripada membiarkan data mengalir dari satu jaringan ke jaringan lainnya. Misalnya, beberapa bisnis mempunyai alasan politis untuk mendukung banyak jaringan setiap divisi mungkin ingin jaringannya sendiri berjalan sesuai keinginannya. Selain itu, mungkin ada alasan keamanan untuk membatasi arus lalu lintas antar jaringan; atau membiarkan data yang ditujukan untuk jaringan tertentu melintasi jaringan lain mungkin menghasilkan terlalu banyak lalu lintas jaringan. Perangkat yang menghubungkan jaringan area lokal juga dapat membantu mengelola jenis layanan ini. Misalnya, saklar dapat menyaring lalu lintas yang tidak ditujukan untuk jaringan tetangga, sehingga meminimalkan jumlah arus lalu lintas secara keseluruhan. Gambar 1-4 memberikan contoh dua LAN yang dihubungkan oleh sebuah switch.



Gambar 1.4 Dua jaringan area lokal dihubungkan oleh sebuah saklar

Tata letak jaringan area pribadi-ke-workstation

Jaringan area pribadi diciptakan pada akhir tahun 1990an dan merupakan salah satu bentuk jaringan komputer yang lebih baru. Dengan menggunakan transmisi nirkabel dengan perangkat seperti personal digital Assistant (PDA), komputer laptop, dan pemutar musik portabel, seseorang dapat mentransfer suara, data, dan musik dari perangkat genggam ke perangkat lain seperti workstation mikrokomputer (lihat Gambar 1.5). Demikian pula, pengguna dapat mengunduh data dari stasiun kerja ke salah satu perangkat portabel ini. Misalnya, pengguna mungkin menggunakan PDA untuk merekam catatan selama rapat. Setelah rapat selesai, pengguna dapat mengirimkan catatan melalui koneksi nirkabel dari PDA ke stasiun kerjanya.

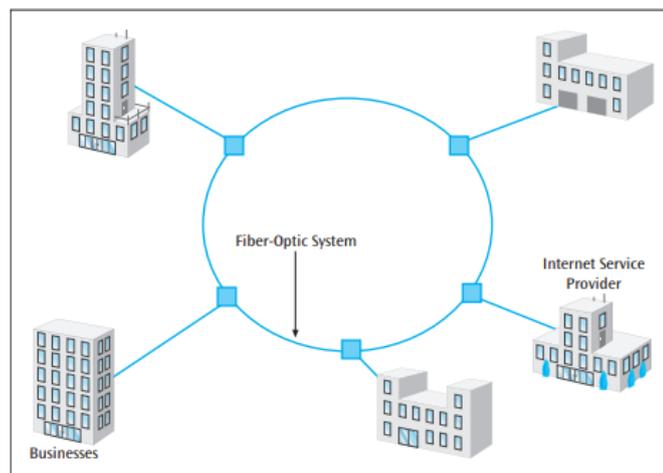


Gambar 1.5 Seorang pengguna mentransfer data dari asisten digital pribadi melalui jaringan area pribadi ke stasiun kerja yang terhubung ke jaringan area lokal

Stasiun kerja kemudian menjalankan pengolahan kata untuk membersihkan catatan, dan catatan yang telah diformat diunggah ke jaringan area lokal untuk disebarluaskan oleh perusahaan. Contoh lainnya adalah sambungan Bluetooth hands-free yang dipasang di telinga sehingga orang dapat berkomunikasi dengan telepon seluler tanpa mendekatkan telepon seluler ke telinga. Saat ini juga sangat umum untuk mentransfer foto dan video digital dari kamera ke komputer mikro menggunakan sinyal nirkabel jarak pendek.

Tata letak jaringan area lokal-ke-metropolitan

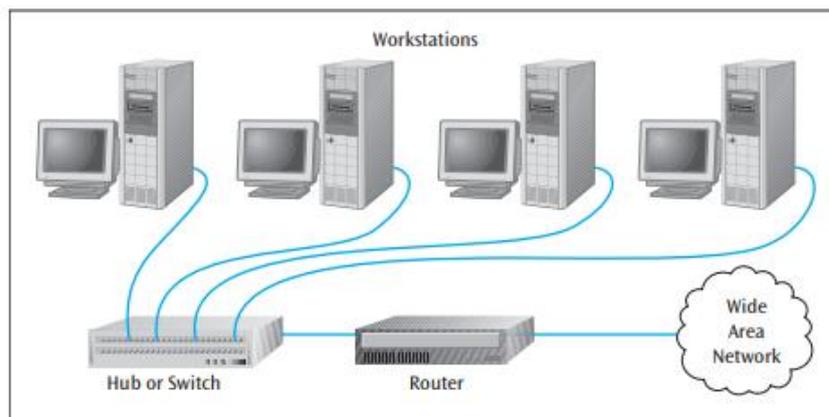
Menjelang akhir abad kedua puluh, muncul bentuk jaringan baru yang menghubungkan bisnis-bisnis dalam wilayah metropolitan. Biasanya, interkoneksi ini hanya menggunakan sambungan serat optik dengan kecepatan sangat tinggi. Jaringan baru ini diberi label jaringan area metropolitan. Jaringan area metropolitan adalah jaringan berkecepatan tinggi yang menghubungkan beberapa situs dalam wilayah geografis yang berdekatan, seperti wilayah perkotaan besar. Misalnya, bisnis yang memerlukan koneksi berkecepatan tinggi ke penyedia layanan Internet mereka mungkin menggunakan jaringan wilayah metropolitan untuk interkoneksi (lihat Gambar 1.6). Seperti yang akan kita lihat lebih detail di Bab Sembilan, jaringan area metropolitan merupakan persilangan antara jaringan area lokal dan jaringan area luas. Mereka dapat mentransfer data dengan kecepatan LAN yang cepat tetapi melintasi wilayah geografis yang lebih luas daripada yang biasanya dikaitkan dengan jaringan area lokal.



Gambar 1.6 Bisnis saling terhubung dalam wilayah metropolitan besar melalui jaringan wilayah metropolitan

Tata letak jaringan area lokal ke jaringan area luas

Anda telah melihat bahwa jaringan area lokal umumnya ditemukan di lingkungan bisnis dan akademik. Jika pengguna yang bekerja di komputer mikro yang terhubung ke jaringan area lokal ingin mengakses Internet (jaringan area luas), jaringan area lokal pengguna harus memiliki koneksi ke Internet. Perangkat yang disebut router digunakan untuk menghubungkan kedua jaringan ini. Router mengubah data jaringan area lokal menjadi data jaringan area luas. Ia juga menjalankan fungsi keamanan dan harus diprogram dengan benar untuk menerima atau menolak jenis paket data masuk dan keluar tertentu. Gambar 1.7 menunjukkan jaringan area lokal yang terhubung ke jaringan area luas melalui router.



Gambar 1.7 Tata letak jaringan area lokal hingga jaringan area luas

Tata letak jaringan area luas ke jaringan area luas

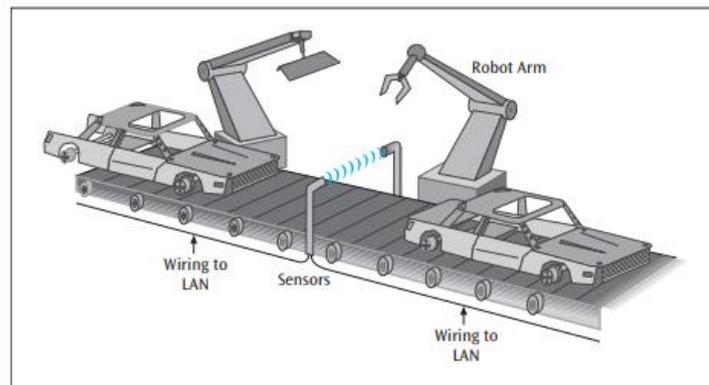
Internet bukanlah sebuah jaringan tunggal melainkan kumpulan ribuan jaringan. Untuk menempuh jarak berapa pun melalui Internet, paket data pasti akan melewati beberapa jaringan area luas. Menghubungkan wide area network ke wide area network memerlukan perangkat khusus yang dapat merutekan lalu lintas data dengan cepat dan efisien. Perangkat ini adalah router berkecepatan tinggi. Setelah paket data memasuki router berkecepatan tinggi, alamat di lapisan jaringan (alamat IP) diekstraksi, keputusan perutean dibuat, dan paket data diteruskan ke segmen jaringan area luas berikutnya. Saat paket data bergerak melalui Internet, router demi router membuat keputusan perutean, memindahkan data menuju tujuan akhirnya. Kita akan mengkaji Internet secara lebih rinci di Bab Sepuluh, kemudian menindaklanjuti dengan pembahasan beberapa jenis teknologi jaringan area luas lainnya di Bab Sebelas.

Tata letak jaringan area sensor-ke-lokal

Tata letak umum lainnya yang ditemukan dalam kehidupan sehari-hari adalah tata letak jaringan area sensor-ke-lokal. Dalam tata letak jenis ini, tindakan seseorang atau objek memicu sensor misalnya, lampu belok kiri di persimpangan lalu lintas yang terhubung ke jaringan. Di banyak jalur belok kiri, sinyal belok kiri terpisah akan muncul jika dan hanya jika satu atau lebih kendaraan berada di jalur belok kiri. Sebuah sensor yang tertanam di jalan raya mendeteksi pergerakan mobil di jalur atas dan memicu mekanisme belok kiri di kotak kendali

sinyal lalu lintas di pinggir jalan. Jika kotak kontrol sinyal lalu lintas ini terhubung ke sistem kontrol lalu lintas yang lebih besar, sensor terhubung ke jaringan area lokal.

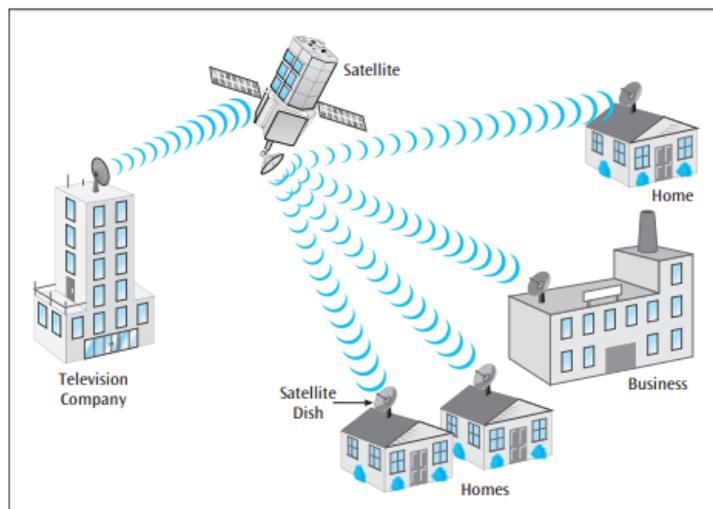
Contoh lain tata letak jaringan area sensor-ke-lokal ditemukan dalam lingkungan manufaktur. Jalur perakitan, perangkat kontrol robotik, kontrol suhu oven, dan peralatan analisis kimia sering kali menggunakan sensor yang terhubung ke komputer pengumpul data yang mengontrol pergerakan dan pengoperasian, membunyikan alarm, dan menghitung hasil eksperimen atau kontrol kualitas. Gambar 1-8 menunjukkan diagram tata letak jaringan area sensor-ke-lokal pada lingkungan manufaktur.



Gambar 1.8 Sebuah mobil bergerak menuruni jalur perakitan dan memicu sebuah sensor

Tata letak satelit dan gelombang mikro

Tata letak satelit dan gelombang mikro merupakan teknologi yang terus berkembang dan digunakan dalam berbagai aplikasi. Jika jarak antara dua jaringan sangat jauh dan memasang kabel di antara keduanya akan sulit (jika bukan tidak mungkin), sistem transmisi satelit dan gelombang mikro dapat menjadi cara yang sangat efektif untuk menghubungkan dua jaringan atau sistem komputer.



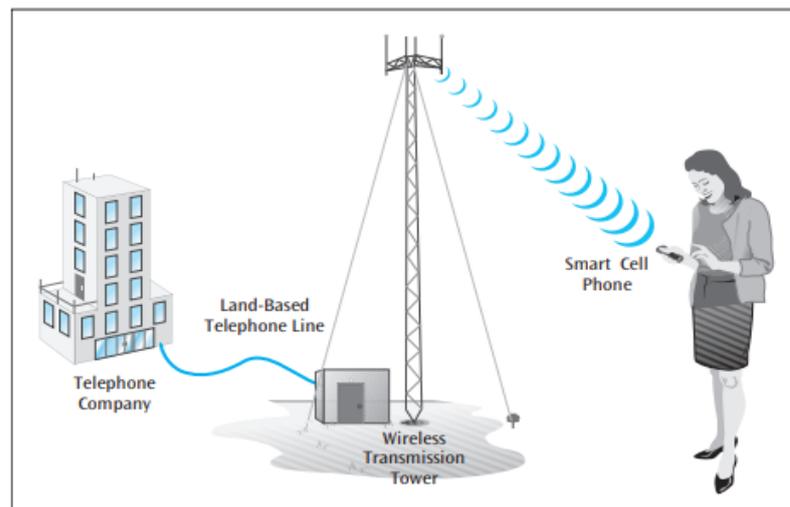
Gambar 1.9 Contoh perusahaan televisi yang menggunakan sistem satelit untuk menyiarkan layanan televisi ke rumah-rumah dan bisnis

Contoh penerapannya meliputi TV satelit digital, meteorologi, operasi intelijen, telepon maritim bergerak, sistem navigasi GPS, email nirkabel, sistem telepon seluler di seluruh dunia, dan konferensi video. Gambar 1.9 menunjukkan diagram sistem satelit pada umumnya.

Tata letak ponsel

Salah satu bidang pertumbuhan paling eksplosif dalam beberapa tahun terakhir adalah jaringan telepon seluler. Gambar 1.10 menunjukkan contoh PDA genggam yang, selain melakukan panggilan telepon, juga dapat mengirim dan menerima data. PDA mempunyai modem yang terpasang, yang mentransmisikan data PDA melalui jaringan telepon seluler ke pusat peralihan telepon seluler. Pusat switching kemudian mentransfer data PDA melalui jaringan telepon umum atau melalui koneksi ke Internet.

Banyak perangkat genggam baru yang menggabungkan kemampuan mengakses data dengan telepon seluler dan dapat mentransfer data melalui koneksi telepon seluler.



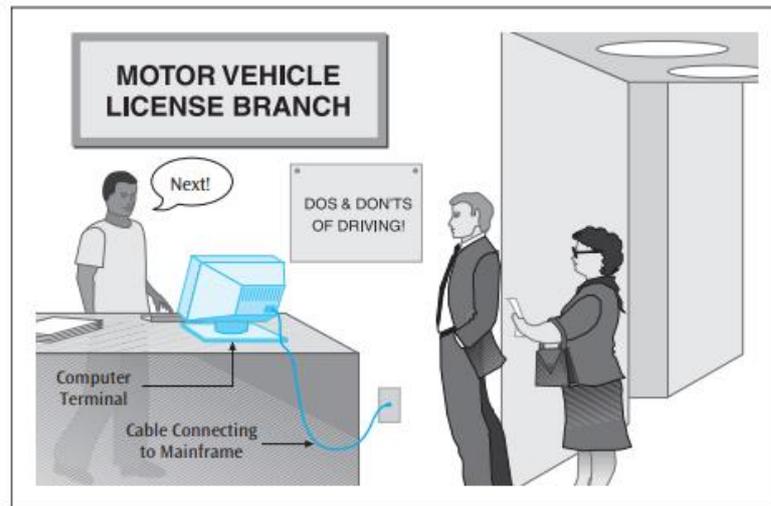
Gambar 1.10 Contoh pengguna ponsel pintar yang mengirim dan menerima data

Tata letak komputer terminal/mikrokomputer ke mainframe

Saat ini, banyak bisnis yang masih menggunakan tata letak terminal-ke-mainframe, meskipun jumlah sistem yang digunakan tidak seperti dulu. Selama tahun 1960an dan 1970an, tata letak terminal-ke-mainframe ada di hampir setiap lingkungan kantor, manufaktur, dan akademik. Sistem jenis ini masih digunakan untuk aplikasi penyelidikan/respons, aplikasi interaktif, dan aplikasi entri data, seperti yang mungkin Anda temukan ketika mengajukan permohonan SIM baru di Departemen Kendaraan Bermotor (Gambar 1.11).

Tata letak terminal-ke-mainframe pada tahun 1960-an dan 1970-an menggunakan terminal “bodoh” karena pengguna akhir melakukan operasi entri dan pengambilan data yang relatif sederhana, dan stasiun kerja dengan daya komputasi dan penyimpanan yang besar tidak diperlukan. Terminal komputer adalah perangkat yang pada dasarnya berupa keyboard dan layar tanpa kemampuan penyimpanan jangka panjang dan sedikit, jika ada, kekuatan pemrosesan. Terminal komputer digunakan untuk memasukkan data ke dalam suatu sistem,

seperti komputer mainframe, dan kemudian menampilkan hasilnya dari mainframe. Karena terminal tidak memiliki daya komputasi yang besar, komputer mainframe mengontrol pengiriman dan penerimaan data ke dan dari setiap terminal. Hal ini memerlukan jenis protokol khusus (seperangkat aturan yang digunakan oleh perangkat komunikasi), dan data biasanya dikirimkan pada kecepatan yang relatif lambat, seperti 9600 atau 19.200 bit per detik (bps).



Gambar 1.11 Menggunakan terminal (atau stasiun kerja klien tipis) untuk melakukan transaksi masukan berbasis teks

Selama periode ini, banyak pengguna akhir yang memiliki terminal di meja mereka kini juga menemukan komputer mikro di sana (sehingga hanya memiliki sedikit ruang untuk hal lain). Belakangan, kartu emulasi terminal dikembangkan, yang memungkinkan komputer mikro meniru kemampuan terminal komputer. Ketika kartu emulasi terminal ditambahkan ke mikrokomputer, terminal dihapus dari meja pengguna akhir, dan mikrokomputer mulai menjalankan kedua fungsi tersebut. Sekarang, jika pengguna menginginkannya, mereka dapat mengunduh informasi dari komputer mainframe ke mikrokomputer mereka, melakukan operasi pada data, dan kemudian mengunggah informasi tersebut ke mainframe. Saat ini, jarang sekali kita melihat terminal komputer yang bodoh. Sebaliknya, sebagian besar pengguna menggunakan mikrokomputer dan mengakses mainframe menggunakan kartu emulasi terminal, browser Web dan antarmuka Web, perangkat lunak Telnet (lebih lanjut tentang ini di Bab Sepuluh), atau klien tipis. Stasiun kerja klien tipis mirip dengan komputer mikro tetapi tidak memiliki penyimpanan hard drive.

1.5 KONVERGENSI

Kamus mungkin mendefinisikan “konvergensi” sebagai proses berkumpul menuju satu titik. Sehubungan dengan jaringan komputer dan sistem komunikasi, definisi ini cukup relevan. Selama bertahun-tahun, industri komunikasi telah melihat dan terus melihat berbagai aplikasi jaringan dan teknologi yang mendukungnya menyatu menjadi satu teknologi yang mampu

mendukung berbagai aplikasi. Secara khusus, kita dapat mendefinisikan tiga jenis konvergensi: konvergensi teknologi, konvergensi protokol, dan konvergensi industri. Misalnya, salah satu contoh konvergensi teknologi yang paling awal dan paling umum adalah penggunaan komputer dan modem untuk mengirimkan data melalui sistem telepon. Ini adalah contoh sistem transmisi suara yang menyatu dengan sistem transmisi data dan menghasilkan satu sistem yang mampu mendukung data dan suara. Pada tahun 1990an, sistem telepon membawa lebih banyak data komputer dibandingkan suara. Pada waktu yang hampir bersamaan, jaringan area lokal mulai mentransfer panggilan telepon. Karena jaringan area lokal awalnya dirancang untuk aplikasi data, ini adalah contoh lain dari konvergensi sistem suara dan data. Sekarang kita melihat pertumbuhan substansial dalam bidang *Voice over Internet Protocol (VoIP)*. VoIP melibatkan konversi sinyal suara menjadi paket dan kemudian mengirimkan paket tersebut melalui jaringan berbasis paket seperti jaringan area lokal dan Internet.

Saat ini kita melihat lebih banyak contoh konvergensi teknologi, khususnya di pasar nirkabel. Misalnya, sekarang sudah menjadi hal yang lumrah untuk mengambil foto menggunakan ponsel dan kemudian mentransfer gambar tersebut melalui jaringan ponsel ke ponsel lain. Tak lama setelah diperkenalkannya telepon seluler berkemampuan foto, telepon seluler juga mampu mengirim dan menerima pesan instan. Kemudian pada tahun 2005, penyedia telepon seluler mulai menawarkan layanan yang memungkinkan pengguna mengirimkan data berkecepatan tinggi melalui koneksi telepon seluler. Ini semua adalah contoh konvergensi dua aplikasi berbeda (misalnya, fotografi digital dan telepon seluler dalam kasus telepon seluler yang mendukung foto) menjadi satu teknologi. Seperti yang akan kita lihat pada bab selanjutnya, banyak perusahaan telepon yang menyediakan layanan telepon lokal dan jarak jauh telah berkonvergensi menjadi lebih sedikit perusahaan. Ini adalah contoh konvergensi industri. Juga di bab selanjutnya, kita akan melihat bagaimana protokol jaringan lama telah digantikan atau digabungkan dengan protokol lain, sehingga menunjukkan konvergensi protokol.

Sepanjang sisa buku ini, kita akan mengkaji contoh konvergensi lainnya dalam industri komunikasi. Selain memperkenalkan teknologi yang terlibat, kami juga akan mengkaji dampak konvergensi teknologi tertentu terhadap pengguna individu dan bisnis.

1.6 ARSITEKTUR JARINGAN

Sekarang setelah Anda mengetahui berbagai jenis jaringan dan tata letaknya, kita memerlukan kerangka kerja untuk memahami bagaimana semua komponen jaringan saling beroperasi. Ketika seseorang menggunakan jaringan komputer untuk menjalankan suatu aplikasi, banyak bagian yang bersatu untuk membantu pengoperasiannya. Arsitektur jaringan, atau model komunikasi, menempatkan bagian-bagian jaringan yang sesuai dalam beberapa lapisan. Lapisan menentukan model untuk fungsi atau layanan yang perlu dilakukan. Setiap lapisan dalam model mendefinisikan layanan apa yang disediakan oleh perangkat keras atau perangkat lunak (atau keduanya). Dua arsitektur paling umum yang dikenal saat ini adalah rangkaian protokol TCP/IP dan model *Open Systems Interconnection (OSI)*. Rangkaian protokol

TCP/IP adalah model kerja (saat ini digunakan di Internet), sedangkan model OSI (awalnya dirancang sebagai model kerja) telah diturunkan menjadi model teoretis. Kami akan membahas kedua arsitektur ini secara lebih rinci di halaman berikut. Namun pertama-tama Anda harus mengetahui lebih banyak tentang komponen-komponen jaringan dan bagaimana arsitektur jaringan membantu mengatur komponen-komponen tersebut.

Pertimbangkan bahwa jaringan komputer pada umumnya dalam suatu bisnis berisi komponen-komponen berikut yang harus berinteraksi dalam berbagai cara:

- Kabel
- Papan sirkuit tercetak
- Konektor dan jack kabel
- Komputer
- Konsentrator perkabelan yang terletak di pusat
- Disk dan tape drive
- Aplikasi komputer seperti pengolah kata, program email, dan perangkat lunak akuntansi, pemasaran, dan perdagangan elektronik
- Program komputer yang mendukung transfer data, memeriksa kesalahan saat data ditransfer, mengizinkan akses ke jaringan, dan melindungi transaksi pengguna dari tampilan yang tidak sah

Sejumlah besar komponen jaringan dan kemungkinan interaksinya menimbulkan dua pertanyaan. Pertama, bagaimana semua bagian ini bekerja sama secara harmonis? Anda tidak ingin dua bagian menjalankan fungsi yang sama, atau tidak ada bagian yang menjalankan fungsi yang diperlukan. Ibarat elemen mesin yang berfungsi dengan baik, seluruh komponen jaringan komputer harus bekerja sama untuk menghasilkan suatu produk.

Kedua, apakah pilihan satu bagian bergantung pada pilihan bagian lainnya? Untuk membuat karya menjadi modular mungkin, Anda tidak ingin pemilihan satu karya membatasi pilihan karya lainnya. Misalnya, jika Anda membuat jaringan dan awalnya berencana menggunakan satu jenis pengkabelan namun kemudian berubah pikiran dan menggunakan jenis pengkabelan yang berbeda, apakah perubahan tersebut akan memengaruhi pilihan pengolah kata Anda? Interaksi seperti itu tampaknya sangat tidak mungkin terjadi. Alternatifnya, dapatkah pilihan kabel mempengaruhi pilihan program perangkat lunak yang memeriksa kesalahan dalam data yang dikirim melalui kabel? Jawaban atas pertanyaan ini tidak begitu jelas.

Untuk menjaga bagian-bagian jaringan komputer bekerja sama secara harmonis dan memungkinkan modularitas antar bagian, organisasi nasional dan internasional mengembangkan arsitektur jaringan, yang merupakan lapisan protokol kohesif yang mendefinisikan serangkaian layanan komunikasi. Perhatikan contoh non-komputer berikut. Kebanyakan organisasi yang memproduksi beberapa jenis produk atau melakukan suatu jasa mempunyai pembagian kerja. Asisten kantor mengerjakan dokumen; akuntan menyimpan pembukuan; pekerja melakukan tugas-tugas manual; ilmuwan merancang produk; insinyur menguji produk; manajer mengendalikan operasi. Jarang ada satu orang yang mampu melakukan semua tugas tersebut. Aplikasi perangkat lunak besar beroperasi dengan cara yang

sama. Prosedur yang berbeda melaksanakan tugas yang berbeda, dan keseluruhannya tidak akan berfungsi tanpa pengoperasian yang tepat dari setiap bagiannya. Aplikasi jaringan komputer tidak terkecuali. Seiring dengan meningkatnya jumlah aplikasi, kebutuhan akan pembagian kerja menjadi semakin penting. Aplikasi jaringan komputer juga memiliki penggambaran fungsi pekerjaan yang serupa. Penggambaran ini adalah arsitektur jaringan. Mari kita periksa dua arsitektur atau model jaringan kita: rangkaian protokol TCP/IP, diikuti oleh model OSI.

Rangkaian protokol TCP/IP

Rangkaian protokol TCP/IP diciptakan oleh sekelompok ilmuwan komputer untuk mendukung jaringan jenis baru (ARPANET) yang dipasang di seluruh Amerika Serikat pada tahun 1960an dan 1970an. Tujuannya adalah untuk menciptakan arsitektur terbuka yang memungkinkan hampir semua jaringan saling berkomunikasi. Desainnya didasarkan pada sejumlah lapisan, di mana pengguna akan terhubung di lapisan paling atas dan akan diisolasi dari detail sinyal listrik yang terdapat di lapisan bawah.

Jumlah lapisan dalam suite tidak statis. Faktanya, beberapa buku menyajikan rangkaian protokol TCP/IP sebagai empat lapisan, sementara yang lain menyajikannya dalam lima lapisan. Meski begitu, sumber yang berbeda menggunakan nama yang berbeda untuk setiap lapisannya. Untuk buku ini, kita akan mendefinisikan lima lapisan, seperti yang ditunjukkan pada Gambar 1-12: aplikasi, transportasi, jaringan, akses jaringan, dan fisik. Perhatikan bahwa lapisan tersebut tidak menentukan protokol yang tepat atau layanan yang tepat. Dengan kata lain, rangkaian protokol TCP/IP tidak memberi tahu kita, misalnya, jenis kabel atau konektor apa yang digunakan untuk menghubungkan bagian-bagian jaringan. Pilihan itu diserahkan kepada perancang atau pelaksana sistem.

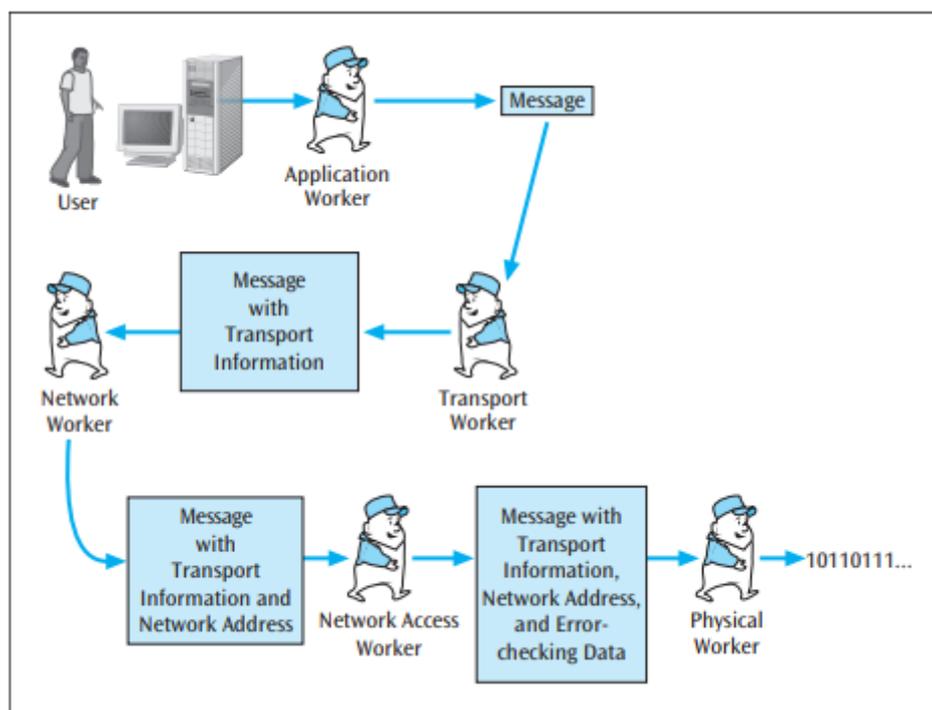


Gambar 1.12 Lima lapisan rangkaian protokol TCP/IP

Sebaliknya, rangkaian tersebut hanya mengatakan bahwa jika Anda menentukan jenis kabel atau konektor tertentu, Anda melakukannya di lapisan tertentu. Selain itu, setiap lapisan rangkaian protokol TCP/IP menyediakan layanan untuk lapisan berikutnya. Misalnya, lapisan transport memastikan data yang diterima pada akhir transmisi sama persis dengan data yang awalnya dikirimkan, namun hal ini bergantung pada lapisan jaringan untuk menemukan jalur terbaik bagi data yang akan diambil dari satu titik ke jaringan berikutnya. Dengan setiap

lapisan menjalankan fungsinya yang ditentukan, lapisan-lapisan tersebut bekerja sama untuk memungkinkan aplikasi mengirimkan datanya melalui jaringan komputer. Mari kita lihat contoh aplikasi email sederhana (Gambar 1.13) untuk memahami bagaimana lapisan rangkaian protokol TCP/IP bekerja sama.

Aplikasi jaringan yang umum adalah email. Sebuah program email yang menerima dan mengirimkan pesan, “*Andy, bagaimana kalau makan siang? Sharon,*” memiliki banyak langkah. Dengan menggunakan rangkaian protokol TCP/IP, langkah-langkahnya mungkin terlihat seperti berikut. Untuk memulai, “*pekerja aplikasi*” email meminta pengguna untuk memasukkan pesan dan menentukan penerima yang dituju. Pekerja aplikasi akan membuat paket data yang sesuai dengan isi pesan dan alamat, dan mengirimkannya ke “*pekerja transportasi,*” yang bertanggung jawab untuk menyediakan integritas transportasi secara keseluruhan. Pekerja transportasi mungkin menjalin koneksi dengan penerima yang dituju, memantau aliran antara pengirim dan penerima, dan melakukan operasi yang diperlukan untuk memulihkan data yang hilang jika beberapa data hilang atau tidak dapat dibaca.



Gambar 1.13 “Pekerja jaringan” menjalankan tugas pekerjaannya pada setiap lapisan dalam model

“*Pekerja jaringan*” kemudian akan mengambil paket data dari pekerja transportasi dan mungkin menambahkan informasi perutean sehingga paket data dapat menemukan jalannya melalui jaringan. Berikutnya yang mendapatkan paket data adalah “*pekerja akses jaringan*”, yang akan memasukkan informasi pengecekan kesalahan dan menyiapkan paket data untuk transmisi. Pekerja terakhir adalah “*pekerja fisik*”, yang akan mengirimkan paket data melalui kabel atau melalui udara menggunakan gelombang radio.

Setiap pekerja mempunyai fungsi pekerjaannya masing-masing. Gambar 1.13 menunjukkan bagaimana para pekerja ini bekerja sama untuk menciptakan satu paket transmisi. Mari kita periksa setiap lapisan lebih detail. Lapisan atas rangkaian protokol TCP/IP, lapisan aplikasi, mendukung aplikasi jaringan dan dalam beberapa kasus mungkin menyertakan layanan tambahan seperti enkripsi atau kompresi. Lapisan aplikasi TCP/IP mencakup beberapa aplikasi yang sering digunakan:

- *Hypertext Transfer Protocol* (HTTP) untuk memungkinkan browser dan server Web mengirim dan menerima halaman World Wide Web
- *Simple Mail Transfer Protocol* (SMTP) yang memungkinkan pengguna mengirim dan menerima surat elektronik
- *File Transfer Protocol* (FTP) untuk mentransfer file dari satu sistem komputer ke sistem komputer lainnya
 - Telnet untuk memungkinkan pengguna jarak jauh log in ke sistem komputer lain
 - Simple Network Management Protocol (SNMP) yang memungkinkan berbagai elemen dalam jaringan komputer dikelola dari satu titik

Lapisan berikutnya dalam rangkaian protokol TCP/IP adalah lapisan transport. Lapisan transport TCP/IP biasanya menggunakan TCP untuk memelihara koneksi end-to-end yang bebas kesalahan. Untuk menjaga koneksi ini, TCP menyertakan informasi kontrol kesalahan jika satu paket dari rangkaian paket tidak tiba di tujuan akhir, dan informasi pengurutan paket sehingga semua paket tetap berada dalam urutan yang benar. Kami mengatakan bahwa lapisan transport melakukan kontrol kesalahan ujung ke ujung dan kontrol aliran ujung ke ujung. Ini berarti lapisan transport tidak digunakan ketika paket data berpindah dari titik ke titik dalam jaringan lapisan ini hanya digunakan pada dua titik akhir koneksi. TCP bukan satu-satunya protokol yang mungkin ditemukan pada lapisan transport TCP/IP. User Datagram Protocol (UDP) adalah alternatif yang juga digunakan, meskipun lebih jarang, dalam rangkaian protokol TCP/IP.

Dua lapisan yang dijelaskan sejauh ini disebut lapisan ujung ke ujung. Mereka bertanggung jawab atas data yang dikirimkan antara titik akhir koneksi jaringan. Dengan kata lain, lapisan ini melakukan operasinya hanya pada titik awal dan titik akhir koneksi jaringan. Tiga lapisan tersisa dari rangkaian protokol TCP/IP jaringan, akses jaringan, dan lapisan fisik bukanlah lapisan ujung ke ujung. Mereka melakukan operasinya di setiap node (atau perangkat) di sepanjang jalur jaringan, tidak hanya di titik akhir.

Lapisan jaringan TCP/IP, terkadang disebut lapisan Internet atau lapisan IP, digunakan untuk mentransfer data di dalam dan antar jaringan. Internet Protocol (IP) adalah perangkat lunak yang menyiapkan paket data sehingga dapat berpindah dari satu jaringan ke jaringan lain di Internet atau dalam sekumpulan jaringan perusahaan. Saat lapisan ini mengirimkan paket dari node ke node, ia menghasilkan alamat jaringan yang diperlukan sistem untuk mengenali penerima berikutnya yang dituju. Untuk memilih jalur melalui jaringan, lapisan jaringan menentukan informasi routing dan menerapkannya pada setiap paket atau kelompok paket.

Lapisan bawah berikutnya dari rangkaian protokol TCP/IP adalah lapisan akses jaringan. Jika lapisan jaringan berhubungan dengan melewati paket melalui Internet, maka lapisan akses jaringan adalah lapisan yang menerima data dari stasiun kerja pengguna ke Internet. Dalam sebagian besar kasus, koneksi yang mendapatkan data dari stasiun kerja pengguna ke Internet adalah jaringan area lokal. Dengan demikian, lapisan akses jaringan menyiapkan paket data (disebut frame pada lapisan ini) untuk transmisi dari stasiun kerja pengguna ke router yang berada di antara jaringan area lokal dan Internet. Bingkai ini berisi pengidentifikasi yang menandakan awal dan akhir bingkai, serta ruang untuk informasi kontrol dan informasi alamat. Selain itu, lapisan akses jaringan dapat menggabungkan beberapa bentuk perangkat lunak pendeteksi kesalahan. Jika kesalahan terjadi selama transmisi, lapisan akses jaringan bertanggung jawab atas pengendalian kesalahan, yang dilakukan dengan memberi tahu pengirim kesalahan tersebut. Lapisan akses jaringan mungkin juga melakukan kontrol aliran. Dalam jaringan besar di mana data berpindah dari satu node ke node lain saat melintasi jaringan, kontrol aliran memastikan bahwa satu node tidak membebani node berikutnya dengan terlalu banyak data. Perhatikan bahwa operasi akses jaringan ini sangat mirip dengan beberapa operasi lapisan transport. Perbedaan utamanya adalah bahwa lapisan transport mungkin melakukan operasinya hanya pada titik akhir, sedangkan lapisan akses jaringan melakukan operasinya pada setiap pemberhentian (node) di sepanjang jalur. Ini juga merupakan lapisan terakhir sebelum data diserahkan untuk transmisi melalui media. Lapisan akses jaringan sering disebut lapisan data link.

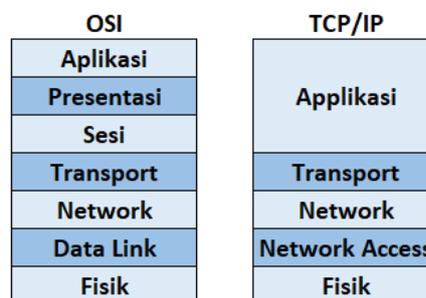
Lapisan paling bawah dalam rangkaian protokol TCP/IP (atau setidaknya menurut cara kita melakukannya) adalah lapisan fisik. Lapisan fisik adalah lapisan di mana transmisi data sebenarnya terjadi. Seperti disebutkan sebelumnya, transmisi ini dapat dilakukan melalui kabel fisik, atau dapat berupa sinyal radio yang ditransmisikan melalui udara. Untuk melakukan transmisi bit ini, lapisan fisik menangani level tegangan, dimensi konektor dan konektor, konfigurasi pin, dan masalah listrik dan mekanis lainnya. Lebih jauh lagi, karena data digital atau analog dikodekan atau dimodulasi menjadi sinyal digital atau analog pada titik proses ini, lapisan fisik juga menentukan teknik pengkodean atau modulasi yang akan digunakan dalam jaringan. Perhatikan bahwa beberapa orang menggabungkan lapisan akses jaringan dan lapisan fisik menjadi satu lapisan.

Memiliki lapisan yang terdefinisi dengan jelas memungkinkan Anda untuk “menarik” satu lapisan dan menyisipkan lapisan yang setara tanpa mempengaruhi lapisan lainnya. Sebagai contoh, mari kita asumsikan suatu jaringan dirancang untuk kabel berbasis tembaga. Belakangan, pemilik sistem memutuskan untuk mengganti kabel berbahan tembaga dengan kabel serat optik. Meskipun perubahan dilakukan pada lapisan fisik, perubahan apa pun tidak perlu dilakukan pada lapisan lainnya. Namun pada kenyataannya, ada beberapa hubungan antar lapisan sistem komunikasi yang tidak dapat diabaikan. Misalnya, jika organisasi fisik jaringan area lokal diubah (katakanlah dari tata letak kabel ke tata letak nirkabel), kemungkinan besar deskripsi bingkai pada lapisan akses jaringan juga perlu diubah. (Kita akan membahas fenomena ini di Bab Tujuh.) Rangkaian protokol TCP/IP mengenali hubungan ini dan menggabungkan banyak layanan lapisan fisik dan data link ke dalam satu lapisan.

Model OSI

Meskipun rangkaian protokol TCP/IP adalah model pilihan untuk hampir semua jaringan yang terpasang, penting untuk mempelajari arsitektur ini dan model OSI. Banyak buku dan artikel, ketika menjelaskan suatu produk atau protokol, sering merujuk pada model OSI dengan pernyataan seperti, “*Produk ini sesuai dengan OSI lapisan x.*” Jika Anda belum terbiasa dengan berbagai lapisan model OSI dan rangkaian protokol TCP/IP, kurangnya pengetahuan dasar yang penting ini mungkin menghalangi pemahaman Anda tentang konsep yang lebih maju di masa depan.

Model OSI dirancang dengan tujuh lapisan, seperti ditunjukkan pada Gambar 1-14. Perhatikan lebih lanjut hubungan antara lima lapisan rangkaian protokol TCP/IP dan tujuh lapisan model OSI. Lapisan paling atas dalam model OSI adalah lapisan aplikasi, tempat aplikasi yang menggunakan jaringan berada. Lapisan OSI ini mirip dengan lapisan aplikasi dalam rangkaian protokol TCP/IP. Lapisan berikutnya dalam model OSI, lapisan presentasi, melakukan serangkaian fungsi lain-lain yang diperlukan untuk menyajikan paket data dengan benar kepada pengirim atau penerima. Misalnya, lapisan presentasi mungkin melakukan konversi karakter ASCII ke non-ASCII, enkripsi dan dekripsi dokumen aman, dan kompresi data menjadi unit yang lebih kecil. Tidak ada lapisan presentasi terpisah dalam rangkaian protokol TCP/IP.



Gambar 1.14 Tujuh lapisan model OSI dibandingkan dengan lima lapisan rangkaian protokol TCP/IP

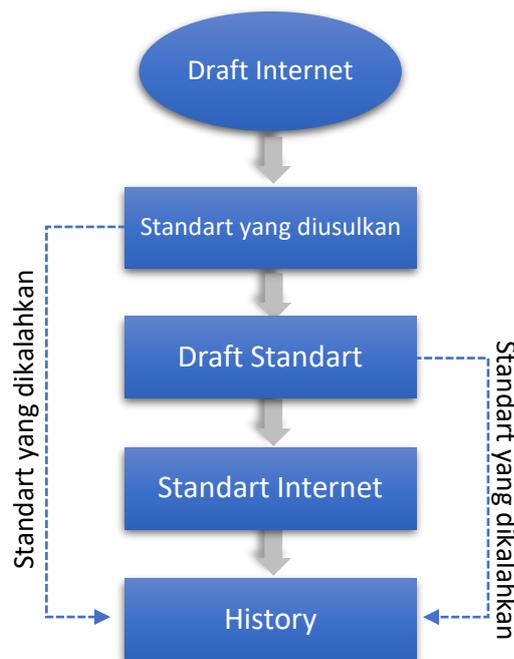
Permintaan Komentar Internet (RFC)

Model jaringan, seperti protokol komunikasi, perangkat keras komputer, dan perangkat lunak aplikasi, terus berkembang setiap hari. Rangkaian protokol TCP/IP adalah contoh bagus dari sekumpulan besar protokol dan standar yang terus-menerus direvisi dan ditingkatkan. Standar Internet adalah spesifikasi teruji yang berguna dan dipatuhi oleh pengguna yang bekerja dengan Internet. Mari kita periksa jalur yang harus diikuti oleh sebuah proposal untuk menjadi standar Internet.

Semua standar Internet dimulai sebagai rancangan Internet, yang merupakan pekerjaan awal yang sedang berjalan. Satu atau lebih komite Internet internal mengerjakan sebuah draf, menyempurnakannya hingga mencapai bentuk yang dapat diterima. Ketika otoritas Internet merasa bahwa draf tersebut sudah siap untuk dipublikasikan, maka draf tersebut dipublikasikan sebagai Request for Comments (RFC), sebuah dokumen yang terbuka

untuk semua pihak yang berkepentingan. RFC diberi nomor, dan memasuki tahap pertama: standar yang diusulkan. Standar yang diusulkan adalah proposal yang stabil, menarik bagi komunitas Internet, dan cukup dipahami dengan baik. Spesifikasi tersebut diuji dan diterapkan oleh sejumlah kelompok berbeda, dan hasilnya dipublikasikan. Jika proposal lolos setidaknya dua implementasi yang independen dan dapat dioperasikan, standar yang diusulkan akan diangkat ke rancangan standar. Jika, setelah masukan dari pelaksanaan pengujian diperhitungkan, rancangan standar tidak mengalami masalah lebih lanjut, proposal tersebut akhirnya diangkat ke standar Internet.

Namun, jika standar yang diusulkan dianggap tidak sesuai pada suatu saat, maka standar tersebut akan menjadi RFC bersejarah dan disimpan dalam perspektif sejarah. (Standar internet yang diganti atau digantikan juga menjadi bersejarah.) RFC juga dapat dikategorikan sebagai eksperimental atau informasional. Dalam kasus ini, RFC yang dipermasalahkan mungkin tidak dimaksudkan sebagai standar Internet, namun dibuat untuk alasan eksperimental atau untuk memberikan informasi. Gambar 1-15 menunjukkan tingkat perkembangan RFC.



Gambar 1.15 Tingkat perkembangan saat RFC bergerak menuju standar

Dimungkinkan untuk memperoleh daftar cetak setiap RFC. Lihat halaman Web Internet Engineering Task Force di www.ietf.org/rfc.html untuk cara terbaik mengakses RFC. Internet dikelola oleh kerja beberapa komite. Komite paling atas adalah Internet Society (ISOC). ISOC adalah komite internasional nirlaba yang memberikan dukungan untuk seluruh proses pembuatan standar Internet. Terkait dengan ISOC adalah *Internet Architecture Board* (IAB), yang merupakan penasihat teknis ISOC. Di bawah IAB terdapat dua komite utama: *Internet Engineering Task Force* (IETF) dan *Internet Research Task Force* (IRTF). IETF mengelola kelompok kerja yang membuat dan mendukung fungsi-fungsi seperti protokol Internet,

keamanan, layanan pengguna, operasi, perutean, dan manajemen jaringan. IRTF mengelola kelompok kerja yang fokus pada tujuan jangka panjang Internet, seperti arsitektur, teknologi, aplikasi, dan protokol.

Komite Internet bukan satu-satunya kelompok yang membuat protokol atau menyetujui standar jaringan komputer, komunikasi data, dan telekomunikasi. Organisasi lain yang menciptakan dan menyetujui standar jaringan adalah Organisasi Internasional untuk Standardisasi (ISO), yang merupakan kelompok multinasional yang terdiri dari sukarelawan dari komite pembuat standar di berbagai pemerintahan di seluruh dunia. ISO terlibat dalam pengembangan standar di bidang teknologi informasi dan menciptakan model Open Systems Interconnection (OSI) untuk arsitektur jaringan. Organisasi pembuat standar lainnya meliputi:

- **American National Standards Institute (ANSI)**: Sebuah organisasi nirlaba swasta yang tidak terkait dengan pemerintah AS, ANSI berupaya mendukung perekonomian AS dan melindungi kepentingan publik dengan mendorong penerapan berbagai standar.
- **Persatuan Telekomunikasi Internasional-Sektor Standardisasi Telekomunikasi (ITU-T)**: Sebelumnya Komite Konsultatif Telegraf dan Telepon Internasional (CCITT), ITU-T dikhususkan untuk penelitian dan pembuatan standar telekomunikasi pada umumnya, dan sistem telepon dan data pada khususnya.
- **Institute of Electrical and Electronics Engineers (IEEE)**: Perkumpulan teknik profesional terbesar di dunia, IEEE berupaya untuk mempromosikan standardisasi bidang teknik elektro, elektronik, dan radio. Yang menarik adalah pekerjaan yang dilakukan IEEE pada standarisasi jaringan area lokal.
- **Electronic Industries Alliance (EIA)**: Sejajar dengan ANSI, EIA adalah organisasi nirlaba yang ditujukan untuk standardisasi produk elektronik. Yang menarik adalah pekerjaan yang dilakukan EIA dalam membakukan antarmuka antara komputer dan modem.

Lapisan sesi adalah lapisan lain yang tidak ada dalam rangkaian protokol TCP/IP dan bertanggung jawab untuk membangun sesi antar pengguna. Ini juga dapat mendukung manajemen token, sebuah layanan yang mengontrol komputer pengguna mana yang berbicara selama sesi saat ini dengan meneruskan token perangkat lunak bolak-balik.

Selain itu, lapisan sesi menetapkan titik sinkronisasi, yang merupakan titik cadangan yang digunakan jika terjadi kesalahan atau kegagalan. Misalnya, saat mentransmisikan dokumen besar seperti buku elektronik, lapisan sesi mungkin menyisipkan titik sinkronisasi di akhir setiap bab. Jika terjadi kesalahan selama transmisi, pengirim dan penerima dapat membuat cadangan ke titik sinkronisasi terakhir (ke awal bab yang dikirimkan sebelumnya) dan memulai transmisi ulang.

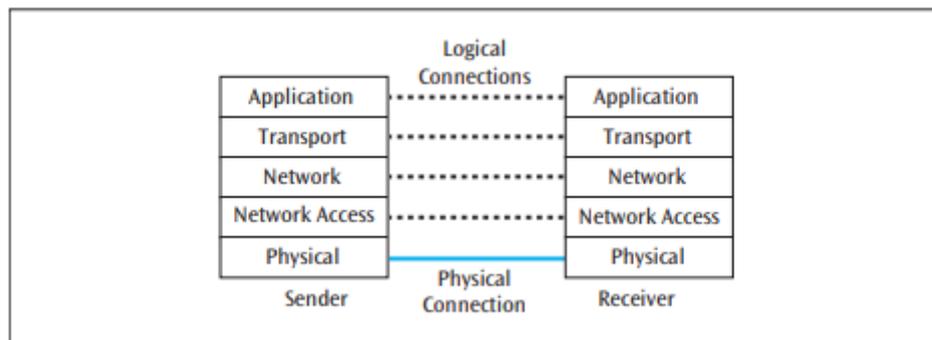
Banyak aplikasi jaringan tidak menyertakan lapisan sesi tertentu dan tidak menggunakan token untuk mengelola percakapan. Jika ya, "token" dimasukkan oleh lapisan aplikasi, atau mungkin lapisan transport, bukan lapisan sesi. Demikian pula, jika aplikasi jaringan menggunakan titik sinkronisasi, titik ini sering kali disisipkan oleh lapisan aplikasi.

Lapisan keempat dalam model OSI, lapisan transport, beroperasi dengan cara yang sama seperti lapisan transport pada rangkaian protokol TCP/IP. Hal ini memastikan bahwa paket data yang tiba di tujuan akhir sama dengan paket data yang meninggalkan stasiun asal.

Lapisan jaringan model OSI mirip dengan lapisan jaringan rangkaian protokol TCP/IP dan bertanggung jawab untuk mengirimkan paket data dari router ke router melalui jaringan. Lapisan data link, mirip dengan lapisan akses jaringan TCP/IP, bertanggung jawab untuk mengambil data dari lapisan jaringan dan mengubahnya menjadi sebuah bingkai. Lapisan paling bawah dalam model OSI lapisan fisik menangani transmisi bit melalui saluran komunikasi. Lapisan ini pada dasarnya identik dengan lapisan fisik rangkaian protokol TCP/IP.

Koneksi logis dan fisik

Konsep penting untuk dipaami sehubungan dengan lapisan model komunikasi adalah jalur komunikasi antara pengirim dan penerima. Perhatikan Gambar 1-16, yang menunjukkan pengirim dan penerima menggunakan aplikasi jaringan yang dirancang pada rangkaian protokol TCP/IP.



Gambar 1.16 Pengirim dan penerima berkomunikasi menggunakan rangkaian protokol TCP/IP

Perhatikan garis putus-putus antara lapisan aplikasi pengirim dan penerima, lapisan transport, lapisan jaringan, dan lapisan akses jaringan. Tidak ada data yang mengalir melalui garis putus-putus ini. Setiap garis putus-putus menunjukkan koneksi logis. Koneksi logis adalah koneksi nonfisik antara pengirim dan penerima yang memungkinkan pertukaran perintah dan tanggapan. Lapisan transport pengirim dan penerima, misalnya, berbagi serangkaian perintah yang digunakan untuk menjalankan fungsi tipe transport, namun informasi atau data sebenarnya harus diteruskan melalui lapisan fisik pengirim dan penerima, karena tidak ada koneksi langsung antara lapisan tersebut. dua lapisan transportasi. Tanpa koneksi logis, pengirim dan penerima tidak akan dapat mengoordinasikan fungsinya. Koneksi fisik adalah satu-satunya koneksi langsung antara pengirim dan penerima, dan berada pada lapisan fisik, di mana angka 1 dan 0 sebenarnya konten digital pesan ditransmisikan melalui kabel atau gelombang udara.

Sebagai contoh hubungan logis dan fisik, pertimbangkan skenario imajiner di mana dekan seni dan sains ingin menciptakan gelar gabungan baru dengan fakultas bisnis. Secara khusus, dekan ingin menciptakan gelar yang merupakan persilangan antara ilmu komputer dan pemasaran. Dekan bidang seni dan sains dapat memanggil dekan bisnis untuk membuat gelar tersebut, namun dekan belum tentu ahli dalam menyusun semua detail yang terkait dengan gelar baru. Sebaliknya, dekan seni dan sains memulai prosesnya dengan

mengeluarkan permohonan gelar baru dari dekan bisnis. Namun, sebelum permintaan ini sampai ke dekan bisnis, permintaan tersebut harus melewati beberapa lapisan. Pertama, permintaan ditujukan kepada ketua departemen ilmu komputer. Ketua akan memeriksa permintaan gelar baru dan menambahkan informasi yang diperlukan kepada staf program. Ketua kemudian akan mengirimkan permintaan tersebut ke komite kurikulum ilmu komputer, yang akan merancang beberapa mata kuliah baru. Komite kurikulum akan mengirimkan permintaan tersebut ke sekretaris departemennya, yang akan mengetik semua memo dan membuat paket yang mudah dibaca. Paket ini kemudian ditempatkan di surat antarkampus dan dikirim ke departemen pemasaran di sekolah bisnis.

Setelah permintaan sampai di bagian pemasaran, sekretaris di bagian pemasaran membuka amplop dan memberikan semua materi kepada panitia kurikulum pemasaran. Komite kurikulum pemasaran melihat mata kuliah yang diusulkan dari komite kurikulum ilmu komputer dan membuat beberapa perubahan dan penambahan. Setelah perubahan ini dilakukan, proposal diberikan kepada ketua departemen pemasaran, yang melihat kebutuhan staf yang disarankan oleh ketua ilmu komputer, memeriksa keakuratan permintaan, dan membuat beberapa perubahan. Ketua pemasaran kemudian menyerahkan permintaan tersebut kepada dekan bisnis, yang memeriksa seluruh dokumen dan memberikan persetujuan dengan beberapa perubahan kecil. Permintaan tersebut kemudian diteruskan kembali ke sekretaris departemen pemasaran, yang mengirimkannya kembali ke sekretaris ilmu komputer. Sekretaris ilmu komputer kemudian mengirimkan balasan permintaan tersebut secara berlapis hingga sampai ke dekan seni dan sains. Gambar 1.17 menunjukkan bagaimana permintaan gelar ini dapat naik dan turun melalui lapisan birokrasi universitas.



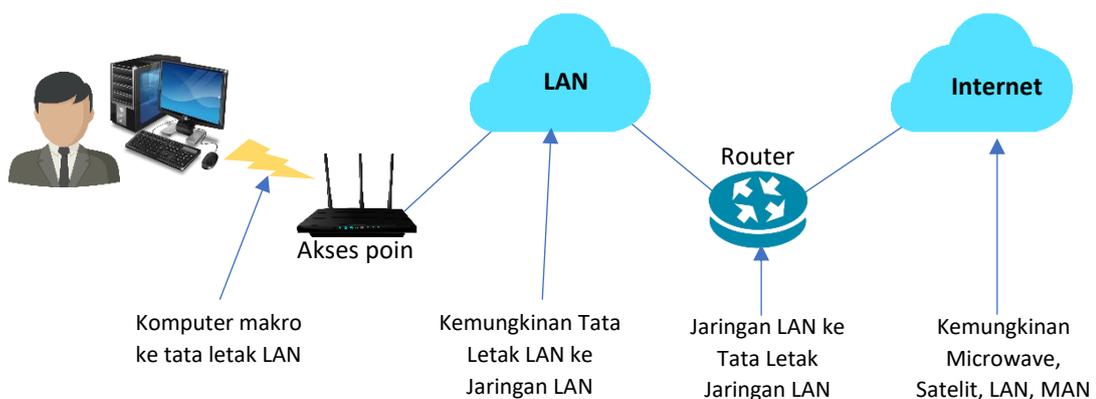
Gambar 1.17 Aliran data melalui lapisan birokrasi

Perlu dicatat bahwa data tidak mengalir langsung antar dekan; juga tidak mengalir langsung antara ketua departemen atau komite kurikulum. Sebaliknya, data harus mengalir sampai ke lapisan fisik (dalam hal ini, sekretaris) dan kemudian kembali ke sisi yang lain. Pada

setiap lapisan dalam proses, informasi yang mungkin berguna bagi lapisan “rekan” di sisi lain ditambahkan. Contoh ini sedikit memperluas kebenaran; kurikulum perguruan tinggi sebenarnya tidak dirancang seperti ini (prosesnya sebenarnya jauh lebih rumit). Oleh karena itu, kita akan melihat contoh yang lebih realistis di mana seseorang yang menggunakan browser Web meminta halaman Web dari suatu tempat di Internet. Namun sebelum kita memeriksa skenario yang lebih sulit ini, mari kita lihat contoh koneksi yang terjadi ketika pengguna menghubungkan laptopnya ke jaringan area lokal perusahaan.

1.7 TATA LETAK JARINGAN BERAKSI

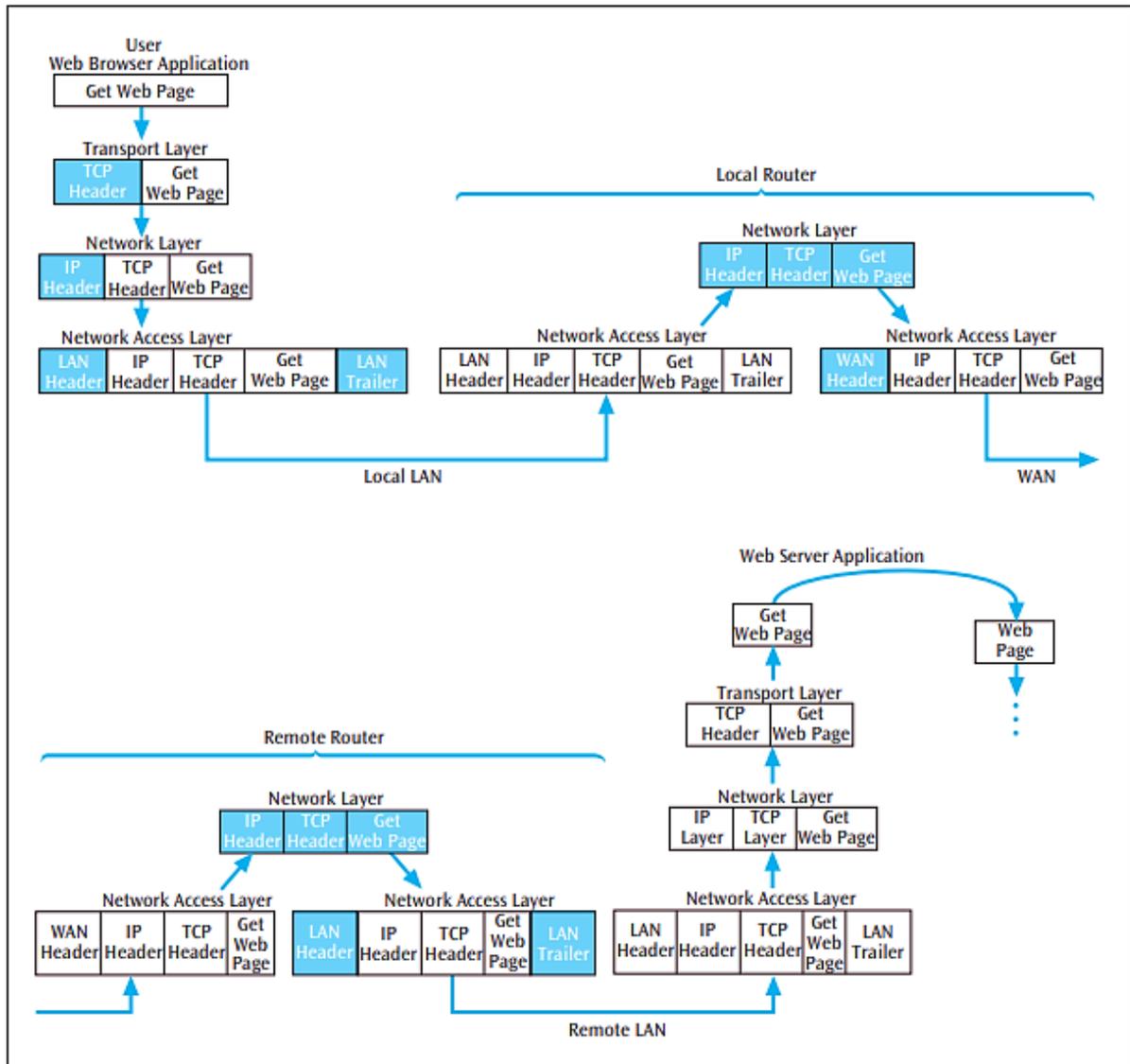
Mari kita pertimbangkan sebuah skenario di mana seorang karyawan sebuah perusahaan sedang duduk dengan komputer laptop di tempat kerja dan mengakses jaringan area lokal perusahaan melalui tata letak nirkabel (lihat Gambar 1.18). Karyawan tersebut menggunakan browser Web dan mencoba mengunduh halaman Web dari Internet. Tata letak jaringan manakah yang terlibat dalam skenario ini? Pertama, tata letak antara laptop nirkabel pengguna dan jaringan area lokal perusahaan adalah tata letak jaringan area mikro-ke-lokal. Setelah permintaan halaman Web berada di jaringan area lokal perusahaan, permintaan tersebut mungkin harus ditransfer melalui beberapa jaringan area lokal dalam sistem perusahaan. Tata letak antara jaringan area lokal ini akan menjadi tata letak jaringan area lokal ke jaringan area lokal. Untuk mengakses Internet, pengguna memerlukan tata letak jaringan area lokal ke jaringan area luas. Atau mungkin jaringan area lokal perusahaan terhubung ke jaringan area metropolitan, dalam hal ini pengguna memerlukan tata letak jaringan area lokal-ke-metropolitan untuk mengakses Internet. Setelah permintaan halaman Web karyawan ada di Internet, sulit untuk mengetahui tata letak apa yang terlibat. Mungkin ada interkoneksi jaringan area luas ke jaringan area luas, serta tata letak gelombang mikro atau satelit. Setelah permintaan halaman Web mendekati tujuan akhirnya, mungkin terdapat jaringan area metropolitan lain, atau beberapa tata letak jaringan area lokal. Perjalanan pulang mungkin mengambil jalur yang sama atau mungkin melibatkan jalur dan tata letak jaringan baru. Jelasnya, banyak tipe tata letak jaringan berbeda yang terlibat bahkan dalam aplikasi sehari-hari yang umum.



Gambar 1.18 Berbagai tata letak jaringan yang terlibat saat pengguna mengunduh halaman Web di tempat kerja

1.8 SUITE PROTOKOL TCP/IP BERAKSI

Contoh permintaan layanan yang lebih rinci dan menantang melalui lapisan model komunikasi akan membantu memperjelas konsep yang terlibat. Perhatikan Gambar 1.19, di mana pengguna menjelajahi Internet pada komputer pribadi meminta halaman Web untuk diunduh dan kemudian ditampilkan di layarnya.



Gambar 1.19 Jalur permintaan halaman Web yang mengalir dari browser ke server Web Internet dan sebaliknya

Dimulai dari sudut kiri atas gambar, proses dimulai ketika pengguna mengklik link pada halaman Web saat ini. Sebagai tanggapan, perangkat lunak browser (aplikasi) membuat perintah Dapatkan Halaman Web yang diberikan kepada lapisan transport browser, TCP. TCP menambahkan berbagai informasi header untuk digunakan oleh perangkat lunak TCP di pihak penerima. Ditambahkan ke bagian depan paket, informasi ini digunakan untuk mengontrol

transfer data. Informasi ini membantu pengendalian kesalahan end-to-end dan kontrol aliran end-to-end dan memberikan alamat aplikasi penerima (server Web).

Paket yang diperbesar sekarang dikirim ke lapisan jaringan, di mana IP menambahkan headernya. Informasi yang terkandung dalam header IP membantu perangkat lunak IP di sisi penerima, dan membantu perangkat lunak IP di setiap node perantara (router) selama kemajuan data melalui Internet. Bantuan ini termasuk memberikan alamat Internet stasiun kerja yang berisi halaman Web yang diminta.

Paket tersebut sekarang diberikan ke lapisan akses jaringan. Karena komputer pengguna terhubung ke jaringan area lokal, header jaringan area lokal yang sesuai ditambahkan. Perhatikan bahwa terkadang selain header, informasi kontrol ditambahkan ke akhir paket data sebagai trailer. Salah satu informasi terpenting yang disertakan dalam header jaringan area lokal adalah alamat perangkat (router) yang menghubungkan jaringan area lokal ke jaringan area luas (Internet).

Pada akhirnya, biner 1 dan 0 dari paket data ditransmisikan melalui jaringan area lokal pengguna melalui lapisan fisik, tempat mereka bertemu dengan router. Router adalah perangkat yang berfungsi sebagai pintu gerbang ke Internet. Router menghapus header dan trailer jaringan area lokal. Informasi dalam header IP diperiksa, dan router menentukan bahwa paket data harus keluar ke Internet. Informasi header WAN baru, yang diperlukan agar paket data melintasi jaringan area luas, diterapkan, dan biner 1 dan 0 dari paket data ditempatkan ke jaringan area luas.

Setelah paket data berpindah melalui Internet, paket tersebut akan tiba di router yang terhubung ke jaringan area lokal yang berisi server Web yang diinginkan. Router jarak jauh ini menghapus informasi jaringan area luas, melihat bahwa paket harus ditempatkan di jaringan area lokal, dan memasukkan informasi header dan trailer jaringan area lokal. Paket tersebut ditempatkan ke jaringan area lokal; dan menggunakan informasi alamat di header LAN, ia berpindah ke komputer yang menyimpan aplikasi server Web. Saat paket data bergerak ke atas lapisan komputer server Web, header LAN, IP, dan TCP akan dihapus. Aplikasi server Web menerima perintah Dapatkan Halaman Web, mengambil halaman Web yang diminta, dan membuat paket data baru dengan informasi yang diminta. Paket data baru ini sekarang berpindah ke lapisan bawah dan kembali melalui router ke jaringan pengguna dan stasiun kerja. Terakhir, halaman Web ditampilkan di monitor pengguna.

Menarik untuk dicatat bahwa ketika paket data mengalir melalui suatu model dan melewati setiap lapisan sistem, ukuran paket data bertambah. Pertumbuhan ini disebabkan oleh fakta bahwa setiap lapisan menambahkan lebih banyak informasi ke data asli. Beberapa dari informasi tambahan lapisan ini diperlukan oleh node dan router di jalur paket data, dan sebagian lagi diperlukan oleh tujuan akhir paket data. Informasi ini membantu dalam menyediakan layanan seperti deteksi kesalahan, pengendalian kesalahan, pengendalian aliran, dan pengalamatan jaringan. Penambahan informasi kontrol ke sebuah paket saat bergerak melalui lapisan disebut enkapsulasi. Perhatikan juga bahwa saat paket bergerak naik melalui lapisan, ukuran paket data menyusut. Setiap lapisan menghapus header yang

diperlukan untuk menjalankan tugas tugasnya. Setelah tugas pekerjaan selesai, informasi header dibuang dan paket yang lebih kecil diserahkan ke lapisan berikutnya yang lebih tinggi.

RINGKASAN

- Banyak layanan dan produk yang kita gunakan setiap hari menggunakan jaringan komputer dan komunikasi data dengan satu atau lain cara. Sistem telepon, sistem perbankan, televisi kabel, sistem audio dan video, sistem pengatur lalu lintas, dan telepon seluler adalah beberapa contohnya.
- Bidang komunikasi data dan jaringan komputer mencakup jaringan data, jaringan suara, jaringan nirkabel, jaringan area lokal, jaringan area metropolitan, jaringan area luas, dan jaringan area pribadi.
 - Area penerapan jaringan komputer dan komunikasi data dapat dipahami dalam tata letak jaringan secara umum:
 - Komputer terminal/mikrokomputer-ke-mainframe
 - Jaringan area mikrokomputer-ke-lokal
 - Komputer mikro-ke-Internet
 - Jaringan area lokal-ke-jaringan area lokal
 - Jaringan area pribadi-ke-workstation
 - Jaringan area lokal-ke-jaringan area metropolitan
 - Jaringan area lokal-ke-jaringan area luas
 - Jaringan area luas-ke-jaringan area luas
 - Jaringan area sensor-ke-lokal
 - Satelit dan gelombang mikro
 - Jaringan telepon seluler
 - Konsep utama dalam jaringan saat ini adalah konvergensi, fenomena di mana aplikasi jaringan dan teknologi yang mendukungnya menyatu menjadi satu teknologi yang mampu mendukung berbagai aplikasi. Secara khusus, kita dapat mendefinisikan tiga jenis konvergensi: konvergensi teknologi, konvergensi protokol, dan konvergensi industri.
 - Arsitektur jaringan, atau model komunikasi, menempatkan potongan-potongan jaringan dalam beberapa lapisan. Lapisan menentukan model untuk fungsi atau layanan yang perlu dilakukan. Setiap lapisan dalam model mendefinisikan layanan yang disediakan oleh perangkat keras, perangkat lunak, atau keduanya.
 - Untuk membakukan desain sistem komunikasi, ISO menciptakan model OSI. Model OSI didasarkan pada tujuh lapisan:
 - Lapisan aplikasi adalah lapisan teratas model OSI, tempat aplikasi yang menggunakan jaringan berada.
 - Lapisan presentasi melakukan serangkaian fungsi lain-lain yang diperlukan untuk menyajikan paket data dengan baik kepada pengirim atau penerima.
 - Lapisan sesi bertanggung jawab untuk membangun sesi antar pengguna.
 - Lapisan transport berkaitan dengan aliran data end-to-end yang bebas kesalahan.

- Lapisan jaringan bertanggung jawab untuk membuat, memelihara, dan mengakhiri koneksi jaringan.
- Lapisan data link bertanggung jawab untuk mengambil data mentah dan mengubahnya menjadi unit kohesif yang disebut frame.
- Lapisan fisik menangani transmisi bit melalui saluran komunikasi.
- Arsitektur jaringan lain (atau model komunikasi) yang disebut rangkaian protokol TCP/IP telah melampaui popularitas model OSI. Rangkaian protokol TCP/IP juga dikenal sebagai model Internet dan terdiri dari lima lapisan:
 - Lapisan aplikasi berisi aplikasi jaringan yang menggunakan jaringan dan layanan presentasi yang mendukung aplikasi tersebut.
 - Lapisan transport memelihara koneksi end-to-end yang bebas kesalahan.
 - Lapisan jaringan, atau lapisan Internet, menggunakan IP untuk mentransfer data antar jaringan.
 - Lapisan akses jaringan mendefinisikan media fisik yang mentransmisikan sinyal dan frame yang menggabungkan kontrol aliran dan kesalahan.
 - Lapisan fisik menangani transmisi bit melalui saluran komunikasi.
- Koneksi logis adalah aliran ide yang terjadi, tanpa koneksi fisik langsung, antara pengirim dan penerima pada lapisan tertentu.

PERTANYAAN TINJAUAN

1. Apa definisi dari:
 - a. jaringan komputer?
 - b. komunikasi data?
 - c. telekomunikasi?
 - d. jaringan area lokal?
 - e. jaringan area pribadi?
 - f. jaringan wilayah metropolitan?
 - g. jaringan area luas?
 - h. manajemen jaringan?
 - i. konvergensi?
2. Apa hubungan antara subjaringan dan node?
3. Jenis aplikasi apa yang mungkin menggunakan tata letak komputer terminal-ke-mainframe?
4. Jenis aplikasi apa yang mungkin menggunakan tata letak komputer mikro-ke-mainframe?
5. "Bahasa" apa yang harus digunakan oleh komputer mikro agar dapat berinteraksi dengan Internet?
6. Jenis aplikasi apa yang mungkin menggunakan tata letak jaringan area sensor-ke-lokal?
7. Mengapa arsitektur jaringan berguna?
8. Sebutkan tujuh lapisan model OSI.
9. Sebutkan lima lapisan rangkaian protokol TCP/IP.
10. Bagaimana lapisan model OSI dibandingkan dengan lapisan rangkaian protokol TCP/IP?

11. Aplikasi apa saja yang umum ditemukan pada rangkaian protokol TCP/IP?
12. Apa perbedaan antara koneksi logis dan koneksi fisik?
13. Bagaimana konvergensi diterapkan pada industri komunikasi?

Latihan Tambahan

1. Buat daftar semua tindakan yang Anda lakukan rata-rata sehari-hari yang menggunakan komunikasi data dan jaringan komputer.
2. Jika Anda dapat mendesain rumah Anda sendiri, jenis jaringan komputer atau perangkat komunikasi data hemat tenaga kerja apa yang akan Anda gunakan?
3. Dua perusahaan sedang mempertimbangkan untuk menggabungkan sumber daya mereka untuk membentuk usaha patungan. CEO perusahaan pertama bertemu dengan tim hukumnya, dan tim hukum berkonsultasi dengan sejumlah manajer menengah di bidang produk yang diusulkan. Sementara itu, CEO perusahaan pertama mengirimkan email ke CEO perusahaan kedua untuk memberikan beberapa saran mengenai usaha patungan tersebut. Apakah skenario ini mengikuti model OSI? Jelaskan jawabanmu.
4. Menggunakan komputer laptop dengan koneksi nirkabel ke jaringan area lokal perusahaan, Anda mendownload halaman Web dari Internet. Buat daftar semua tata letak jaringan berbeda yang terlibat dalam operasi ini.
5. Anda bekerja dari rumah menggunakan mikrokomputer, modem DSL, dan sambungan telepon ke Internet. Perusahaan Anda terhubung ke Internet dan memiliki jaringan area lokal dan komputer mainframe. Buat daftar semua tata letak jaringan berbeda yang terlibat dalam operasi ini.
6. Anda sedang duduk di kedai kopi lokal, menikmati latte favorit Anda. Anda mengeluarkan laptop Anda dan, menggunakan jaringan nirkabel yang tersedia di kedai kopi, mengakses email Anda. Buat daftar semua tata letak jaringan berbeda yang terlibat dalam operasi ini.
7. Dengan ponsel baru Anda, Anda baru saja mengambil foto sahabat Anda. Anda memutuskan untuk mengirimkan cuplikan ini ke akun email teman bersama di seluruh negeri. Buat daftar semua tata letak jaringan berbeda yang terlibat dalam operasi ini.
8. Anda sedang mengemudi di kota baru dan baru saja tersesat. Dengan menggunakan sistem navigasi bawaan mobil Anda, Anda mengirimkan permintaan petunjuk arah mengemudi dari persimpangan terdekat ke tujuan Anda. Daftar semuanya tata letak jaringan berbeda yang terlibat dalam operasi ini.
9. Lapisan rangkaian protokol TCP/IP dan model OSI berbeda. Lapisan manakah yang “hilang” dari rangkaian protokol TCP/IP? Apakah mereka benar-benar hilang?
10. Jika lapisan data link menyediakan pemeriksaan kesalahan dan lapisan transport menyediakan pemeriksaan kesalahan, bukankah ini mubazir? Jelaskan jawabanmu.
11. Demikian pula, lapisan data link menyediakan kontrol aliran, dan lapisan transport menyediakan kontrol aliran. Apakah ini bentuk kontrol aliran yang berbeda? Jelaskan jawabanmu.

12. Anda sedang menonton acara televisi di mana salah satu karakter menggugat karakter lainnya. Pengacara kedua belah pihak bertemu dan mencoba mencari penyelesaian. Apakah ada hubungan logis atau fisik antara para pengacara? Bagaimana dengan kedua pihak?
13. Anda ingin mendownload file dari situs jarak jauh menggunakan FTP. Untuk melakukan transfer file, komputer Anda mengeluarkan perintah Dapatkan File. Tampilkan perkembangan pesan saat perintah Dapatkan File berpindah dari komputer Anda, melalui router, ke komputer jarak jauh, dan sebaliknya.
14. Karakteristik apa yang membedakan jaringan area pribadi dari jenis jaringan lainnya?
15. Bukankah jaringan area metropolitan hanyalah jaringan area lokal yang besar? Jelaskan jawabanmu.
16. Daftarkan lapisan OSI yang menjalankan masing-masing fungsi berikut:
 - a. kompresi data
 - b. multipleks
 - c. rute
 - d. definisi karakteristik listrik suatu sinyal
 - e. surel
 - f. deteksi kesalahan
 - g. kontrol aliran ujung ke ujung
17. Untuk setiap fungsi pada latihan sebelumnya, daftarkan lapisan rangkaian protokol TCP/IP yang menjalankan fungsi tersebut.
18. Anda mengirim dan menerima pesan teks (instan) (IM) dengan seorang teman. Apakah sesi IM ini merupakan koneksi logis atau koneksi fisik? Jelaskan jawabanmu.

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Anda diminta membuat model arsitektur jaringan baru. Apakah akan berlapis-lapis, atau akankah komponen-komponennya berbentuk lain? Tunjukkan lapisan model Anda atau bentuk barunya, dan jelaskan fungsi yang dilakukan oleh masing-masing komponennya.
2. Ambil contoh dari tempat kerja atau sekolah Anda di mana seseorang meminta suatu layanan dan kemudian buat diagram permintaan tersebut. Apakah permintaan melewati lapisan apa pun sebelum mencapai penerima yang dituju? Apakah ada koneksi logis dan koneksi fisik? Jika ya, tunjukkan pada diagram.
3. Bab ini mencantumkan beberapa jenis tata letak jaringan. Apakah ada tata letak lain di dunia nyata yang tidak tercantum dalam bab ini? Jika ya, apakah itu?
4. Jelaskan situasi kehidupan nyata yang menggunakan setidaknya lima tata letak jaringan yang dijelaskan dalam bab ini.

SOAL TAMBAHAN

1. Ingat kembali pekerjaan yang pernah Anda miliki (atau masih Anda miliki). Apakah ada rantai komando untuk menyelesaikan tugas? Jika ya, gambarkan rantai komando

tersebut di atas kertas atau gunakan program perangkat lunak. Bagaimana rantai komando ini dibandingkan dengan model OSI atau rangkaian protokol TCP/IP?

2. Karena rangkaian protokol TCP/IP tidak dibuat-buat, buku lain mungkin membahas lapisan yang sedikit berbeda. Temukan dua contoh rangkaian protokol TCP/IP lainnya yang berbeda dari lapisan dalam buku ini dan kutip sumbernya. Apa persamaan kedua suite tersebut, dan apa perbedaannya? Bagaimana perbandingannya dengan rangkaian protokol TCP/IP yang dibahas dalam bab ini? Tulis laporan singkat dan ringkas yang merangkum temuan Anda.
3. Apa bentuk yang lebih tepat dari perintah Dapatkan Halaman Web yang ditunjukkan pada Gambar 1.19? Tunjukkan bentuk komandonya, dan uraikan tanggung jawab masing-masing bidang.
4. Jenis aplikasi jaringan apa yang ada di tempat kerja atau kampus Anda? Apakah jaringan area lokal terlibat? Jaringan area luas? Buat daftar berbagai tata letak jaringan. Gambarlah diagram atau peta aplikasi ini dan tata letaknya.
5. Model jaringan apa lagi yang ada atau pernah ada selain model OSI dan rangkaian protokol TCP/IP? Teliti topik ini dan tulis deskripsi singkat tentang setiap model jaringan yang Anda temukan.
6. Apa nama beberapa protokol routing yang saat ini digunakan di Internet? Tulis satu atau dua kalimat untuk menjelaskan setiap protokol.

BAB 2

DASAR-DASAR DATA DAN SINYAL

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Membedakan antara data dan sinyal, dan menyebutkan keunggulan data dan sinyal digital dibandingkan data dan sinyal analog
- Identifikasi tiga komponen dasar sinyal
- Diskusikan bandwidth suatu sinyal dan kaitannya dengan kecepatan transfer data
- Identifikasi kekuatan dan redaman sinyal, serta keterkaitannya
- Menguraikan ciri-ciri dasar transmisi data analog dengan sinyal analog, data digital dengan sinyal digital, data digital dengan sinyal analog diskrit, dan data analog dengan sinyal digital
- Buat daftar dan gambar diagram teknik dasar pengkodean digital, dan jelaskan kelebihan dan kekurangan masing-masing teknik
- Identifikasi berbagai teknik shift keying (modulasi), dan jelaskan kelebihan, kekurangan, dan kegunaannya
- Identifikasi dua teknik digitalisasi yang paling umum, dan jelaskan kelebihan dan kekurangannya
- Identifikasi berbagai kode data dan cara penggunaannya dalam sistem komunikasi

Sinyal digital, kami diberitahu, akan memberikan gambaran yang jauh lebih baik. Mulai tahun 1998, beberapa stasiun televisi di Amerika Serikat mulai menyiarkan gambar dan suara digital dalam skala terbatas. Menurut Komisi Komunikasi Federal (FCC), lebih dari 1000 stasiun menyiarkan sinyal televisi digital pada Mei 2003. FCC mengumumkan bahwa ketika setidaknya 85 persen rumah di suatu wilayah mampu menerima sinyal televisi digital, maka mereka akan menerima sinyal televisi digital. menghentikan penyediaan siaran televisi analog di wilayah tersebut. Tanggal rencana pertama ditetapkan pada 18 Februari 2009. Namun karena pemerintah kewalahan dengan permintaan kotak konverter digital, FCC membatalkan tanggal tersebut dan menetapkan tanggal baru yaitu 12 Juni 2009. Tanggal tersebut tiba dan tidak terlalu banyak. Yang mengejutkan, ribuan pemirsa menjadi lengah dan tidak dapat lagi menerima sinyal televisi menggunakan peralatan analog yang lebih tua. Banyak orang mengantri panjang berharap mendapatkan kotak konverter atau setidaknya kupon untuk kemudian menerima kotak konverter. Era digital televisi telah resmi dimulai. Saya rasa sebagian besar orang pasti setuju bahwa menonton televisi dengan antena model lama sudah pasti mengalami kemajuan. Jika dulu terdapat gambar kabur dengan banyak hantu, kini kita melihat gambar sebening kristal, sering kali dalam definisi tinggi.

Meskipun demikian, jika menyangkut sinyal analog versus sinyal digital, masih banyak pertanyaan yang tersisa:

Mengapa sinyal digital jauh lebih baik daripada sinyal analog?

Aplikasi apa lagi yang telah dialihkan dari analog ke digital?

Apakah masih ada aplikasi yang suatu hari nanti dapat diubah menjadi digital?

2.1 PENDAHULUAN

Ketika rata-rata pengguna komputer diminta untuk membuat daftar elemen jaringan komputer, sebagian besar mungkin akan menyebutkan komputer, kabel, disk drive, modem, dan komponen fisik lain yang mudah diidentifikasi. Banyak yang bahkan mungkin melihat lebih jauh dari sekedar fisiknya dan mengutip contoh perangkat lunak, seperti program aplikasi dan protokol jaringan. Bab ini terutama akan membahas dua hal yang bahkan lebih sulit dilihat secara fisik: data dan sinyal.

Data dan sinyal adalah dua blok bangunan dasar dari setiap jaringan komputer. Penting untuk dipahami bahwa istilah “data” dan “sinyal” tidak memiliki arti yang sama; dan agar jaringan komputer dapat mengirimkan data, data tersebut harus diubah terlebih dahulu menjadi sinyal yang sesuai. Satu hal yang sama antara data dan sinyal adalah keduanya bisa dalam bentuk analog atau digital, sehingga memberi kita empat kemungkinan kombinasi konversi data ke sinyal:

- Sinyal data-ke-analog analog, yang melibatkan teknik modulasi amplitudo dan frekuensi
- Sinyal data-ke-digital digital, yang melibatkan teknik pengkodean
- Sinyal analog data-ke-(diskrit), yang melibatkan teknik modulasi
- Sinyal analog data-ke-digital, yang melibatkan teknik digitalisasi

Masing-masing dari keempat kombinasi ini cukup sering terjadi dalam jaringan komputer, dan masing-masing memiliki aplikasi dan properti unik, seperti yang ditunjukkan pada Tabel 2-1.

Tabel 2.1 Empat kombinasi data dan sinyal

Data	Sinyal	Teknik Pengkodean atau Konversi	Perangkat Umum	Sistem Umum
Analog	Analog	Modulasi amplitudo Modulasi frekuensi	Penyetel radio penyetel TV	Telepon Radio AM dan FM Siaran TV Kabel TV
Digital	Digital	NRZ-L NRZI Manchester Diferensial Manchester Bipolar-AMI 4B/5B	Pembuat encode digital	Jaringan area lokal Sistem telepon
Digital	(Diskrit) Analog	Penguncian pergeseran amplitudo Penguncian pergeseran frekuensi	Modem	Akses Internet dial- up DSL Modem kabel TV Siaran Digital

		Penguncian pergeseran fase		
Analog	Digital	Modulasi kode pulsa Modulasi delta	Kodek	Sistem telepon Sistem musik

Mengubah data analog menjadi sinyal analog cukup umum. Konversi dilakukan dengan teknik modulasi dan ditemukan dalam sistem seperti telepon, radio AM, dan radio FM. Nanti di bab ini, kita akan membahas bagaimana sinyal radio AM tercipta. Mengubah data digital menjadi sinyal digital relatif mudah dan melibatkan banyak teknik pengkodean digital. Dengan teknik ini, biner 1 dan 0 diubah menjadi berbagai jenis level tegangan hidup dan mati. Jaringan area lokal adalah salah satu contoh paling umum dari sistem yang menggunakan jenis konversi ini. Kita akan memeriksa beberapa teknik pengkodean representatif dan mendiskusikan kelebihan dan kekurangan dasarnya. Mengubah data digital menjadi sinyal analog (diskrit) memerlukan beberapa bentuk modem. Sekali lagi kita mengubah biner 1 dan 0 ke bentuk lain; namun tidak seperti konversi data digital menjadi sinyal digital, konversi data digital menjadi sinyal analog diskrit melibatkan bentuk sinyal analog yang lebih kompleks yang memiliki jumlah level yang diskrit atau tetap.

Terakhir, konversi data analog menjadi sinyal digital umumnya disebut digitalisasi. Sistem telepon dan sistem musik adalah dua contoh umum digitalisasi. Ketika sinyal suara Anda menyebar dari rumah Anda dan mencapai pusat peralihan perusahaan telepon, sinyal tersebut akan didigitalkan. Demikian pula, musik dan video didigitalkan sebelum dapat direkam pada CD atau DVD. Dalam bab ini, dua teknik dasar digitalisasi akan diperkenalkan dan kelebihan serta kekurangannya akan ditampilkan. Dalam semua contoh bab ini, data diubah menjadi sinyal oleh komputer atau perangkat terkait komputer, kemudian dikirimkan melalui media komunikasi ke komputer lain atau perangkat terkait komputer, yang mengubah sinyal kembali menjadi data. Perangkat asal adalah pemancar, dan perangkat tujuan adalah penerima.

Sebuah pertanyaan besar muncul selama studi data dan sinyal: Mengapa orang yang tertarik pada aspek bisnis jaringan komputer harus memperhatikan tingkat detail ini? Salah satu jawaban atas pertanyaan tersebut adalah bahwa pemahaman yang kuat tentang dasar-dasar sistem komunikasi akan memberikan landasan yang kuat untuk studi lebih lanjut tentang topik jaringan komputer yang lebih maju. Selain itu, bab ini akan memperkenalkan banyak istilah yang digunakan oleh personel jaringan. Untuk dapat memahami individu-individu ini dan berinteraksi secara mendalam dengan mereka, kita harus meluangkan sedikit waktu untuk membahas dasar-dasar sistem komunikasi. Bayangkan Anda sedang merancang sistem inventaris online baru dan Anda ingin mengizinkan berbagai pengguna di dalam perusahaan untuk mengakses sistem ini. Teknisi jaringan memberi tahu Anda bahwa hal ini tidak dapat dilakukan karena mengunduh satu catatan inventaris dalam jangka waktu yang wajar (X detik) akan memerlukan koneksi setidaknya Y juta bit per detik yang tidak mungkin dilakukan, mengingat struktur jaringan saat ini. Bagaimana Anda tahu teknisi jaringan itu benar? Apakah Anda benar-benar ingin mempercayai semua yang dia katakan? Studi tentang

data dan sinyal juga akan menjelaskan mengapa hampir semua bentuk komunikasi, seperti data, suara, musik, dan video, perlahan-lahan diubah dari bentuk analog aslinya ke bentuk digital yang lebih baru. Apa hebatnya bentuk komunikasi digital ini, dan seperti apa sinyal yang mewakili bentuk komunikasi ini? Kami akan menjawab pertanyaan-pertanyaan ini dan lebih banyak lagi di bab ini.

2.2 DATA DAN SINYAL

Informasi yang disimpan dalam sistem komputer dan ditransfer melalui jaringan komputer dapat dibagi menjadi dua kategori: data dan sinyal. Data adalah entitas yang menyampaikan makna dalam komputer atau sistem komputer. Contoh umum data meliputi:

- File komputer berisi nama dan alamat yang disimpan di hard disk drive
- Bit atau elemen individual film yang disimpan dalam DVD
- Biner 1 dan 0 musik yang disimpan di CD atau di dalam iPod
- Titik-titik (piksel) dari sebuah foto yang telah didigitalkan oleh kamera digital dan disimpan dalam memory stick
- Angka 0 sampai 9, yang mungkin mewakili angka penjualan suatu bisnis

Dalam masing-masing contoh ini, beberapa jenis informasi telah ditangkap secara elektronik dan disimpan pada beberapa jenis perangkat penyimpanan.

Jika Anda ingin mentransfer data ini dari satu titik ke titik lain, baik melalui kabel fisik atau melalui gelombang radio, data tersebut harus diubah menjadi sinyal. Sinyal adalah impuls listrik atau elektromagnetik yang digunakan untuk menyandikan dan mengirimkan data. Contoh umum sinyal meliputi:

- Transmisi percakapan telepon melalui saluran telepon
- Wawancara berita televisi langsung dari Eropa yang disiarkan melalui sistem satelit
- Transmisi makalah melalui kabel printer antara komputer dan printer
- Pengunduhan halaman Web saat ditransfer melalui saluran telepon antara penyedia layanan Internet dan komputer di rumah Anda

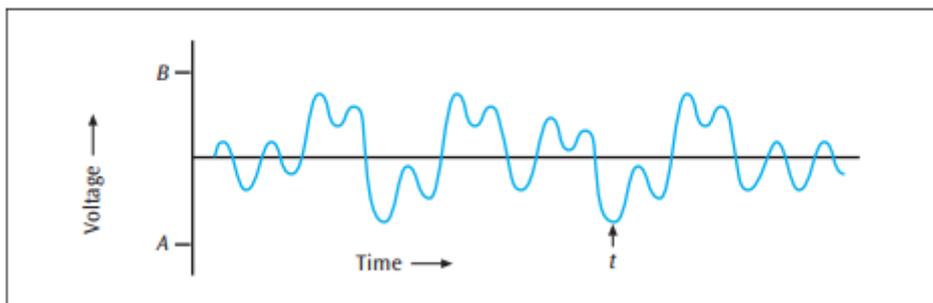
Dalam masing-masing contoh ini, data, entitas statis atau benda berwujud, ditransmisikan melalui kabel atau gelombang udara dalam bentuk sinyal yang merupakan entitas dinamis atau benda tak berwujud. Beberapa jenis perangkat keras diperlukan untuk mengubah data statis menjadi sinyal dinamis yang siap dikirim dan kemudian mengubah sinyal kembali menjadi data di tujuan penerima.

Namun, sebelum memeriksa karakteristik dasar data dan sinyal serta konversi dari data menjadi sinyal, mari kita jelajahi karakteristik paling penting yang dimiliki oleh data dan sinyal.

Analog vs digital

Meskipun data dan sinyal adalah dua entitas berbeda yang memiliki sedikit kesamaan, satu karakteristik yang sama-sama dimiliki oleh keduanya adalah bahwa keduanya dapat hadir dalam bentuk analog atau digital. Data analog dan sinyal analog direpresentasikan sebagai bentuk gelombang kontinu yang dapat berada pada titik tak terhingga antara titik minimum dan maksimum tertentu. Berdasarkan konvensi, nilai minimum dan maksimum ini disajikan

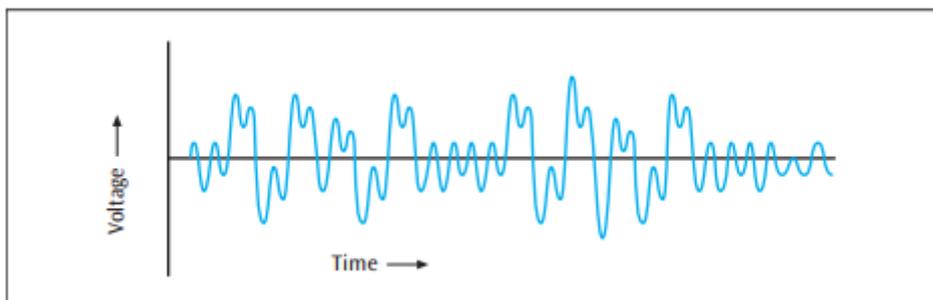
sebagai tegangan. Gambar 2.1 menunjukkan bahwa antara nilai minimum A dan nilai maksimum B, bentuk gelombang pada waktu t dapat berada pada jumlah tempat yang tak terhingga. Contoh paling umum dari data analog adalah suara manusia. Misalnya, ketika seseorang berbicara melalui telepon, penerima di corong mengubah gelombang ucapan menjadi gelombang analog tegangan listrik. Musik dan video, ketika muncul dalam keadaan aslinya, juga merupakan data analog. Meskipun suara manusia berfungsi sebagai contoh data analog, contoh sinyal analog adalah transmisi percakapan suara secara elektronik pada sistem telepon. Dengan demikian, kita melihat bahwa data dan sinyal analog cukup umum, dan banyak sistem telah menggabungkannya selama bertahun-tahun.



Gambar 2.1 Contoh sederhana bentuk gelombang analog

Salah satu kelemahan utama data analog dan sinyal analog adalah sulitnya memisahkan noise dari bentuk gelombang aslinya. Kebisingan adalah energi listrik atau elektromagnetik yang tidak diinginkan yang menurunkan kualitas sinyal dan data. Karena kebisingan ditemukan di setiap jenis data dan sistem transmisi, dan karena dampaknya berkisar dari sedikit desisan di latar belakang hingga hilangnya data atau sinyal sepenuhnya, maka sangat penting untuk mengurangi kebisingan sebanyak mungkin. Sayangnya, noise itu sendiri muncul sebagai bentuk gelombang analog; dan hal ini menyulitkan, bahkan sangat sulit, untuk memisahkan kebisingan dari bentuk gelombang analog yang mewakili data.

Perhatikan bentuk gelombang pada Gambar 2.2, yang menunjukkan beberapa nada pertama dari pembukaan simfoni imajiner. Kebisingan bercampur dengan musik data. Bisakah Anda mengetahui dengan melihat gambar apa itu data dan apa itu noise? Meskipun contoh ini mungkin mendekati ekstrem, contoh ini menunjukkan bahwa noise dan data analog bisa tampak serupa.



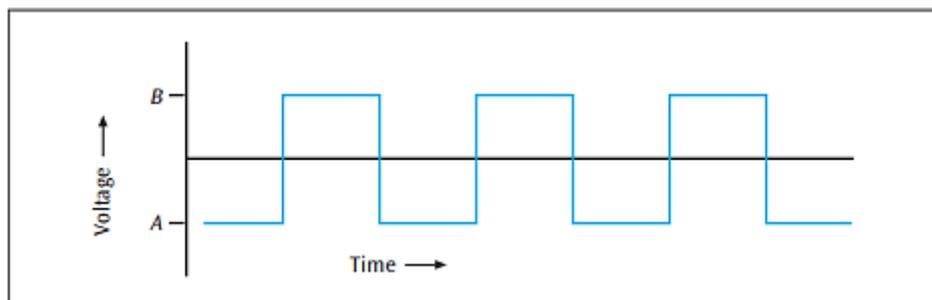
Gambar 2.2 Bentuk gelombang pembukaan simfoni dengan noise

Kinerja pemutar rekaman memberikan contoh lain tentang kebisingan yang mengganggu data. Banyak orang memiliki koleksi album yang menghasilkan bunyi pop, desis, dan klik saat diputar; album terkadang bahkan dilewati. Apakah mungkin untuk membuat perangkat yang menyaring letupan, desisan, dan klik dari album rekaman tanpa merusak data asli, musiknya? Berbagai perangkat diciptakan pada tahun 1960an dan 1970an untuk melakukan penyaringan semacam ini, namun hanya perangkat yang menghilangkan desisan yang (secara relatif) berhasil. Perangkat pemfilteran yang menghilangkan letupan dan klik juga cenderung menghilangkan bagian-bagian musik. Filter sekarang ada yang cukup efektif menghilangkan sebagian besar bentuk kebisingan dari rekaman analog; tapi menariknya, ini adalah perangkat digital bukan analog. Yang lebih menarik lagi, beberapa orang mengunduh perangkat lunak dari Internet yang memungkinkan mereka memasukkan klik dan pop ke dalam musik digital agar terdengar kuno (dengan kata lain, seolah-olah diputar dari album rekaman).

Contoh lain dari kebisingan yang mengganggu sinyal analog adalah desisan dan suara statis yang Anda dengar saat Anda berbicara di telepon. Seringkali kebisingan latar belakang sangat kecil sehingga kebanyakan orang tidak menyadarinya. Namun, kadang-kadang, kebisingannya meningkat sedemikian rupa sehingga mengganggu percakapan. Contoh umum lainnya dari gangguan kebisingan terjadi ketika Anda mendengarkan stasiun radio AM saat terjadi badai listrik. Sinyal radio berbunyi setiap kali sambaran petir di area tersebut.

Data digital dan sinyal digital terdiri dari sejumlah nilai yang terpisah atau tetap, bukan sejumlah nilai yang kontinu atau tidak terbatas. Seperti yang telah kami sebutkan, data digital berbentuk biner 1 dan 0. Namun sinyal digital lebih kompleks. Agar pembahasannya sesederhana mungkin, kami akan memperkenalkan dua bentuk sinyal digital. Jenis sinyal digital yang pertama cukup jelas dan berbentuk apa yang disebut “gelombang persegi”. Gelombang persegi ini adalah pola tegangan tinggi dan rendah yang relatif sederhana.

Dalam contoh yang ditunjukkan pada Gambar 2.3, gelombang persegi digital hanya mengambil dua nilai diskrit: tegangan tinggi (misalnya 5 volt) dan tegangan rendah (misalnya 0 volt).

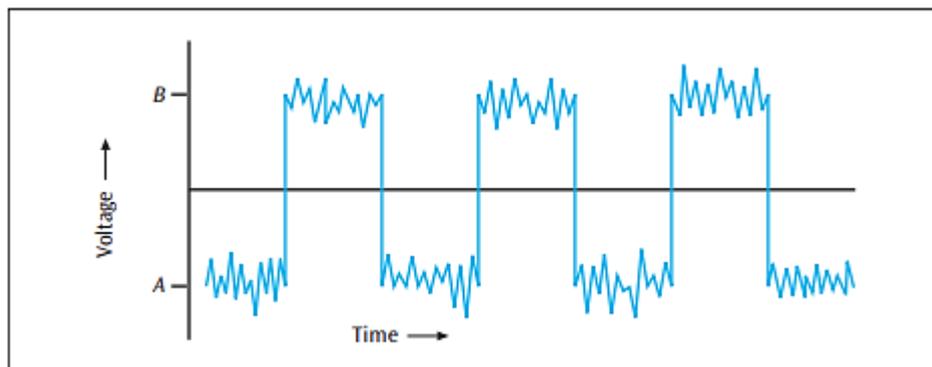


Gambar 2.3 Contoh sederhana bentuk gelombang digital

Bentuk kedua dari sinyal digital, seperti yang akan kita lihat sebentar lagi, melibatkan kombinasi sinyal analog termodulasi yang lebih kompleks. Meskipun sinyal yang dihasilkan

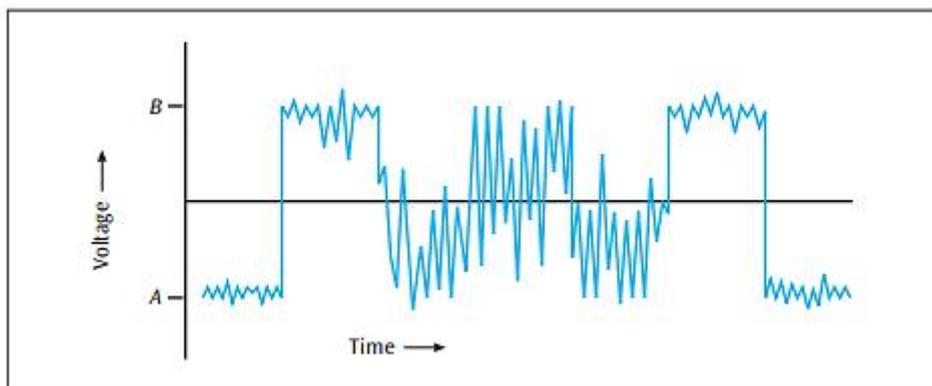
merupakan komposisi sinyal analog, kami memperlakukan produk akhir sebagai sinyal digital karena terdapat sejumlah kombinasi dan level sinyal yang berbeda.

Meskipun hal ini mungkin sulit untuk divisualisasikan pada saat ini, bertahanlah; kita akan membahasnya kembali dengan banyak contoh. Apa yang terjadi jika Anda memasukkan noise ke dalam sinyal digital? Seperti dinyatakan sebelumnya, kebisingan memiliki sifat bentuk gelombang analog dan, dengan demikian, dapat menempati rentang nilai yang tak terhingga; bentuk gelombang digital hanya menempati rentang nilai yang terbatas. Saat Anda menggabungkan derau analog dengan bentuk gelombang digital, cukup mudah untuk memisahkan bentuk gelombang digital asli dari derau. Gambar 2.4 menunjukkan sinyal digital (gelombang persegi) dengan beberapa noise.



Gambar 2.4 Sinyal digital dengan beberapa noise yang muncul

Jika jumlah noise tetap cukup kecil sehingga bentuk gelombang digital aslinya masih dapat diinterpretasikan, maka noise tersebut dapat disaring, sehingga meninggalkan bentuk gelombang aslinya. Dalam contoh sederhana pada Gambar 2.4, selama Anda dapat membedakan bentuk gelombang tinggi dan rendah, Anda masih dapat mengenali bentuk gelombang digital.



Gambar 2.5 Bentuk gelombang digital dengan noise yang sangat besar sehingga Anda tidak dapat lagi mengenali bentuk gelombang aslinya

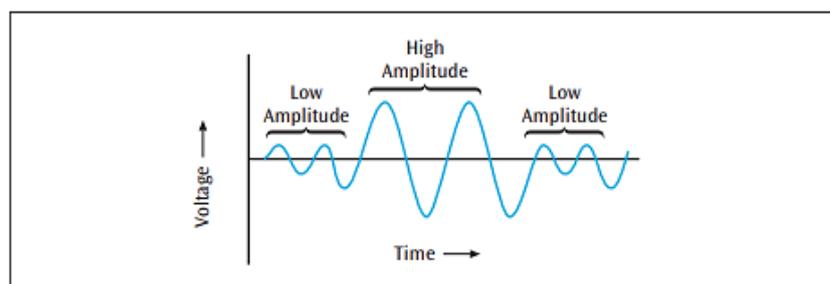
Namun, jika noise menjadi sangat besar sehingga tidak mungkin lagi membedakan nada tinggi dan rendah, seperti yang ditunjukkan pada Gambar 2.5, maka noise telah mengambil alih sinyal dan Anda tidak dapat lagi memahami bagian bentuk gelombang ini. Kemampuan untuk memisahkan kebisingan dari bentuk gelombang digital adalah salah satu kekuatan sistem digital. Ketika data ditransmisikan sebagai sinyal, sinyal tersebut akan selalu menimbulkan tingkat kebisingan tertentu. Namun dalam kasus sinyal digital, relatif mudah untuk melewati sinyal digital yang berisik melalui perangkat penyaringan yang menghilangkan sejumlah besar kebisingan dan membiarkan sinyal digital asli tetap utuh.

Terlepas dari keunggulan digital dibandingkan analog, tidak semua sistem menggunakan sinyal digital untuk mengirimkan data. Alasannya adalah peralatan elektronik yang digunakan untuk mengirimkan sinyal melalui kabel atau gelombang udara biasanya menentukan jenis sinyal yang dapat dikirimkan oleh kabel tersebut. Peralatan elektronik tertentu hanya mampu mendukung sinyal analog, sedangkan peralatan lainnya hanya mampu mendukung sinyal digital. Ambil contoh, jaringan area lokal dalam bisnis atau rumah Anda. Kebanyakan dari mereka selalu mendukung sinyal digital terutama karena jaringan area lokal dirancang untuk mentransmisikan data komputer, yang bersifat digital. Dengan demikian, peralatan elektronik yang mendukung transmisi sinyal jaringan area lokal juga bersifat digital.

Sekarang kita telah mempelajari karakteristik utama yang dimiliki oleh data dan sinyal (bahwa keduanya dapat berada dalam bentuk analog atau digital), serta fitur utama yang membedakan analog dari digital (yang pertama ada sebagai bentuk gelombang kontinu, sedangkan yang terakhir adalah diskrit), mari kita periksa karakteristik penting dari sinyal secara lebih rinci.

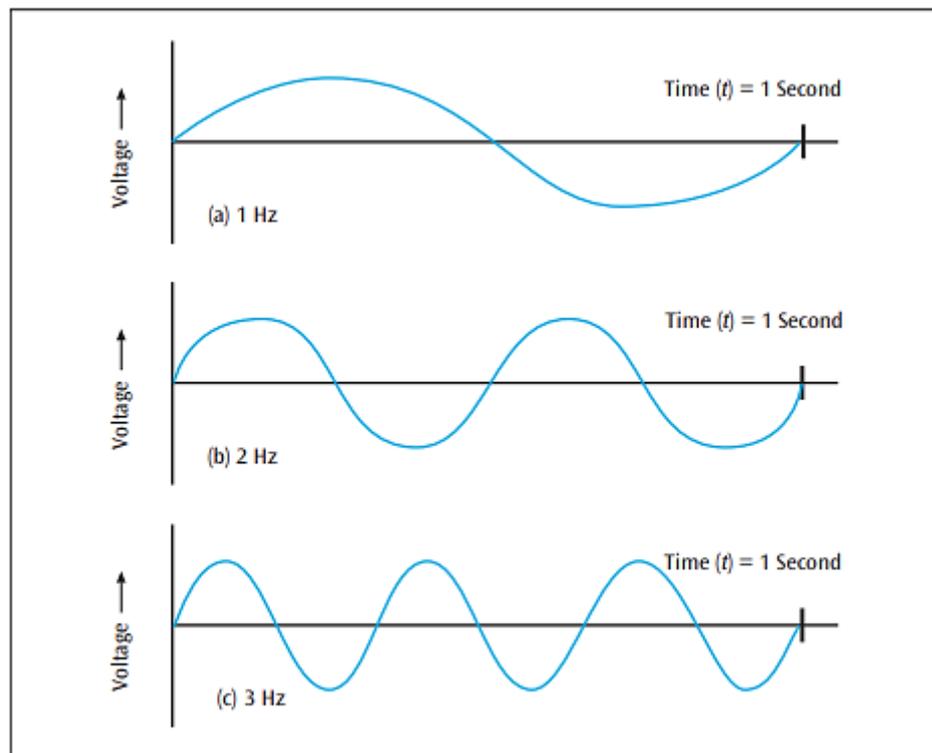
Dasar-dasar sinyal

Mari kita mulai mempelajari sinyal analog dan digital dengan memeriksa tiga komponen dasarnya: amplitudo, frekuensi, dan fase. Gelombang sinus digunakan untuk mewakili sinyal analog, seperti yang ditunjukkan pada Gambar 2.6. Amplitudo sinyal adalah ketinggian gelombang di atas (atau di bawah) titik referensi tertentu. Ketinggian ini sering kali menunjukkan level tegangan sinyal (diukur dalam volt), namun juga dapat menunjukkan level sinyal saat ini (diukur dalam amp) atau level daya sinyal (diukur dalam watt). Artinya, amplitudo suatu sinyal dapat dinyatakan dalam volt, amp, atau watt. Perhatikan bahwa sinyal dapat mengubah amplitudo seiring berjalannya waktu. Pada Gambar 2-6, Anda melihat satu sinyal dengan dua amplitudo berbeda.



Gambar 2.6 Sinyal dengan dua amplitudo berbeda

Frekuensi sinyal adalah berapa kali sinyal membuat siklus lengkap dalam jangka waktu tertentu. Lamanya, atau selang waktu, suatu siklus disebut periodenya. Periode dapat dihitung dengan mengambil kebalikan dari frekuensi ($1/\text{frekuensi}$). Gambar 2.7 menunjukkan tiga sinyal analog yang berbeda. Jika waktu t adalah satu detik, sinyal pada Gambar 2.7(a) menyelesaikan satu siklus dalam satu detik. Sinyal pada Gambar 2.7(b) menyelesaikan dua siklus dalam satu detik. Sinyal pada Gambar 2.7(c) menyelesaikan tiga siklus dalam satu detik. Siklus per detik, atau frekuensi, diwakili oleh hertz (Hz). Jadi, sinyal pada Gambar 2.7(c) mempunyai frekuensi 3 Hz.

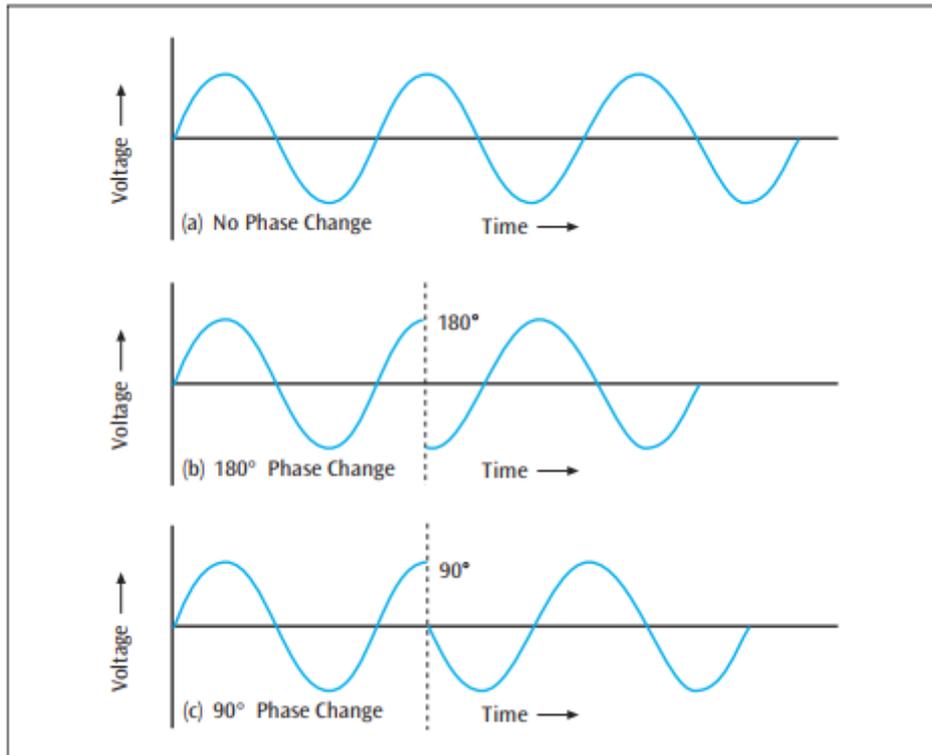


Gambar 2.7 Tiga sinyal (a) 1 Hz, (b) 2 Hz, dan (c) 3 Hz

Sinyal suara, audio, dan video manusia dan sebagian besar sinyal sebenarnya terdiri dari beberapa frekuensi. Frekuensi ganda inilah yang memungkinkan kita membedakan suara seseorang dengan suara orang lain dan alat musik yang satu dengan yang lain. Rentang frekuensi rata-rata suara manusia biasanya tidak lebih rendah dari 300 Hz dan tidak lebih tinggi dari sekitar 3400 Hz. Karena telepon dirancang untuk mengirimkan suara manusia, sistem telepon mentransmisikan sinyal dalam rentang 300 Hz hingga 3400 Hz. Piano memiliki rentang frekuensi yang lebih luas dibandingkan suara manusia. Nada terendah pada piano adalah 30 Hz, dan nada tertinggi adalah 4200 Hz.

Rentang frekuensi sinyal dari minimum hingga maksimum disebut spektrum. Spektrum contoh telepon kita hanyalah 300 Hz hingga 3400 Hz. Bandwidth suatu sinyal adalah nilai absolut selisih antara frekuensi terendah dan tertinggi. Bandwidth sistem telepon yang mentransmisikan satu suara dalam rentang 300 Hz hingga 3400 Hz adalah 3100 Hz. Karena kebisingan asing menurunkan sinyal asli, perangkat elektronik biasanya memiliki bandwidth

efektif yang lebih kecil dari bandwidthnya. Ketika membuat keputusan komunikasi, banyak profesional lebih mengandalkan bandwidth efektif daripada bandwidth karena sebagian besar situasi harus berhadapan dengan masalah kebisingan dan interferensi di dunia nyata.



Gambar 2.8 Gelombang sinus menunjukkan (a) tidak ada perubahan fasa, (b) perubahan fasa 180 derajat, dan (c) perubahan fasa 90 derajat

Fase suatu sinyal adalah posisi bentuk gelombang relatif terhadap momen waktu tertentu, atau relatif terhadap waktu nol. Pada gambar gelombang sinus sederhana pada Gambar 2.8(a), bentuk gelombang berosilasi ke atas dan ke bawah secara berulang. Perhatikan bahwa gelombang tidak pernah membuat perubahan mendadak tetapi merupakan gelombang sinus kontinu. Perubahan fasa (atau pergeseran fasa) melibatkan lompatan maju (atau mundur) dalam bentuk gelombang pada waktu tertentu. Melompat ke depan setengah dari siklus lengkap sinyal menghasilkan perubahan fase 180 derajat, seperti terlihat pada Gambar 2.8(b). Melompat maju seperempat siklus menghasilkan perubahan fase sebesar 90 derajat, seperti pada Gambar 2.8(c). Seperti yang akan Anda lihat di bagian *“Transmisi data digital dengan sinyal analog diskrit”*, beberapa sistem dapat menghasilkan sinyal yang melakukan perubahan fase sebesar 45, 135, 225, dan 315 derajat sesuai permintaan.

Saat merambat melalui media jenis apa pun, sinyal selalu mengalami kehilangan kekuatannya akibat gesekan. Hilangnya daya, atau hilangnya kekuatan sinyal, disebut atenuasi. Atenuasi dalam media seperti kawat tembaga merupakan kerugian logaritmik (dimana penurunan nilai 1 menunjukkan penurunan sepuluh kali lipat) dan merupakan fungsi dari jarak dan hambatan di dalam kawat. Mengetahui jumlah redaman sinyal (berapa banyak

daya sinyal yang hilang) memungkinkan Anda menentukan kekuatan sinyal. Desibel (dB) adalah ukuran relatif dari kehilangan atau perolehan sinyal dan digunakan untuk mengukur kehilangan atau perolehan sinyal secara logaritmik. Amplifikasi adalah kebalikan dari redaman. Ketika sinyal diperkuat oleh amplifier, sinyal bertambah dalam desibel.

Karena atenuasi adalah kerugian logaritmik dan desibel adalah nilai logaritmik, menghitung kerugian atau keuntungan keseluruhan suatu sistem melibatkan penjumlahan semua kerugian dan keuntungan desibel individual. Gambar 2.10 menunjukkan jalur komunikasi yang berjalan dari titik A sampai titik B, dan berakhir di titik C. Jalur komunikasi dari A ke B mengalami loss sebesar 10 dB, titik B mempunyai penguat sebesar 20 dB (yaitu, penguatan 20 dB terjadi di titik B), dan jalur komunikasi dari B ke C mengalami kerugian 15 dB. Berapa keuntungan atau kerugian keseluruhan sinyal antara titik A dan titik C? Untuk menjawab pertanyaan ini, tambahkan semua keuntungan dan kerugian dB:

$$-10 \text{ dB} + 20 \text{ dB} + (-15 \text{ dB}) = -5 \text{ Db}$$

RINCIAN

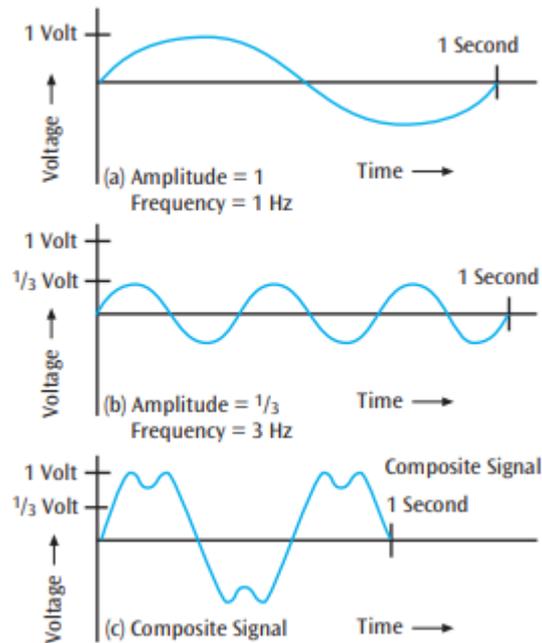
Sinyal Komposit

Hampir semua contoh sinyal yang ditunjukkan dalam bab ini adalah gelombang sinus periodik yang sederhana. Namun, Anda tidak selalu menemukan gelombang sinus periodik yang sederhana di dunia nyata. Faktanya, Anda lebih mungkin menjumpai kombinasi berbagai jenis sinus dan cosinus yang bila digabungkan akan menghasilkan bentuk gelombang yang unik.

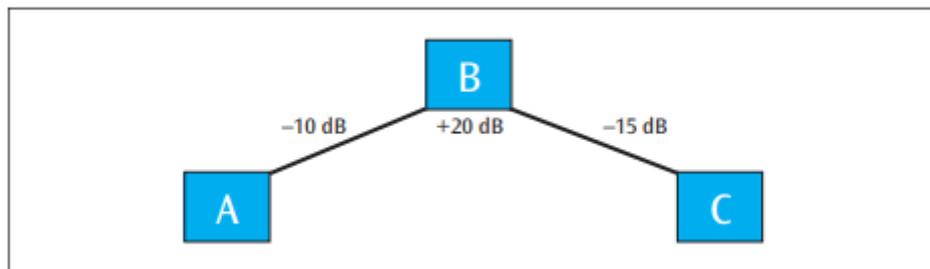
Salah satu contoh terbaiknya adalah bagaimana beberapa gelombang sinus dapat digabungkan untuk menghasilkan gelombang persegi. Dengan kata lain, beberapa sinyal analog dapat digabungkan untuk menghasilkan sinyal digital. Cabang matematika yang disebut analisis Fourier menunjukkan bahwa setiap bentuk gelombang periodik yang kompleks adalah gabungan dari bentuk gelombang periodik yang lebih sederhana. Perhatikan, misalnya, dua bentuk gelombang pertama yang ditunjukkan pada Gambar 2.9. Rumus bentuk gelombang pertama adalah $1 \sin(2\pi ft)$, dan rumus bentuk gelombang kedua adalah $1=3 \sin(2\pi 3ft)$. Dalam setiap rumus, angka di depan (masing-masing 1 dan 1=3) merupakan nilai amplitudo, istilah “sin” mengacu pada fungsi sinus trigonometri, dan istilah “ft” dan “3ft” mengacu pada frekuensi selama periode waktu tertentu. Pengujian bentuk gelombang dan rumusnya menunjukkan kepada kita bahwa amplitudo bentuk gelombang kedua adalah sepertiga amplitudo bentuk gelombang pertama, sedangkan frekuensi bentuk gelombang kedua adalah tiga kali lebih tinggi dari frekuensi gelombang kedua. bentuk gelombang pertama. Bentuk gelombang ketiga pada Gambar 2.9(c) merupakan gabungan, atau tambahan, dari dua bentuk gelombang pertama.

Perhatikan bentuk gelombang komposit yang relatif persegi. Sekarang misalkan Anda terus menambahkan lebih banyak bentuk gelombang ke sinyal komposit ini—khususnya, bentuk gelombang dengan nilai amplitudo 1=5, 1=7, 1=9, dan seterusnya (penyebut bernilai ganjil) dan nilai pengali frekuensi 5, 7, 9, dan seterusnya. Semakin banyak bentuk gelombang

yang Anda tambahkan, sinyal komposit akan semakin menyerupai bentuk gelombang persegi dari sinyal digital. Cara lain untuk menafsirkan transformasi ini adalah dengan menyatakan bahwa menambahkan bentuk gelombang dengan frekuensi yang semakin tinggi yaitu, peningkatan bandwidth akan menghasilkan komposit yang terlihat (dan berperilaku) semakin mirip sinyal digital. Menariknya, bentuk gelombang digital sebenarnya merupakan kombinasi gelombang sinus analog.



Gambar 2.9 Dua gelombang sinus periodik sederhana (a) dan (b) serta gabungannya (c)



Gambar 2.10 Contoh yang menunjukkan kerugian dan keuntungan desibel

Mari kita kembali ke contoh sebelumnya tentang spesialis jaringan yang memberi tahu Anda bahwa mungkin tidak mungkin untuk menginstal stasiun kerja komputer sesuai rencana. Anda sekarang memahami bahwa sinyal kehilangan kekuatan seiring jarak. Meskipun Anda tidak tahu berapa banyak sinyal yang akan hilang, atau pada titik mana kekuatan sinyal akan lebih lemah dibandingkan noise, Anda dapat mempercayai sebagian dari apa yang dikatakan oleh pakar jaringan kepada Anda. Tapi mari kita selidiki lebih jauh. Misalnya, jika suatu sinyal kehilangan 3 dB, apakah ini kerugian yang signifikan atau tidak?

Desibel adalah ukuran relatif dari kehilangan atau perolehan sinyal dan dinyatakan sebagai

$$\text{dB} = 10 \times \log_{10}(P_2/P_1)$$

dimana P_2 dan P_1 masing-masing merupakan level daya akhir dan awal dari sinyal yang dinyatakan dalam watt. Jika sinyal dimulai pada pemancar dengan daya 10 watt dan sampai pada penerima dengan daya 5 watt, maka kehilangan sinyal dalam dB dihitung sebagai berikut:

$$\begin{aligned} \text{dB} &= 10 \times \log_{10}(5/10) \\ &= 10 \times \log_{10}(0.5) \\ &= 10 \times (-0.3) \\ &= -3 \end{aligned}$$

Dengan kata lain, terjadi kerugian sebesar 3 dB antara pemancar dan penerima. Karena desibel adalah ukuran relatif dari kerugian atau keuntungan, Anda tidak dapat mengambil satu tingkat daya pada waktu t dan menghitung nilai desibel sinyal tersebut tanpa memiliki referensi atau tingkat daya awal.

Daripada mengingat rumus ini, mari kita gunakan jalan pintas. Seperti yang kita lihat dari perhitungan sebelumnya, setiap kali sinyal kehilangan setengah kekuatannya, maka terjadi kerugian sebesar 3 dB. Jika sinyal turun dari 10 watt menjadi 5 watt, maka terjadi kerugian sebesar 3 dB. Jika sinyal turun dari 1000 watt menjadi 500 watt, kerugiannya tetap sebesar 3 dB. Sebaliknya, sinyal yang kekuatannya digandakan akan mengalami penguatan sebesar 3 dB. Oleh karena itu, jika sinyal turun dari 1000 watt menjadi 250 watt, ini merupakan kerugian 6 dB (1000 hingga 500 adalah kerugian 3 dB, dan 500 hingga 250 sama dengan 3 dB lainnya). Sekarang kita memiliki pemahaman yang lebih baik tentang terminologi tersebut. Misalnya, jika spesialis jaringan memberi tahu kita bahwa suatu bagian kabel kehilangan 6 dB, maka sinyal yang melewati kabel tersebut telah kehilangan tiga perempat kekuatannya!

Sekarang setelah kita memahami dasar-dasar dan perbedaan antara data dan sinyal, mari kita selidiki cara mengubah data menjadi sinyal untuk transmisi.

2.3 MENGUBAH DATA MENJADI SINYAL

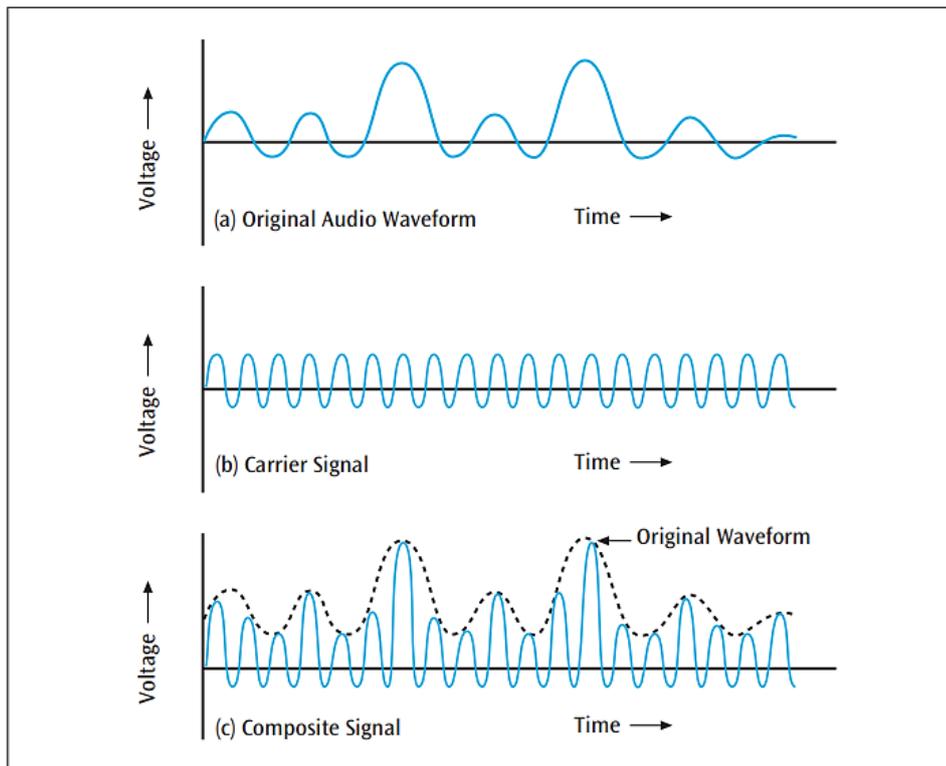
Seperti halnya sinyal, data bisa berbentuk analog atau digital. Seringkali, sinyal analog menyampaikan data analog, dan sinyal digital menyampaikan data digital. Namun, Anda dapat menggunakan sinyal analog untuk menyampaikan data digital, dan sinyal digital untuk menyampaikan data analog. Keputusan apakah akan menggunakan sinyal analog atau digital sering kali bergantung pada peralatan transmisi dan lingkungan di mana sinyal harus merambat. Ingatlah bahwa peralatan elektronik tertentu hanya mampu mendukung sinyal analog, sedangkan jenis peralatan lainnya hanya mendukung sinyal digital. Misalnya, sistem telepon diciptakan untuk mengirimkan suara manusia, yaitu data analog. Jadi, sistem telepon pada awalnya dirancang untuk mengirimkan sinyal analog. Saat ini, sebagian besar sistem

telepon menggunakan sinyal digital. Satu-satunya bagian yang tetap analog adalah loop lokal, atau sambungan dari rumah ke kantor pusat perusahaan telepon. Transmisi data analog dengan sinyal digital juga cukup umum. Awalnya, perusahaan televisi kabel mentransmisikan saluran televisi analog menggunakan sinyal analog. Baru-baru ini, saluran televisi analog diubah menjadi sinyal digital untuk menghasilkan gambar yang lebih jelas dan sinyal definisi tinggi. Seperti yang kita lihat di bab pendahuluan, siaran televisi kini ditransmisikan menggunakan sinyal digital. Seperti yang Anda lihat dari contoh ini, ada empat kombinasi utama data dan sinyal:

- Data analog ditransmisikan menggunakan sinyal analog
- Data digital dikirimkan menggunakan sinyal digital
- Data digital dikirimkan menggunakan sinyal analog diskrit
- Data analog ditransmisikan menggunakan sinyal digital Mari kita periksa satu per satu.

Mengirimkan data analog dengan sinyal analog

Dari empat kombinasi data dan sinyal, konversi data analog ke sinyal analog mungkin yang paling sederhana untuk dipahami. Hal ini karena data merupakan bentuk gelombang analog yang diubah menjadi bentuk gelombang analog lain, yaitu sinyal, untuk transmisi. Operasi dasar yang dilakukan adalah modulasi. Modulasi adalah proses pengiriman data melalui sinyal dengan memvariasikan amplitudo, frekuensi, atau fase. Telepon rumah (hanya loop lokal), radio AM, radio FM, dan siaran televisi sebelum Juni 2009 adalah contoh paling umum dari konversi sinyal data analog ke analog. Perhatikan Gambar 2.11, yang menunjukkan radio AM sebagai contoh. Data audio yang dihasilkan oleh stasiun radio mungkin tampak seperti gelombang sinus pertama yang ditunjukkan pada gambar. Untuk menyampaikan data analog ini, stasiun menggunakan sinyal gelombang pembawa, seperti yang ditunjukkan pada Gambar 2.11(b). Dalam proses modulasi, bentuk gelombang audio asli dan gelombang pembawa pada dasarnya dijumlahkan untuk menghasilkan bentuk gelombang ketiga. Perhatikan bagaimana garis putus-putus yang ditumpangkan pada bentuk gelombang ketiga mengikuti garis yang sama dengan bentuk gelombang audio asli. Di sini, data audio asli telah dimodulasi ke frekuensi pembawa tertentu (frekuensi di mana Anda mengatur putaran untuk menyetel stasiun) menggunakan modulasi amplitudo—oleh karena itu, dinamakan radio AM. Modulasi frekuensi juga dapat digunakan dengan cara serupa untuk memodulasi data analog menjadi sinyal analog, dan menghasilkan radio FM.



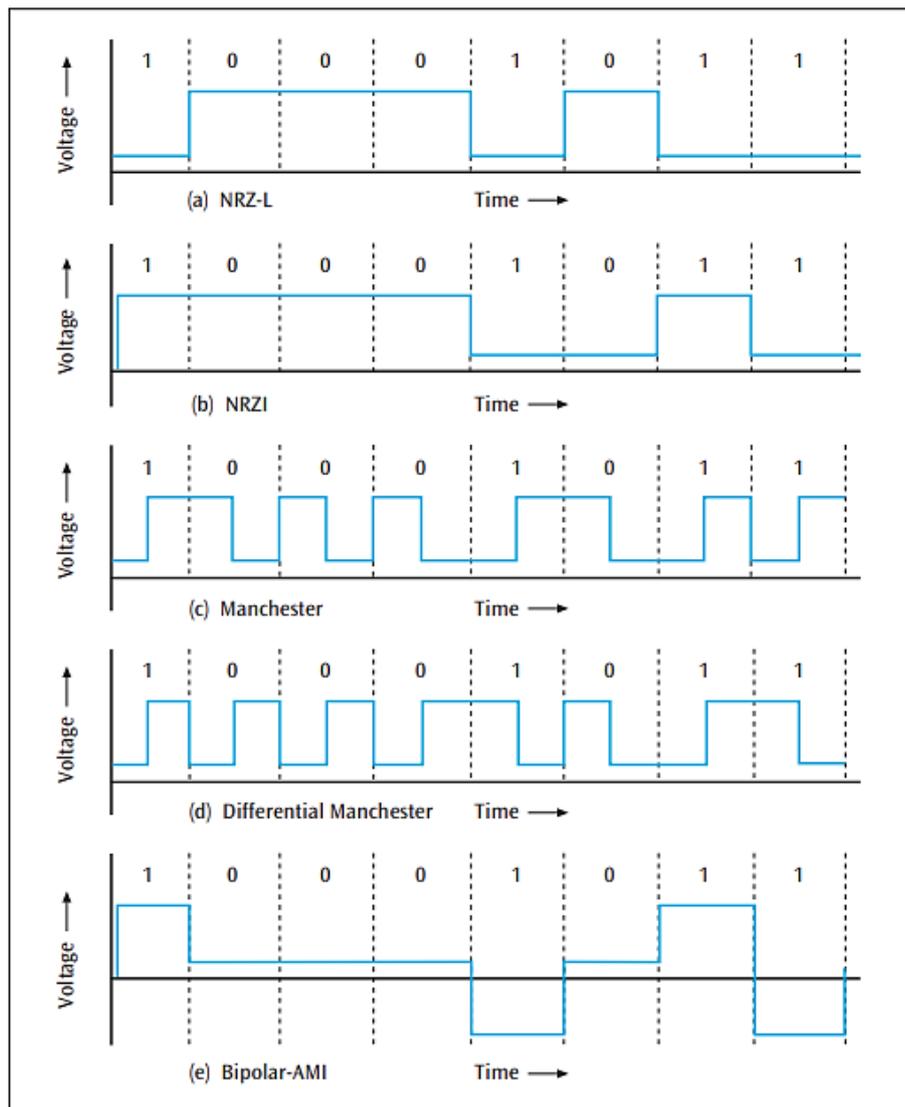
Gambar 2.11 Bentuk gelombang audio yang dimodulasi ke frekuensi pembawa menggunakan modulasi amplitudo

Transmisi data digital dengan sinyal digital: skema pengkodean digital

Untuk mengirimkan data digital menggunakan sinyal digital, angka 1 dan 0 dari data digital harus diubah ke bentuk fisik yang sesuai yang dapat ditransmisikan melalui kabel atau gelombang udara. Jadi, jika Anda ingin mengirimkan nilai data 1, Anda dapat melakukannya dengan mentransmisikan tegangan positif pada medium. Jika Anda ingin mengirimkan nilai data 0, Anda dapat mengirimkan tegangan nol. Anda juga bisa menggunakan skema sebaliknya: nilai data 0 adalah tegangan positif dan nilai data 1 adalah tegangan nol. Skema pengkodean digital seperti ini digunakan untuk mengubah 0 dan 1 data digital menjadi bentuk transmisi yang sesuai. Kami akan memeriksa enam skema pengkodean digital yang mewakili sebagian besar skema pengkodean digital: NRZ-L, NRZI, Manchester, differential Manchester, bipolar-AMI, dan 4B/5B.

Skema Pengkodean Digital Tidak Kembali ke Nol

Skema pengkodean digital non-return to zero-level (NRZ-L) mentransmisikan 1s sebagai tegangan nol dan 0s sebagai tegangan positif. Skema pengkodean NRZ-L mudah dibuat dan murah untuk diimplementasikan pada perangkat keras. Gambar 2-12(a) menunjukkan contoh skema NRZ-L.



Gambar 2.12 Contoh lima skema pengkodean digital

Skema pengkodean digital kedua, ditunjukkan pada Gambar 2.12(b), adalah nonreturn to zero inverted (NRZI). Skema pengkodean ini memiliki perubahan tegangan pada awal 1 dan tidak ada perubahan tegangan pada awal 0. Terdapat perbedaan mendasar antara NRZ-L dan NRZI. Dengan NRZ-L, penerima harus memeriksa level tegangan setiap bit untuk menentukan apakah bit tersebut 0 atau 1. Dengan NRZI, penerima harus memeriksa apakah ada perubahan pada awal bit untuk menentukan apakah bitnya 0 atau 1. Lihat lagi Gambar 2.12 untuk melihat perbedaan antara kedua skema NRZ.

Masalah yang melekat pada skema pengkodean digital NRZ-L dan NRZI adalah urutan 0 yang panjang dalam data menghasilkan sinyal yang tidak pernah berubah. Seringkali penerima mencari perubahan sinyal sehingga dapat menyinkronkan pembacaan datanya dengan pola data sebenarnya. Jika string panjang 0s ditransmisikan dan sinyalnya tidak berubah, bagaimana penerima dapat mengetahui kapan satu bit berakhir dan bit berikutnya dimulai? (Bayangkan betapa sulitnya menari mengikuti lagu yang tidak memiliki irama teratur, atau lebih buruk lagi, tidak ada irama sama sekali.) Salah satu solusi potensial adalah

memasang jam internal pada receiver yang mengetahui kapan harus mencari setiap bit yang berurutan. Namun bagaimana jika penerima mempunyai jam yang berbeda dengan jam yang digunakan pemancar untuk menghasilkan sinyal? Siapa bilang kedua jam ini memiliki waktu yang sama? Sistem yang lebih akurat akan menghasilkan sinyal yang memiliki perubahan untuk setiap bit. Jika penerima dapat mengandalkan setiap bit untuk mengalami beberapa bentuk perubahan sinyal, maka ia dapat tetap tersinkronisasi dengan aliran data yang masuk.

Skema Pengkodean Digital Manchester

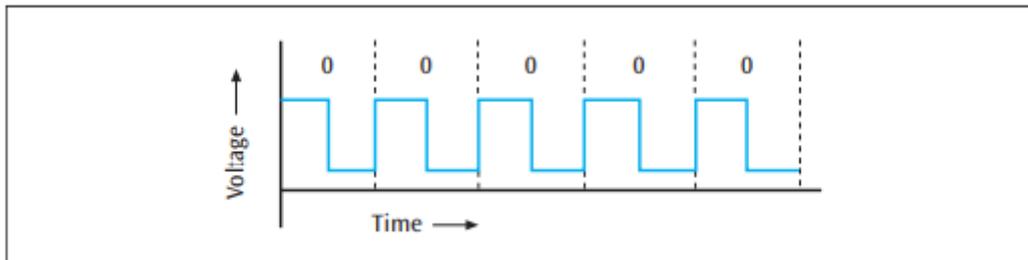
Skema pengkodean digital kelas Manchester memastikan bahwa setiap bit memiliki beberapa jenis perubahan sinyal, dan dengan demikian memecahkan masalah sinkronisasi. Ditunjukkan pada Gambar 2.12(c), skema pengkodean Manchester mempunyai sifat sebagai berikut: Untuk mengirimkan 1, sinyal berubah dari rendah ke tinggi di tengah interval, dan untuk mengirimkan 0, sinyal berubah dari tinggi ke rendah di pertengahan interval. Perhatikan bahwa transisi selalu berada di tengah, angka 1 adalah transisi rendah ke tinggi, dan 0 adalah transisi tinggi ke rendah. Jadi, jika sinyal saat ini rendah dan bit berikutnya yang dikirim adalah 0, sinyal harus berpindah dari rendah ke tinggi pada awal interval sehingga dapat melakukan transisi tinggi ke rendah di tengah. Pengkodean Manchester digunakan dalam jaringan area lokal berkecepatan rendah untuk mentransmisikan data digital melalui kabel jaringan area lokal.

Skema pengkodean digital diferensial Manchester digunakan dalam bentuk jaringan area lokal (token ring) yang sekarang sudah punah tetapi masih ada dalam sejumlah aplikasi unik. Mirip dengan skema Manchester yang selalu ada transisi di pertengahan interval. Namun berbeda dengan kode Manchester, arah transisi di tengah ini tidak membedakan antara 0 atau 1. Sebaliknya, jika ada transisi di awal interval, maka 0 yang ditransmisikan. Jika tidak ada transisi pada awal interval, maka 1 sedang ditransmisikan. Karena penerima harus memperhatikan awal interval untuk menentukan nilai bit, diferensial Manchester mirip dengan skema NRZI (dalam hal ini). Gambar 2.12(d) menunjukkan contoh pengkodean diferensial Manchester.

Skema Manchester memiliki keunggulan dibandingkan skema NRZ: Dalam skema Manchester, selalu ada transisi di tengah-tengah. Dengan demikian, penerima dapat mengharapkan perubahan sinyal secara berkala dan dapat menyinkronkan dirinya dengan aliran bit yang masuk. Skema pengkodean Manchester disebut self-clocking karena terjadinya transisi reguler mirip dengan detik yang berdetak pada jam. Seperti yang akan Anda lihat di Bab Empat, sangat penting bagi receiver untuk tetap tersinkronisasi dengan aliran bit yang masuk, dan kode Manchester memungkinkan receiver mencapai sinkronisasi ini.

Kerugian besar dari skema Manchester adalah kira-kira separuh waktu akan terdapat dua transisi pada setiap bit. Misalnya, jika skema pengkodean diferensial Manchester digunakan untuk mengirimkan serangkaian 0, maka sinyal harus berubah di awal setiap bit, serta perubahan di tengah setiap bit. Jadi, untuk setiap nilai data 0, sinyalnya berubah dua kali. Berapa kali sinyal berubah nilai per detik disebut baud rate, atau baud saja. Pada Gambar 2.13, serangkaian biner 0 ditransmisikan menggunakan skema pengkodean diferensial Manchester. Perhatikan bahwa sinyal berubah dua kali untuk setiap bit. Setelah satu detik,

sinyal berubah 10 kali. Oleh karena itu, baud ratenya adalah 10. Selama periode waktu yang sama, hanya 5 bit yang dikirimkan. Kecepatan data, diukur dalam bit per detik (bps), adalah 5, yang dalam hal ini adalah setengah baud rate. Banyak orang yang keliru menyamakan baud rate dengan bps (atau data rate). Dalam keadaan tertentu, baud rate mungkin sama dengan bps, seperti pada skema pengkodean NRZ-L atau NRZI yang ditunjukkan pada Gambar 2.12. Dalam hal ini, terdapat paling banyak satu perubahan sinyal untuk setiap bit yang ditransmisikan. Namun dengan skema seperti kode Manchester, baud rate tidak sama dengan bps.



Gambar 2.13 Mentransmisikan lima biner 0 menggunakan pengkodean diferensial Manchester

Mengapa penting bahwa beberapa skema pengkodean memiliki baud rate dua kali bps? Karena kode Manchester memiliki baud rate dua kali bps, dan kode NRZ-L dan NRZI memiliki baud rate yang sama dengan bps, perangkat keras yang menghasilkan sinyal berkode Manchester harus bekerja dua kali lebih cepat daripada perangkat keras yang menghasilkan sinyal berkode Manchester. sinyal berkode NRZ. Jika 100 juta 0s per detik ditransmisikan menggunakan pengkodean diferensial Manchester, sinyal harus berubah 200 juta kali per detik (berbeda dengan 100 juta kali per detik dengan pengkodean NRZ). Seperti kebanyakan hal dalam hidup, Anda tidak mendapatkan sesuatu secara cuma-cuma. Perangkat keras atau perangkat lunak yang menangani skema pengkodean Manchester lebih rumit dan lebih mahal dibandingkan perangkat keras atau perangkat lunak yang menangani skema pengkodean NRZ. Yang lebih penting lagi, seperti yang akan segera kita lihat, sinyal yang berubah dengan kecepatan lebih tinggi lebih rentan terhadap noise dan kesalahan.

Skema Pengkodean Bipolar-AMI

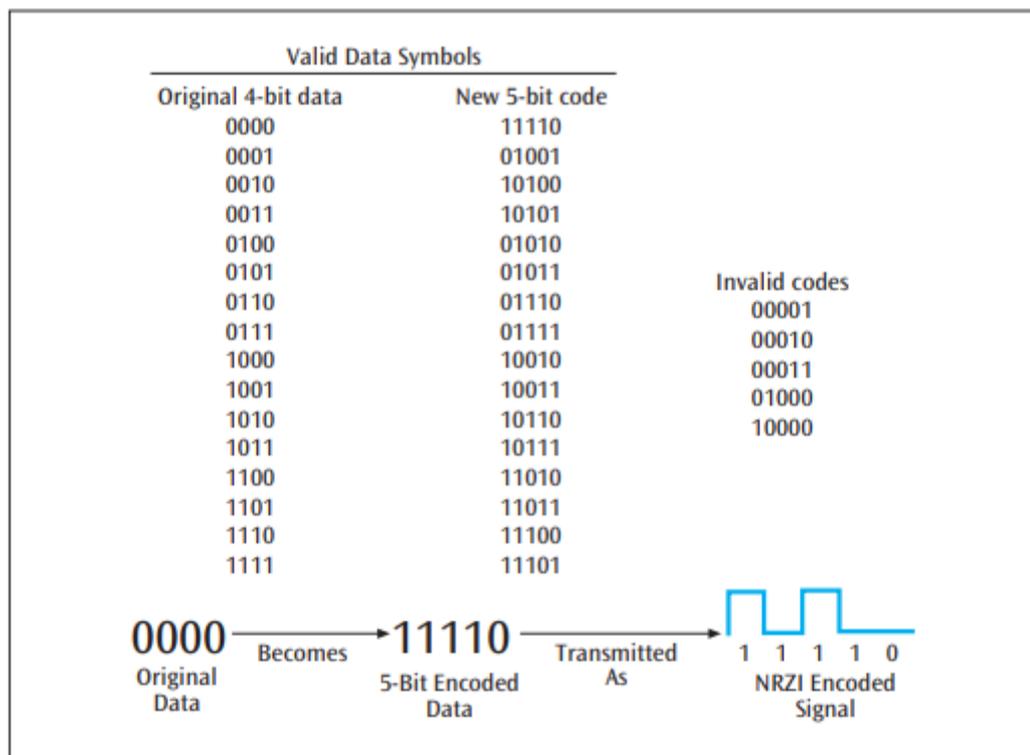
Skema pengkodean bipolar-AMI unik di antara semua skema pengkodean yang terlihat sejauh ini karena menggunakan tiga level tegangan. Ketika perangkat mentransmisikan biner 0, tegangan nol ditransmisikan. Ketika perangkat mentransmisikan biner 1, tegangan positif atau tegangan negatif ditransmisikan. Yang mana yang ditransmisikan bergantung pada nilai biner 1 yang terakhir ditransmisikan. Misalnya, jika biner 1 terakhir mengirimkan tegangan positif, maka biner 1 berikutnya akan mengirimkan tegangan negatif. Demikian pula jika biner 1 terakhir mengirimkan tegangan negatif, maka biner 1 berikutnya akan mengirimkan tegangan positif (Gambar 2.12).

Skema bipolar memiliki dua kelemahan yang jelas. Pertama, seperti yang Anda lihat pada Gambar 2.12(e), kita menghadapi masalah sinkronisasi string panjang 0 lagi, seperti yang

kita alami pada skema NRZ. Kedua, perangkat keras sekarang harus mampu menghasilkan dan mengenali tegangan negatif serta tegangan positif. Di sisi lain, keuntungan utama dari skema bipolar adalah ketika semua tegangan dijumlahkan setelah transmisi yang panjang, seharusnya terdapat tegangan total nol. Artinya, tegangan positif dan negatif pada dasarnya saling meniadakan. Jenis penjumlahan tegangan nol ini dapat berguna pada jenis sistem elektronik tertentu (pertanyaan mengapa hal ini berguna berada di luar cakupan teks ini).

Skema Pengkodean Digital 4B/5B

Skema pengkodean Manchester menyelesaikan masalah sinkronisasi tetapi relatif tidak efisien karena memiliki baud rate dua kali bps. Skema 4B/5B mencoba untuk memenuhi masalah sinkronisasi dan menghindari masalah “baud sama dengan dua kali bps”. Skema pengkodean 4B/5B mengambil 4 bit data, mengubah 4 bit tersebut menjadi urutan 5-bit yang unik, dan mengkodekan 5 bit tersebut menggunakan NRZI.



Gambar 2.14 Skema pengkodean digital 4B/5B

Langkah pertama yang dilakukan perangkat keras dalam menghasilkan kode 4B/5B adalah mengubah jumlah 4-bit dari data asli menjadi jumlah 5 bit yang baru. Menggunakan 5 bit (atau lima 0 dan 1) untuk mewakili satu nilai menghasilkan 32 kombinasi potensial ($2^5 = 32$). Dari kemungkinan-kemungkinan ini, hanya 16 kombinasi yang digunakan, sehingga tidak ada kode yang memiliki tiga atau lebih angka 0 berturut-turut. Dengan cara ini, jika perangkat transmisi mengirimkan jumlah 5-bit menggunakan pengkodean NRZI, tidak akan pernah ada lebih dari dua baris 0 yang ditransmisikan (kecuali satu karakter 5-bit diakhiri dengan 00, dan karakter 5-bit berikutnya dimulai dengan a 0). Jika Anda tidak pernah mengirimkan lebih dari dua 0 berturut-turut menggunakan pengkodean NRZI, maka Anda tidak akan pernah

mengalami periode panjang di mana tidak ada transisi sinyal. Gambar 2.14 menunjukkan kode 4B/5B secara rinci.

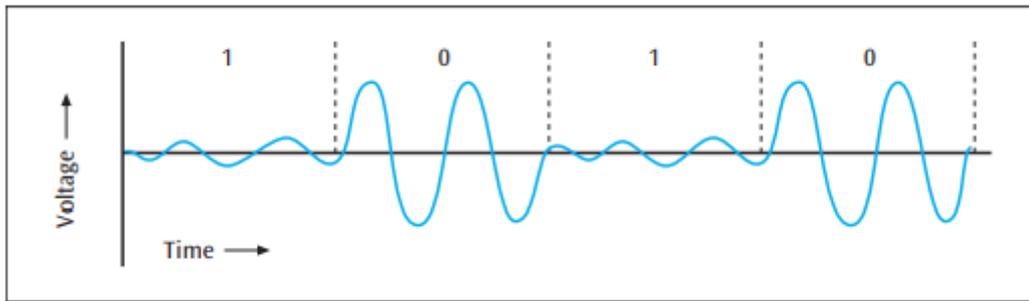
Bagaimana cara kerja kode 4B/5B? Katakanlah, misalnya, 4 bit berikutnya dalam aliran data yang akan dikirim adalah 0000, yang, seperti Anda lihat, memiliki rangkaian angka nol yang berurutan dan oleh karena itu akan menghasilkan sinyal yang tidak berubah. Melihat kolom pertama pada Gambar 2.14, kita melihat bahwa pengkodean 4B/5B menggantikan 0000 dengan 11110. Perhatikan bahwa 11110, seperti semua kode 5-bit pada kolom kedua Gambar 2.14, tidak memiliki lebih banyak dari dua angka nol yang berurutan. Setelah mengganti 0000 dengan 11110, perangkat keras sekarang akan mengirimkan 11110. Karena kode 5-bit ini ditransmisikan menggunakan NRZI, baud rate sama dengan bps sehingga lebih efisien. Sayangnya, mengubah kode 4-bit menjadi kode 5-bit menghasilkan overhead sebesar 20 persen (satu bit tambahan). Bandingkan dengan kode Manchester, yang baud ratenya bisa dua kali bps sehingga menghasilkan overhead 100 persen. Jelasnya, overhead 20 persen lebih baik daripada overhead 100 persen. Banyak sistem pengkodean digital baru yang menggunakan kabel serat optik juga menggunakan teknik yang sangat mirip dengan 4B/5B. Dengan demikian, pemahaman tentang 4B/5B yang lebih sederhana dapat mengarah pada pemahaman tentang beberapa teknik pengkodean digital yang lebih baru.

Mengirimkan data digital dengan sinyal analog diskrit

Teknik mengubah data digital menjadi sinyal analog juga merupakan contoh modulasi. Namun dalam jenis modulasi ini, sinyal analog mengambil sejumlah level sinyal yang berbeda-beda. Ini bisa berupa dua level sinyal (seperti teknik pertama yang ditunjukkan pada paragraf berikutnya) atau sesuatu yang lebih kompleks seperti 256 level seperti yang digunakan pada sinyal televisi digital. Penerima kemudian mencari level sinyal unik ini secara khusus. Oleh karena itu, meskipun sinyal-sinyal tersebut pada dasarnya analog, sinyal-sinyal tersebut beroperasi dengan jumlah level yang berbeda-beda, seperti sinyal digital pada bagian sebelumnya. Jadi untuk menghindari kebingungan, kami akan memberi label pada sinyal analog terpisah. Mari kita periksa sejumlah teknik modulasi diskrit yang dimulai dengan teknik yang lebih sederhana (shift keying) dan diakhiri dengan teknik yang lebih kompleks yang digunakan untuk sistem seperti sinyal televisi digital modulasi amplitudo kuadratur.

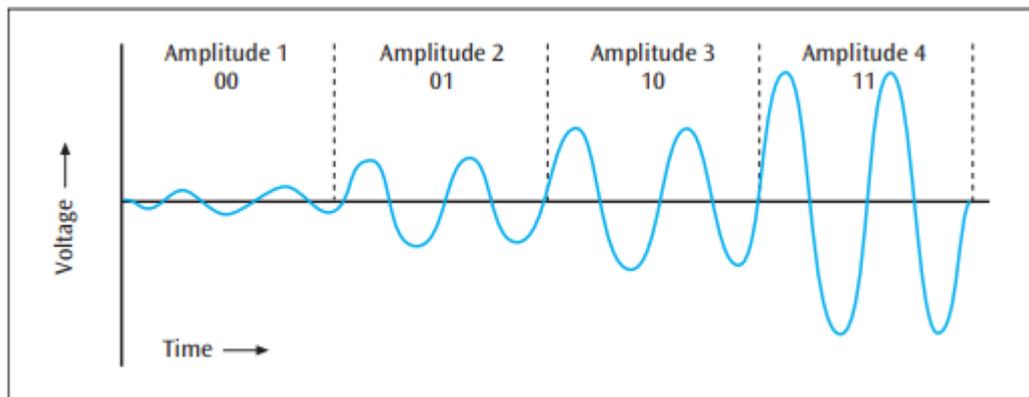
Penguncian Pergeseran Amplitudo

Teknik modulasi yang paling sederhana adalah amplitudo shift keying. Seperti ditunjukkan pada Gambar 2.15, nilai data 1 dan nilai data 0 diwakili oleh dua amplitudo sinyal yang berbeda. Misalnya, amplitudo yang lebih tinggi dapat mewakili 1, sedangkan amplitudo yang lebih rendah (atau amplitudo nol) dapat mewakili 0. Perhatikan bahwa selama setiap periode bit, amplitudo sinyal adalah konstan.



Gambar 2.15 Contoh sederhana dari penguncian pergeseran amplitudo

Penguncian pergeseran amplitudo tidak dibatasi pada dua kemungkinan tingkat amplitudo. Misalnya, kita dapat membuat teknik penguncian pergeseran amplitudo yang menggabungkan empat tingkat amplitudo berbeda, seperti yang ditunjukkan pada Gambar 2.16. Masing-masing dari empat tingkat amplitudo yang berbeda akan mewakili 2 bit. Anda mungkin ingat bahwa ketika menghitung dalam biner, 2 bit menghasilkan empat kemungkinan kombinasi: 00, 01, 10, dan 11. Jadi, setiap kali sinyal berubah (setiap kali amplitudo berubah), 2 bit ditransmisikan. Hasilnya, kecepatan data (bps) menjadi dua kali lipat kecepatan baud. Ini kebalikan dari kode Manchester yang kecepatan datanya setengah baud rate. Sebuah sistem yang mentransmisikan 2 bit per perubahan sinyal lebih efisien daripada sistem yang memerlukan dua perubahan sinyal untuk setiap bit.

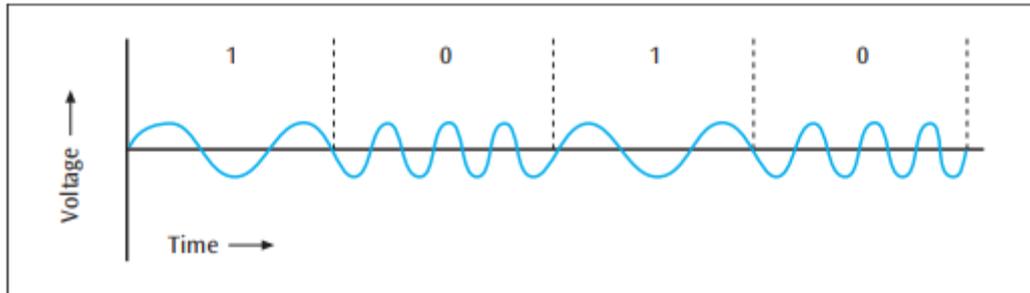


Gambar 2.16 Penguncian pergeseran amplitudo menggunakan empat tingkat amplitudo yang berbeda

Penguncian pergeseran amplitudo memiliki kelemahan: rentan terhadap impuls kebisingan yang tiba-tiba seperti muatan statis yang dihasilkan oleh badai petir. Ketika sinyal terganggu oleh pelepasan muatan statis yang besar, sinyal mengalami peningkatan amplitudo yang signifikan. Karena alasan ini, dan karena sulit untuk secara akurat membedakan lebih dari beberapa tingkat amplitudo, penguncian pergeseran amplitudo adalah salah satu teknik pengkodean yang paling tidak efisien dan tidak digunakan pada sistem yang memerlukan kecepatan transmisi data yang tinggi. Saat mentransmisikan data melalui saluran telepon standar, penguncian pergeseran amplitudo biasanya tidak melebihi 1200 bps.

Penguncian Pergeseran Frekuensi

Penguncian pergeseran frekuensi menggunakan dua rentang frekuensi berbeda untuk mewakili nilai data 0 dan 1, seperti yang ditunjukkan pada Gambar 2-17. Misalnya, sinyal frekuensi yang lebih rendah mungkin mewakili angka 1, sedangkan sinyal frekuensi yang lebih tinggi mungkin mewakili angka 0. Selama setiap periode bit, frekuensi sinyal adalah konstan.

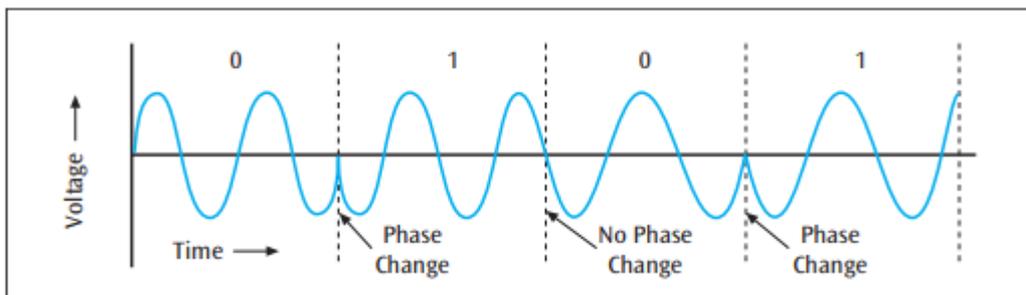


Gambar 2.17 Contoh sederhana penguncian pergeseran frekuensi

Berbeda dengan penguncian pergeseran amplitudo, penguncian pergeseran frekuensi tidak mempunyai masalah dengan lonjakan kebisingan mendadak yang dapat menyebabkan hilangnya data. Meskipun demikian, penguncian pergeseran frekuensi tidak sempurna. Hal ini rentan terhadap distorsi intermodulasi, sebuah fenomena yang terjadi ketika frekuensi dari dua atau lebih sinyal bercampur dan menciptakan frekuensi baru. Jadi, seperti penguncian pergeseran amplitudo, penguncian pergeseran frekuensi tidak digunakan pada sistem yang memerlukan kecepatan data yang tinggi.

Penguncian Pergeseran Fase

Teknik modulasi ketiga adalah penguncian pergeseran fasa. Penguncian pergeseran fasa mewakili 0 dan 1 dengan perubahan berbeda dalam fasa bentuk gelombang. Misalnya, angka 0 berarti tidak ada perubahan fasa, sedangkan angka 1 berarti perubahan fasa sebesar 180 derajat, seperti ditunjukkan pada Gambar 2.18.

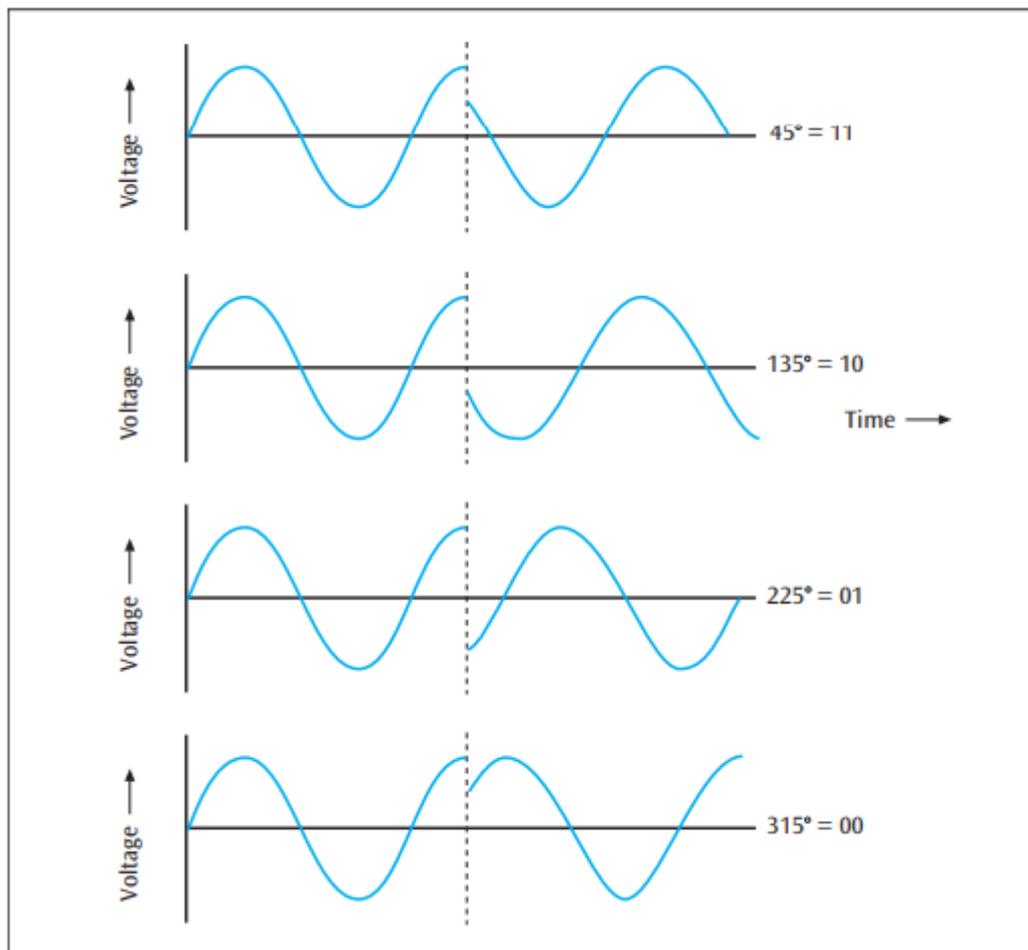


Gambar 2.18 Contoh sederhana penguncian pergeseran fasa

Perubahan fasa tidak dipengaruhi oleh perubahan amplitudo, juga tidak dipengaruhi oleh distorsi intermodulasi. Dengan demikian, penguncian pergeseran fasa kurang rentan terhadap kebisingan dan dapat digunakan pada frekuensi yang lebih tinggi. Penguncian pergeseran fasa sangat akurat sehingga pemancar sinyal dapat meningkatkan efisiensi dengan

memperkenalkan beberapa sudut pergeseran fasa. Misalnya, penguncian pergeseran fasa kuadratur menggabungkan empat sudut fasa yang berbeda, yang masing-masing mewakili 2 bit: pergeseran fasa 45 derajat mewakili nilai data 11, pergeseran fasa 135 derajat mewakili 10, pergeseran fasa 225 derajat mewakili nilai data 11, pergeseran fasa 135 derajat mewakili 10, dan pergeseran fasa 225 derajat. mewakili 01, dan pergeseran fasa 315 derajat mewakili 00. Gambar 2.19 menunjukkan gambar sederhana dari empat pergeseran fasa yang berbeda.

Karena setiap pergeseran fasa mewakili 2 bit, penguncian pergeseran fasa kuadratur memiliki efisiensi dua kali lipat dari penguncian pergeseran fasa sederhana. Dengan teknik pengkodean ini, satu perubahan sinyal sama dengan 2 bit informasi; artinya, 1 baud sama dengan 2 bps.

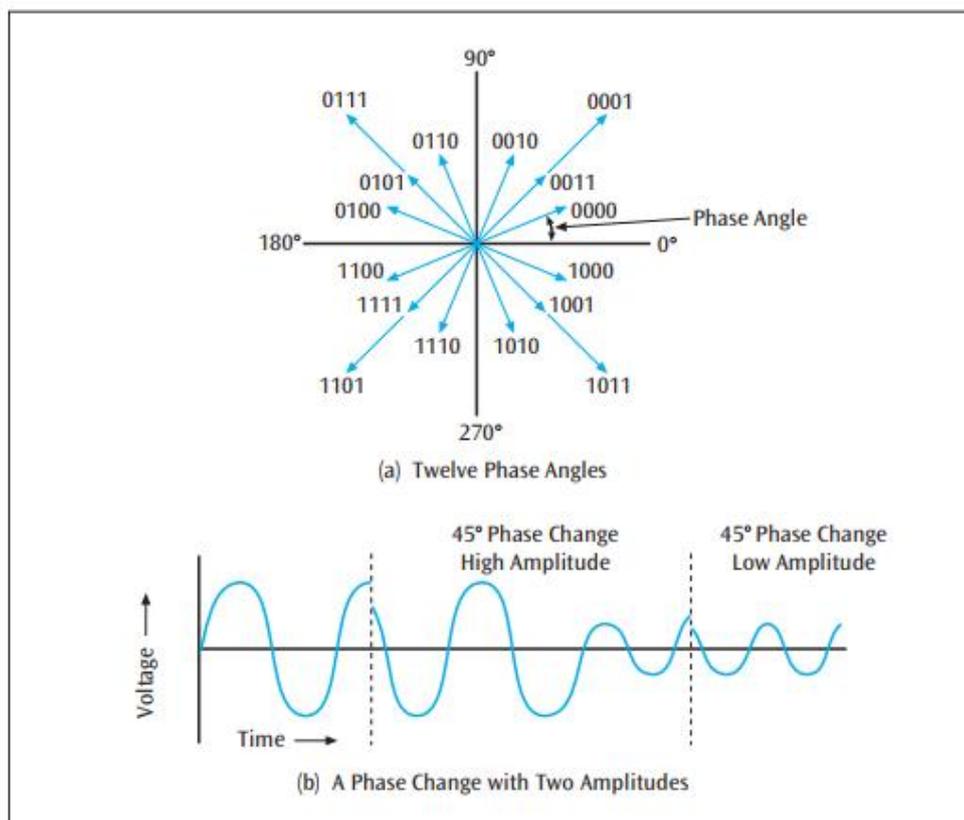


Gambar 2.19 Empat sudut fasa 45, 135, 225, dan 315 derajat, seperti terlihat pada penguncian pergeseran fasa kuadratur

Tapi mengapa berhenti di situ? Mengapa tidak membuat teknik penguncian pergeseran fasa yang menggabungkan delapan sudut fasa berbeda? Hal ini dimungkinkan, dan jika ada, seseorang dapat mengirimkan 3 bit per perubahan fasa (3 bit per perubahan sinyal, atau 3 bit per baud). Enam belas perubahan fase akan menghasilkan 4 bit per baud; Perubahan 32 fase akan menghasilkan 5 bit per baud. Perhatikan bahwa 2 dipangkatkan dengan jumlah

bit per baud sama dengan jumlah perubahan fasa. Atau sebaliknya, \log_2 jumlah perubahan fasa sama dengan jumlah bit per baud. Konsep ini adalah kunci sistem komunikasi yang efisien: semakin tinggi jumlah bit per baud, semakin cepat kecepatan data sistem. Kami akan meninjau kembali konsep ini.

Bagaimana jika kita membuat metode pensinyalan yang menggabungkan 12 sudut pergeseran fasa berbeda dengan dua amplitudo berbeda? Gambar 2.20(a) (dikenal sebagai diagram konstelasi) menunjukkan 12 sudut pergeseran fasa yang berbeda dengan 12 busur yang memancar dari sebuah titik pusat. Dua amplitudo berbeda diterapkan pada masing-masing empat sudut (tetapi hanya empat sudut). Gambar 2.20(b) menunjukkan pergeseran fasa dengan dua amplitudo berbeda. Jadi, delapan sudut fasa mempunyai amplitudo tunggal, dan empat sudut fasa mempunyai amplitudo ganda, sehingga menghasilkan 16 kombinasi berbeda. Teknik pengkodean ini adalah contoh dari keluarga teknik pengkodean yang disebut modulasi amplitudo kuadratur, yang biasanya digunakan pada modem berkecepatan tinggi dan menggunakan setiap perubahan sinyal untuk mewakili 4 bit (4 bit menghasilkan 16 kombinasi). Oleh karena itu, bps data yang dikirimkan menggunakan modulasi amplitudo kuadratur adalah empat kali baud rate. Misalnya, sistem yang menggunakan sinyal dengan baud rate 2400 mencapai kecepatan transfer data 9600 bps (4×2400). Menariknya, teknik seperti inilah yang memungkinkan kita mengakses Internet melalui DSL dan menonton siaran televisi digital.



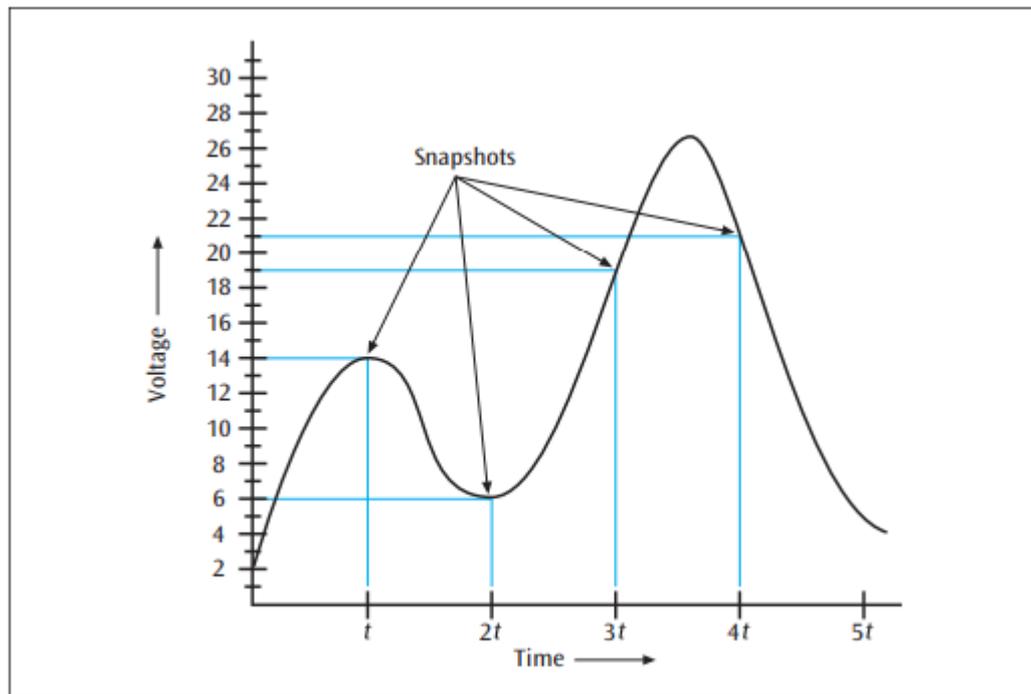
Gambar 2.20 Gambar (a) menunjukkan 12 fasa yang berbeda, sedangkan Gambar (b) menunjukkan perubahan fasa dengan dua amplitudo yang berbeda

Transmisi data analog dengan sinyal digital

Seringkali diperlukan untuk mengirimkan data analog melalui media digital. Misalnya, banyak laboratorium ilmiah memiliki peralatan pengujian yang menghasilkan hasil pengujian dalam bentuk data analog. Data analog ini diubah menjadi sinyal digital sehingga data asli dapat ditransmisikan melalui sistem komputer dan akhirnya disimpan dalam memori atau pada disk magnetik. Perusahaan rekaman musik yang membuat CD juga mengubah data analog menjadi sinyal digital. Seorang artis membawakan lagu yang menghasilkan musik, yaitu data analog. Sebuah perangkat kemudian mengubah data analog ini menjadi data digital sehingga biner 1 dan 0 dari musik digital dapat disimpan, diedit, dan akhirnya direkam pada CD. Ketika CD digunakan, seseorang memasukkan disk tersebut ke dalam pemutar CD yang mengubah biner 1 dan 0 kembali menjadi musik analog. Mari kita lihat dua teknik untuk mengubah data analog menjadi sinyal digital.

Modulasi Kode Pulsa

Salah satu teknik pengkodean yang mengubah data analog menjadi sinyal digital adalah modulasi kode pulsa (PCM). Perangkat keras—khususnya, codec—mengonversi data analog menjadi sinyal digital dengan melacak bentuk gelombang analog dan mengambil “snapshot” data analog pada interval tetap. Pengambilan snapshot melibatkan penghitungan ketinggian, atau voltase, bentuk gelombang analog di atas ambang batas tertentu.



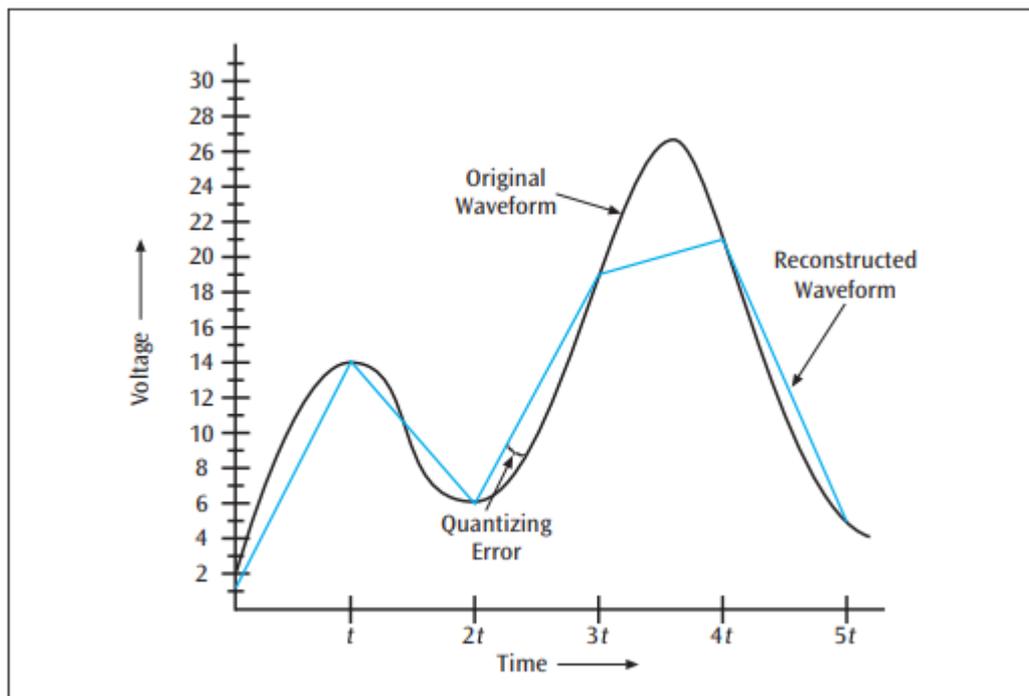
Gambar 2.21 Contoh pengambilan “snapshot” bentuk gelombang analog untuk dikonversi menjadi sinyal digital

Ketinggian ini, yang merupakan nilai analog, diubah menjadi nilai biner berukuran tetap yang setara. Nilai biner ini kemudian dapat ditransmisikan melalui format pengkodean digital. Melacak bentuk gelombang analog dan mengubahnya menjadi pulsa yang mewakili

ketinggian gelombang di atas (atau di bawah) ambang batas disebut modulasi amplitudo pulsa (PAM). Istilah “modulasi kode pulsa” sebenarnya berlaku untuk konversi pulsa individu menjadi nilai biner. Namun, agar singkatnya, kami akan menyebut seluruh proses hanya sebagai modulasi kode pulsa.

Gambar 2.21 menunjukkan contoh modulasi kode pulsa. Pada waktu t (pada sumbu x), cuplikan bentuk gelombang analog diambil, menghasilkan nilai desimal 14 (pada sumbu y). 14 diubah menjadi nilai biner 5-bit (seperti 01110) oleh codec dan dikirimkan ke perangkat untuk penyimpanan. Pada Gambar 2.21, sumbu y dibagi menjadi 32 gradasi, atau tingkat kuantisasi. (Perhatikan bahwa nilai pada sumbu y berkisar dari 0 hingga 31, sesuai dengan 32 divisi.) Karena terdapat 32 tingkat kuantisasi, setiap snapshot menghasilkan nilai 5-bit ($2^5 = 32$).

Apa yang terjadi jika nilai snapshot berada di antara 13 dan 14? Jika mendekati 14, kita akan memperkirakan dan memilih 14. Jika mendekati 13, kita akan memperkirakan dan memilih 13. Apa pun yang terjadi, perkiraan kita akan menyebabkan kesalahan pada pengkodean karena kita tidak mengkodekan nilai pasti dari nilai tersebut. bentuk gelombang. Jenis kesalahan ini disebut kesalahan kuantisasi, atau gangguan kuantisasi, dan menyebabkan data analog yang dihasilkan berbeda dari data analog asli.

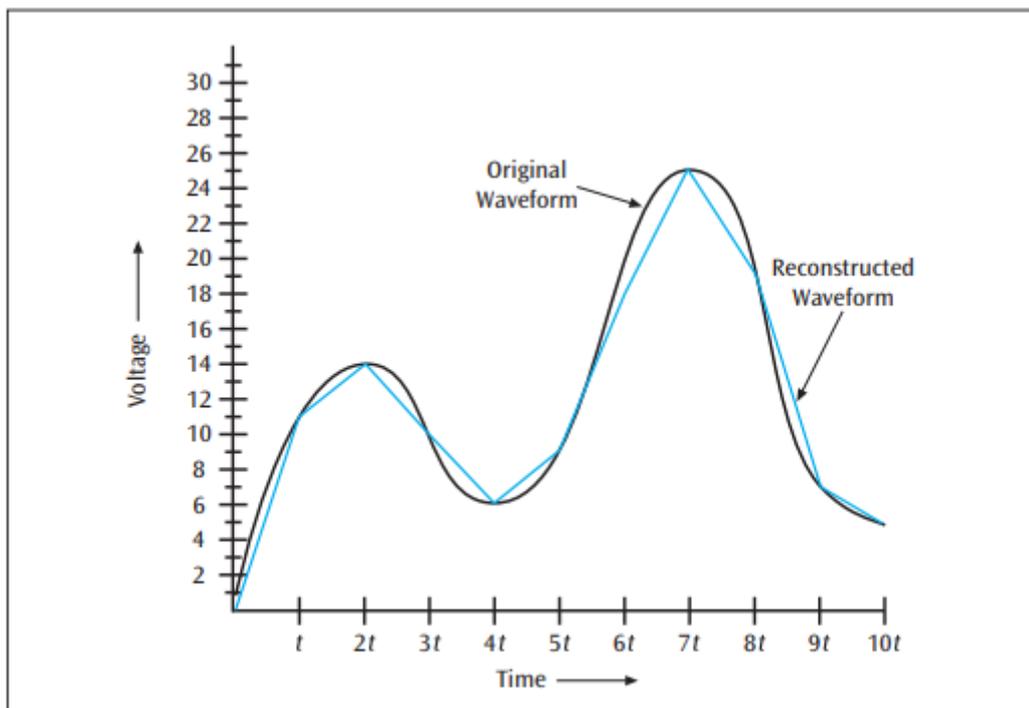


Gambar 2.22 Rekonstruksi bentuk gelombang analog dari “snapshot” digital

Untuk mengurangi jenis kesalahan kuantisasi ini, kita dapat menyetel sumbu y secara lebih halus dengan membaginya menjadi 64 (yaitu, menggandakan jumlah) tingkat kuantisasi. Seperti biasa, kita tidak mendapatkan sesuatu dengan cuma-cuma. Ketelitian ekstra ini memerlukan perangkat keras yang lebih presisi, dan hal ini akan menghasilkan nilai bit yang lebih besar untuk setiap sampel (karena memiliki 64 tingkat kuantisasi memerlukan nilai 6-bit, atau $2^6 = 64$). Melanjutkan pengkodean bentuk gelombang pada Gambar 2.21, kita melihat

bahwa pada waktu $2t$, codec mengambil snapshot kedua. Tegangan bentuk gelombang di sini ditemukan memiliki nilai desimal 6, sehingga 6 ini diubah menjadi nilai biner 5-bit kedua dan disimpan. Proses pengkodean berlanjut dengan cara ini dengan codec mengambil snapshot, mengubah nilai tegangan (juga dikenal sebagai nilai PAM) ke bentuk biner, dan menyimpannya sepanjang bentuk gelombang.

Untuk merekonstruksi bentuk gelombang analog asli dari nilai digital yang disimpan, perangkat keras khusus mengubah setiap nilai biner n -bit kembali ke desimal dan menghasilkan pulsa listrik dengan besaran (tinggi) yang sesuai. Dengan aliran nilai konversi yang masuk secara kontinyu, bentuk gelombang yang mendekati aslinya dapat direkonstruksi, seperti yang ditunjukkan pada Gambar 2.22.



Gambar 2.23 Rekonstruksi bentuk gelombang asli yang lebih akurat menggunakan laju pengambilan sampel yang lebih tinggi

Terkadang bentuk gelombang yang direkonstruksi ini tidak merupakan reproduksi yang baik dari gelombang aslinya. Apa yang dapat dilakukan untuk meningkatkan keakuratan bentuk gelombang yang direproduksi? Seperti yang telah kita lihat, kita mungkin dapat meningkatkan jumlah tingkat kuantisasi pada sumbu y . Selain itu, semakin dekat pengambilan foto satu sama lain (semakin kecil interval waktu antar foto, atau semakin halus resolusinya), semakin akurat bentuk gelombang yang direkonstruksi. Gambar 2.23 menunjukkan rekonstruksi yang mendekati bentuk gelombang analog aslinya. Namun sekali lagi, Anda tidak mendapatkan sesuatu secara cuma-cuma. Untuk mengambil snapshot dalam interval waktu yang lebih singkat, codec harus memiliki kualitas yang cukup tinggi untuk melacak sinyal masuk dengan cepat dan melakukan konversi yang diperlukan. Dan semakin banyak snapshot yang diambil per detik, semakin banyak data biner yang dihasilkan per detik. Frekuensi

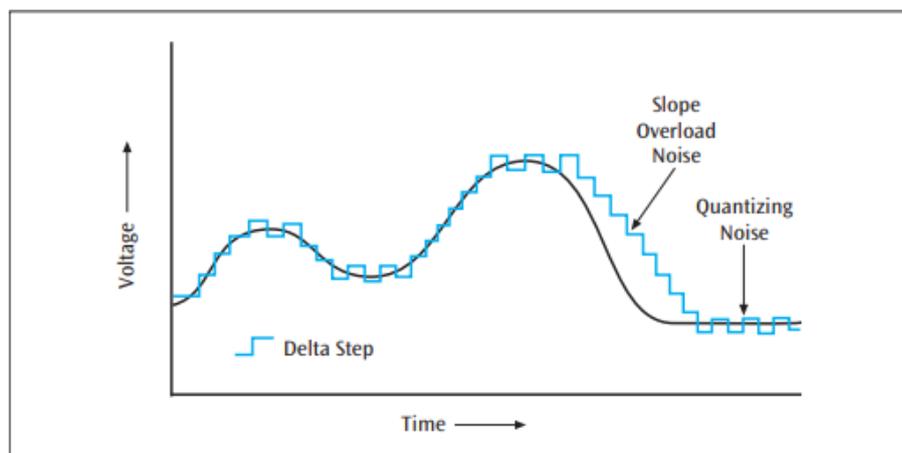
pengambilan snapshot disebut laju pengambilan sampel. Jika codec mengambil sampel pada tingkat pengambilan sampel yang terlalu tinggi, codec akan mengeluarkan banyak energi dan hanya mendapatkan sedikit keuntungan dalam resolusi rekonstruksi bentuk gelombang. Seringkali, sistem codec menghasilkan terlalu sedikit sampel menggunakan laju pengambilan sampel yang rendah yang merekonstruksi bentuk gelombang yang bukan merupakan reproduksi akurat dari aslinya.

Lalu, bagaimana keseimbangan optimal antara tingkat pengambilan sampel yang terlalu tinggi dan terlalu rendah? Menurut teorema komunikasi terkenal yang dibuat oleh Nyquist, laju pengambilan sampel menggunakan modulasi kode pulsa harus dua kali frekuensi tertinggi bentuk gelombang analog asli untuk memastikan reproduksi yang wajar. Dengan menggunakan sistem telepon sebagai contoh dan dengan asumsi frekuensi suara tertinggi yang mungkin adalah 3400 Hz, laju pengambilan sampel harus 6800 sampel per detik untuk memastikan reproduksi bentuk gelombang analog yang wajar. Sistem telepon sebenarnya mengalokasikan saluran 4000-Hz untuk sinyal suara, dan dengan demikian mengambil sampel sebanyak 8000 kali per detik.

Modulasi Delta

Metode kedua konversi sinyal data analog ke digital adalah modulasi delta. Gambar 2.24 menunjukkan sebuah contoh. Dengan modulasi delta, codec melacak data analog yang masuk dengan menilai “langkah” naik atau turun. Selama setiap periode waktu, codec menentukan apakah bentuk gelombang telah naik satu langkah delta atau turun satu langkah delta. Jika bentuk gelombang naik satu langkah delta, angka 1 ditransmisikan.

Jika bentuk gelombang turun satu langkah delta, 0 dikirimkan. Dengan teknik pengkodean ini, hanya 1 bit per sampel yang dihasilkan. Dengan demikian, konversi dari analog ke digital menggunakan modulasi delta lebih cepat dibandingkan dengan modulasi kode pulsa, di mana setiap nilai analog terlebih dahulu diubah menjadi nilai PAM, kemudian nilai PAM diubah menjadi biner.



Gambar 2.24 Contoh modulasi delta yang mengalami derau beban berlebih lereng dan derau kuantisasi

Ada dua masalah yang melekat pada modulasi delta. Jika bentuk gelombang analog naik atau turun terlalu cepat, codec mungkin tidak dapat mengikuti perubahan tersebut, dan menimbulkan kebisingan kelebihan beban. Bagaimana jika perangkat mencoba mendigitalkan suara atau musik yang mempertahankan frekuensi dan amplitudo konstan, seperti seseorang menyanyikan satu nada dengan volume tetap? Bentuk gelombang analog yang tidak berubah sama sekali menimbulkan masalah lain pada modulasi delta. Karena codec menghasilkan 1 atau 0 hanya untuk naik atau turun, bentuk gelombang yang tidak berubah menghasilkan pola 1010101010 . . . , sehingga menghasilkan kuantisasi kebisingan. Gambar 2.24 menunjukkan modulasi delta dan menunjukkan kebisingan kelebihan beban lereng dan kebisingan kuantisasi.

2.4 KODE DATA

Salah satu bentuk data paling umum yang dikirimkan antara pemancar dan penerima adalah data tekstual. Misalnya, lembaga perbankan yang ingin mentransfer uang sering kali mengirimkan informasi tekstual, seperti nomor rekening, nama pemilik rekening, nama bank, alamat, dan jumlah uang yang akan ditransfer. Informasi tekstual ini ditransmisikan sebagai rangkaian karakter.

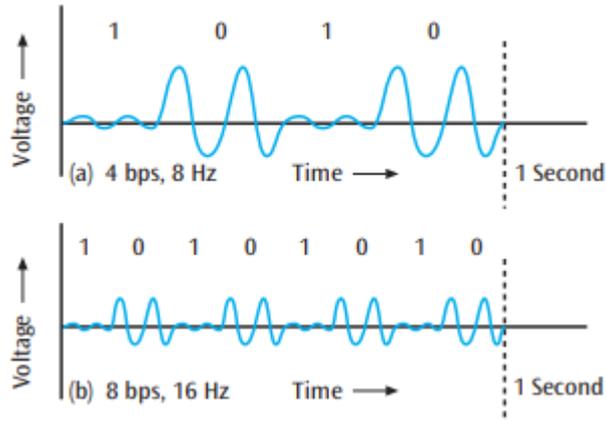
Hubungan Antara Frekuensi dan Bit per Detik

“Mengapa jaringan ini sangat lambat? Butuh waktu lama untuk mengunduhnya!” Ketika aplikasi jaringan lambat, pengguna sering kali meminta seseorang, seperti spesialis jaringan, melakukan sesuatu untuk membuat segalanya berjalan lebih cepat. Apa yang banyak pengguna jaringan tidak pahami adalah jika Anda ingin mengirim data dengan kecepatan lebih cepat, salah satu dari dua hal ini harus diubah:

- (1) data harus dikirimkan dengan sinyal frekuensi yang lebih tinggi, atau
- (2) lebih banyak bit per baud harus ditransmisikan. Selain itu, solusi ini tidak akan berhasil kecuali media yang mentransmisikan sinyal mampu mendukung frekuensi yang lebih tinggi. Untuk mulai memahami semua saling ketergantungan ini, akan sangat membantu jika kita memahami hubungan antara bit per detik dan frekuensi sinyal, dan dapat menggunakan dua ukuran sederhana teorema Nyquist dan teorema Shannon—untuk menghitung kecepatan transfer data. dari suatu sistem.

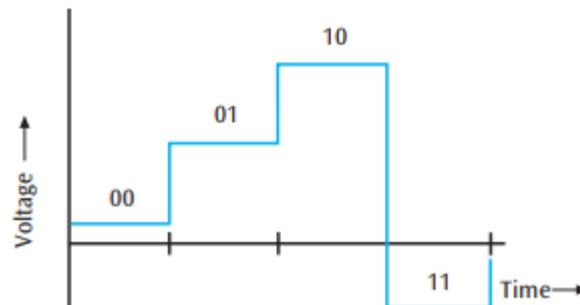
Ada hubungan penting antara frekuensi sinyal dan jumlah bit yang dapat disampaikan sinyal per detik: Semakin besar frekuensi sinyal, semakin tinggi kemungkinan kecepatan transfer data. Hal sebaliknya juga berlaku: Semakin tinggi kecepatan transfer data yang diinginkan, semakin besar pula frekuensi sinyal yang dibutuhkan. Anda dapat melihat hubungan langsung antara frekuensi sinyal dan kecepatan transfer (dalam bit per detik, atau bps) data yang dapat dibawa oleh sinyal. Pertimbangkan pengkodean modulasi amplitudo, yang ditunjukkan dua kali pada Gambar 2.25, dari bit string 1010 Pada bagian pertama Gambar 2.25, sinyal (amplitudo) berubah empat kali selama periode satu detik (baud rate sama dengan 4). Frekuensi sinyal ini adalah 8 Hz (delapan siklus lengkap dalam satu detik), dan kecepatan transfer data adalah 4 bps. Pada bagian kedua gambar, sinyal berubah amplitudo delapan kali (baud rate sama dengan 8) selama periode satu detik. Frekuensi sinyalnya adalah 16 Hz, dan

kecepatan transfer datanya adalah 8 bps. Ketika frekuensi sinyal meningkat, kecepatan transfer data (dalam bps) meningkat.



Gambar 2.25 Perbandingan frekuensi sinyal dengan bit per detik

Contoh ini sederhana karena hanya berisi dua level sinyal (amplitudo), satu untuk biner 0 dan satu lagi untuk biner 1. Bagaimana jika kita memiliki teknik pengkodean dengan empat level sinyal, seperti yang ditunjukkan pada Gambar 2.26? Karena ada empat level sinyal, setiap level sinyal dapat mewakili 2 bit. Lebih tepatnya, level sinyal pertama dapat mewakili biner 00, level sinyal kedua adalah biner 01, level sinyal ketiga adalah biner 10, dan level sinyal keempat adalah biner 11. Sekarang ketika level sinyal berubah, 2 bit data akan ditransfer.



Gambar 2.26 Teknik pensinyalan hipotetis dengan empat level sinyal

Dua rumus mengungkapkan hubungan langsung antara frekuensi sinyal dan kecepatan transfer datanya: teorema Nyquist dan teorema Shannon. Teorema Nyquist menghitung kecepatan transfer data suatu sinyal menggunakan frekuensinya dan jumlah level sinyal

$$\text{Data Rate} = 2 \times f \times \log_2(L)$$

dimana kecepatan data dalam bit per detik (kapasitas saluran), f adalah frekuensi sinyal, dan L adalah jumlah level sinyal. Misalnya, dengan sinyal 3100 Hz dan dua level sinyal (seperti amplitudo tinggi dan amplitudo rendah), kapasitas saluran yang dihasilkan adalah 6200 bps,

yang dihasilkan dari $2 \times 3100 \times \log_2(2) = 2 \times 3100 \times 1$. Hati-hati menggunakan \log_2 dan bukan \log_{10} . Sinyal 3100 Hz dengan empat level sinyal menghasilkan 12.400 bps. Perhatikan lebih lanjut bahwa rumus Nyquist tidak memasukkan kebisingan, yang selalu ada. (Rumus Shannon, yang ditunjukkan di bawah, dapat melakukan hal tersebut.) Oleh karena itu, banyak orang yang menggunakan rumus Nyquist bukan untuk mencari kecepatan data, melainkan, berdasarkan kecepatan data dan frekuensi, untuk mencari jumlah level sinyal L.

Teorema Shannon menghitung kecepatan transfer data maksimum dari sinyal analog (dengan sejumlah level sinyal) dan menggabungkan noise

$$\text{Data Rate} = 2 \times f \times \log_2(1 + S/N)$$

dimana kecepatan data dalam bit per detik, f adalah frekuensi sinyal, S adalah kekuatan sinyal dalam watt, dan N adalah kekuatan noise dalam watt.

Misalkan sinyal 3100 Hz dengan tingkat daya 0,2 watt dan tingkat kebisingan 0,0002 watt:

$$\begin{aligned} \text{Data Rate} &= 3100 \times \log_2\left(1 + \frac{0.2}{0.0002}\right) \\ &= 3100 \times \log_2(1001) \\ &= 3100 \times 9.97 \\ &= 30.901 \text{ bps} \end{aligned}$$

(Jika kalkulator Anda tidak memiliki kunci \log_2 , seperti kebanyakan kalkulator lainnya, Anda selalu dapat memperkirakan jawabannya dengan mengambil \log_{10} lalu membaginya dengan 0,301.)

Untuk membedakan satu karakter dengan karakter lainnya, setiap karakter diwakili oleh pola biner unik 1 dan 0. Himpunan semua karakter tekstual atau simbol dan pola biner terkaitnya disebut kode data. Tiga kode data penting adalah EBCDIC, ASCII, dan Unicode. Mari kita periksa masing-masing secara berurutan.

EBCDIC

Kode Pertukaran Desimal Berkode Biner yang Diperluas, atau EBCDIC, adalah kode 8-bit yang memungkinkan 256 ($2^8 = 256$) kemungkinan kombinasi simbol tekstual. 256 kombinasi simbol tekstual ini mencakup semua huruf besar dan kecil, angka 0 hingga 9, sejumlah besar simbol khusus dan tanda baca, dan sejumlah karakter kontrol. Karakter kontrol, seperti linefeed (LF) dan carriage return (CR), memberikan kontrol antara prosesor dan perangkat input/output. Karakter kontrol tertentu memberikan kontrol transfer data antara sumber komputer dan komputer tujuan. Semua karakter EBCDIC ditunjukkan pada Gambar 2.27.

Bits	4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1		
	3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1		
	2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1		
	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1		
8	7	6	5																
0	0	0	0	NUL	SOH	STX	EXT	PF	HT	LC	DEL			SMM	VT	FF	CR	SO	SI
0	0	0	1	DLE	DC ₁	DC ₂	DC ₃	RES	NL	BS	IL	CAN	EM	CC		IFS	IGS	IHS	IUS
0	0	1	0	DS	SOS	FS		BYP	LF	EOB	PRE			SM			ENQ	ACK	BEL
0	0	1	1			SYN		PN	RS	UC	EOT					DC ₄	NAK		SUB
0	1	0	0	SP												<	(+	
0	1	0	1	&										!	\$.)	:	⌋
0	1	1	0	—												%	-	>	?
0	1	1	1												@		=	"	
1	0	0	0		a	b	c	d	e	f	g	h	i						
1	0	0	1		j	k	l	m	n	o	p	q	r						
1	0	1	0			s	t	u	v	w	x	y	z						
1	0	1	1																
1	1	0	0		A	B	C	D	E	F	G	H	I						
1	1	0	1		J	K	L	M	N	O	P	Q	R						
1	1	1	0			S	T	U	V	W	X	Y	Z						
1	1	1	1	0	1	2	3	4	5	6	7	8	9						

Gambar 2.27 Kumpulan kode karakter EBCDIC

Misalnya, jika Anda ingin komputer mengirim pesan “Transfer \$1200.00” menggunakan EBCDIC, karakter berikut akan dikirimkan:

```

1110 0011    T
1001 1001    r
1000 0001    a
1001 0101    n
1010 0010    s
1000 0110    f
1000 0101    e
1001 1001    r
0100 0000    spasi
0101 1011    $
1111 0001    1
1111 0010    2
1111 0000    0
1111 0000    0
0101 1100    0
1111 0000    0
1111 0000    0
    
```

Komputer mainframe IBM adalah pengguna utama rangkaian karakter EBCDIC.

ASCII

American Standard Code for Information Interchange (ASCII) adalah standar pemerintah di Amerika Serikat dan merupakan salah satu kode data yang paling banyak digunakan di dunia. Kumpulan karakter ASCII ada dalam beberapa bentuk berbeda, termasuk

versi 7-bit yang memungkinkan 128 ($2^7 = 128$) kemungkinan kombinasi simbol tekstual, mewakili huruf besar dan kecil, angka 0 hingga 9, simbol khusus, dan karakter kontrol. Karena byte, yang terdiri dari 8 bit, adalah unit data yang umum, karakter ASCII versi 7-bit biasanya menyertakan bit kedelapan. Bit kedelapan ini dapat digunakan untuk mendeteksi kesalahan transmisi (topik yang akan dibahas pada Bab Enam). Ini dapat menyediakan 128 karakter tambahan yang ditentukan oleh aplikasi menggunakan kumpulan kode ASCII, atau bisa juga berupa biner 0. Gambar 2.28 menunjukkan kumpulan karakter ASCII dan nilai 7-bit yang sesuai.

		High-Order Bits (7, 6, 5)							
		000	001	010	011	100	101	110	111
Low-Order Bits (4, 3, 2, 1)	0000	NUL	DLE	SPACE	0	@	P	`	p
	0001	SOH	DC1	!	1	A	Q	a	q
	0010	STX	DC2	"	2	B	R	b	r
	0011	ETX	DC3	#	3	C	S	c	s
	0100	EOT	DC4	\$	4	D	T	d	t
	0101	ENQ	NAK	%	5	E	U	e	u
	0110	ACK	SYN	&	6	F	V	f	v
	0111	BEL	ETB	'	7	G	W	g	w
	1000	BS	CAN	(8	H	X	h	x
	1001	HT	EM)	9	I	Y	i	y
	1010	LF	SUB	*	:	J	Z	j	z
	1011	VT	ESC	+	:	K	[k	{
	1100	FF	FS	,	<	L	\	l	
	1101	CR	GS	-	=	M]	m	}
	1110	SO	RS	.	>	N	^	n	~
	1111	SI	US	/	?	O	_	o	DEL

Gambar 2.28 Kumpulan kode karakter ASCII

Untuk mengirim pesan "Transfer \$1200.00" menggunakan ASCII, karakter yang sesuai adalah:

```

1010100 T
1110010 r
1100001 a
1101110 n
1110011 s
1100110 f
1100101 e
1110010 r
0100000 spasi
0100100 $
0110001 1
0110010 2
0110000 0
0110000 0

```

```

0101110 .
0110000 0
0110000 0

```

Unikode

Salah satu masalah utama EBCDIC dan ASCII adalah keduanya tidak dapat mewakili simbol selain yang ditemukan dalam bahasa Inggris. Lebih jauh lagi, mereka bahkan tidak dapat mewakili semua jenis simbol dalam bahasa Inggris, seperti banyak simbol teknis yang digunakan dalam bidang teknik dan matematika. Dan bagaimana jika kita ingin mewakili bahasa lain di seluruh dunia? Untuk ini, yang kita butuhkan adalah teknik pengkodean yang lebih canggih Unicode.

Kembali ke contoh pengiriman pesan teks, jika Anda mengirim “Transfer \$1200.00” menggunakan Unicode, karakter yang sesuai adalah:

```

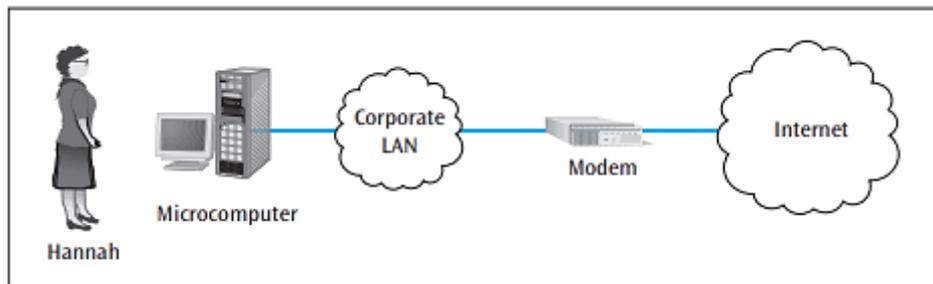
0000 0000 0101 0100    T
0000 0000 0111 0010    r
0000 0000 0110 0001    a
0000 0000 0110 1110    n
0000 0000 0111 0011    s
0000 0000 0110 0110    f
0000 0000 0110 0101    e
0000 0000 0111 0010    r
0000 0000 0010 0000    spasi
0000 0000 0010 0100    $
0000 0000 0011 0001    1
0000 0000 0011 0010    2
0000 0000 0011 0000    0
0000 0000 0011 0000    0
0000 0000 0010 1110    .
0000 0000 0011 0000    0
0000 0000 0011 0000    0

```

Unikode adalah teknik pengkodean yang memberikan nilai pengkodean unik untuk setiap karakter dalam setiap bahasa, apa pun platformnya. Saat ini, Unicode mendukung lebih dari 110 bagan kode berbeda (bahasa dan kumpulan simbol). Misalnya, simbol Yunani β memiliki nilai Unicode heksadesimal 03B2 (biner 0000 0011 1011 0010). Bahkan ASCII adalah salah satu grafik kode yang didukung. Banyak perusahaan komputer besar seperti Apple, HP, IBM, Microsoft, Oracle, Sun, dan Unisys telah mengadopsi Unicode, dan banyak perusahaan lain yang merasa bahwa penerimaannya akan terus meningkat seiring berjalannya waktu. Ketika industri komputer menjadi pasar global, Unicode akan terus menjadi semakin penting. Karena Unicode sangat besar, kami tidak akan menampilkannya di sini. Jika Anda tertarik, Anda dapat melihat situs Web Unicode di www.unicode.org.

KONVERSI DATA DAN SINYAL BERAksi: DUA CONTOH

Mari kita periksa dua aplikasi bisnis yang umum di mana berbagai konversi data dan sinyal dilakukan untuk melihat bagaimana data analog dan digital, sinyal analog dan digital, dan kode data bekerja sama. Pertama, pertimbangkan seseorang di tempat kerja yang ingin mengirim email ke rekan kerjanya, menanyakan waktu pertemuan berikutnya. Untuk mempermudah, mari kita asumsikan pesannya berbunyi, “Sam, jam berapa rapat bagian akuntansi? Hannah” dan dikirim dari komputer mikro yang terhubung ke jaringan area lokal, yang kemudian terhubung ke Internet. Kita anggap saja ini adalah bisnis kecil, sehingga koneksi ke Internet dilakukan melalui DSL (Gambar 2.29).

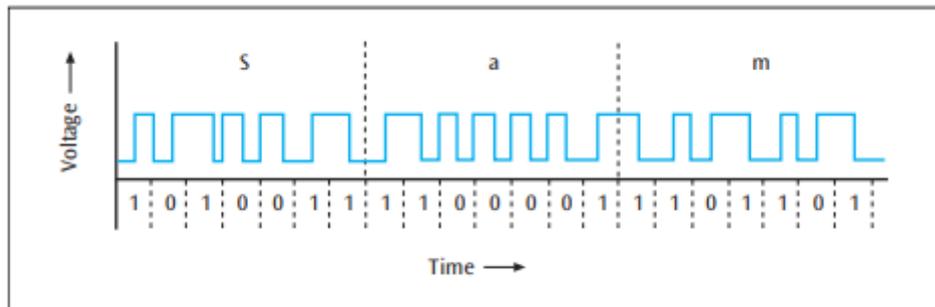


Gambar 2.29 Pengguna mengirim email dari komputer mikro melalui jaringan area lokal yang terhubung ke Internet

Hannah memasukkan pesan ke dalam program email dan mengklik ikon Kirim. Program email menyiapkan pesan email yang berisi data “Sam, jam berapa rapat dengan bagian akuntansi? Hannah” ditambah informasi lain apa pun yang diperlukan agar program email dapat mengirim pesan dengan benar. Karena program email ini menggunakan ASCII, teks pesan ini diubah menjadi berikut ini:

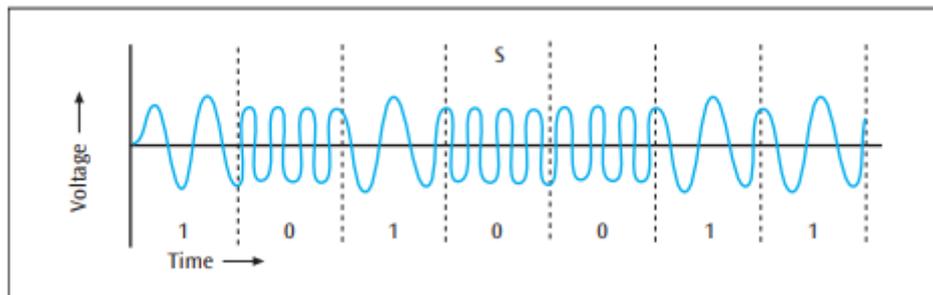
Original message:	Sam, what time is the meeting with accounting?	
ASCII string:	1010011 1100001 1101101 . . .	Hannah (For brevity, only the "Sam" portion of the message appears here in ASCII.)
	S a m	

Selanjutnya, pesan ASCII dikirimkan melalui jaringan area lokal di dalam perusahaan. Asumsikan LAN ini menggunakan pengkodean diferensial Manchester. String ASCII sekarang muncul sebagai sinyal digital, seperti yang ditunjukkan pada Gambar 2-30.



Gambar 2.30 Tiga huruf pertama dari pesan “Sam, jam berapa rapat bagian akuntansi? Hannah” menggunakan pengkodean diferensial Manchester

Pengkodean pesan Manchester diferensial ini berjalan melalui jaringan area lokal dan tiba di komputer lain, yang terhubung ke modem DSL. Komputer ini mengubah pesan kembali menjadi string ASCII dan kemudian mengirimkan string ASCII ke modem. Modem mempersiapkan pesan untuk transmisi melalui Internet, menggunakan modulasi frekuensi (modulasi DSL jauh lebih kompleks dari itu, tapi ini sudah cukup untuk saat ini). Untuk singkatnya, hanya 7 bit pertama dari string ASCII (dalam hal ini, sesuai dengan “Sd” di Sam) yang dikonversi menggunakan penguncian pergeseran frekuensi sederhana (Gambar 2.31).



Gambar 2.31 Sinyal termulasi frekuensi untuk huruf “S”

Sinyal termulasi frekuensi ini berjalan melalui saluran telepon dan tiba di gateway Internet yang sesuai (penyedia layanan Internet), yang mendemodulasi sinyal tersebut menjadi string ASCII. Dari sana, string ASCII yang mewakili pesan asli berpindah ke Internet dan akhirnya sampai di komputer penerima yang dituju. Proses transmisi melalui Internet dan penyampaian pesan ke komputer penerima yang dituju melibatkan beberapa konversi kode lagi. Karena kita belum membahas apa yang terjadi melalui Internet, dan kita juga belum mengetahui jenis koneksi yang dimiliki receiver, bagian contoh ini dihilangkan. Namun demikian, contoh yang relatif sederhana ini menunjukkan berapa kali konversi dari data ke sinyal ke data dilakukan selama transfer pesan.

Contoh kedua melibatkan telepon biasa. Sistem telepon di Amerika Serikat merupakan perpaduan yang semakin kompleks antara saluran telepon analog tradisional dan teknologi digital modern. Satu-satunya bagian dari sistem telepon yang tetap analog adalah loop lokal—kabel yang meninggalkan rumah, apartemen, atau bisnis Anda dan menuju ke pusat peralihan telepon terdekat. Suara Anda, saat Anda berbicara di telepon, merupakan data analog yang

diubah menjadi sinyal analog yang disalurkan melalui kabel ke pusat peralihan lokal, di mana suara tersebut didigitalkan dan dikirimkan ke pusat peralihan lain di suatu tempat dalam jaringan telepon yang luas.

Karena suara manusia bersifat analog, namun sebagian besar sistem telepon bersifat digital, konversi sinyal analog-ke-digital seperti apa yang dilakukan? Seperti disebutkan sebelumnya dalam bab ini, suara manusia menempati frekuensi analog dari 300 Hz hingga 3400 Hz dan ditransmisikan melalui sistem telepon dengan bandwidth 4000 Hz (4 kHz). Ketika sinyal 4000 Hz ini mencapai kantor telepon lokal, sinyal tersebut diambil sampelnya pada frekuensi dua kali lipat terbesar (menurut teorema Nyquist), atau 8000 sampel per detik. Penelitian melalui telepon menunjukkan bahwa suara manusia dapat didigitalkan hanya dengan menggunakan 128 tingkat kuantisasi yang berbeda. Karena 27 sama dengan 128, masing-masing dari 8000 sampel per detik dapat diubah menjadi nilai 7-bit, menghasilkan 8000×7 , atau 56.000 bit per detik. Jika sinyal suara didigitalkan menggunakan 256 tingkat kuantisasi berbeda, maka akan menghasilkan sinyal 64.000-bps ($256 = 2^8$, 8×8000 menghasilkan 64.000). Bagaimana 64.000 bit per detik ini kemudian dikirim melalui kabel atau gelombang udara? Itu tergantung pada teknik modulasi yang dipilih. Aliran data berkecepatan rendah mungkin menggunakan modulasi frekuensi, sedangkan aliran data berkecepatan lebih tinggi mungkin menggunakan beberapa variasi modulasi amplitudo kuadratur. Ringkasnya, kami memulai dengan suara manusia analog, yang didigitalkan dan kemudian diubah kembali menjadi sinyal analog untuk transmisi. Dua contoh yang serupa dan umum adalah televisi kabel digital dan televisi siaran digital.

Seperti yang telah dinyatakan, untuk mengirimkan suara seseorang melalui sirkuit telepon, 128 tingkat kuantisasi sudah cukup. Namun bagaimana jika kita ingin membuat rekaman artis yang menyanyikan sebuah lagu dan bermain gitar? Dengan asumsi bahwa kita ingin membuat rekaman dengan kualitas yang cukup tinggi untuk dibakar pada CD, kita memerlukan lebih dari 128 tingkat kuantisasi yang berbeda. Faktanya, mendigitalkan sebuah lagu untuk dibakar ke dalam CD memerlukan ribuan, bahkan mungkin puluhan ribu, tingkat kuantisasi. Lebih tepatnya, CD musik memiliki laju pengambilan sampel 44,1 kHz dan menggunakan konversi 16-bit ($2^{16} = 65.536$ tingkat kuantisasi). Dengan demikian, sirkuit digitalisasi yang mengubah musik analog menjadi bentuk digital untuk disimpan pada CD secara teknis jauh lebih rumit daripada sirkuit yang digunakan untuk melakukan panggilan telepon sederhana.

RINGKASAN

- Data dan sinyal adalah dua blok dasar jaringan komputer. Semua data yang dikirimkan melalui media komunikasi apa pun bersifat digital atau analog. Data ditransmisikan dengan sinyal yang, seperti data, dapat berupa digital atau analog. Perbedaan paling penting antara data dan sinyal analog dan digital adalah lebih mudah menghilangkan noise dari data dan sinyal digital dibandingkan dari data dan sinyal analog.
- Semua sinyal terdiri dari tiga komponen dasar: amplitudo, frekuensi, dan fase.

- Dua faktor penting yang mempengaruhi transfer sinyal melalui media adalah noise dan redaman.
- Karena data dan sinyal dapat berupa digital atau analog, empat kombinasi dasar data dan sinyal dapat dilakukan: data analog diubah menjadi sinyal analog, data digital diubah menjadi sinyal digital, data digital diubah menjadi analog diskrit sinyal, dan data analog diubah menjadi sinyal digital.
- Untuk mengirimkan data analog melalui sinyal analog, bentuk gelombang analog dari data tersebut digabungkan dengan bentuk gelombang analog lainnya dalam proses yang dikenal sebagai modulasi.
- Data digital yang dibawa oleh sinyal digital diwakili oleh format pengkodean digital, termasuk skema pengkodean Manchester. Kode Manchester selalu mempunyai transisi di tengah-tengah bit, yang memungkinkan penerima untuk menyinkronkan dirinya dengan sinyal yang masuk.
- Agar data digital dapat ditransmisikan menggunakan sinyal analog diskrit, data digital terlebih dahulu harus melalui proses yang disebut shift keying. Tiga teknik dasar penguncian shift adalah penguncian pergeseran amplitudo, penguncian pergeseran frekuensi, dan penguncian pergeseran fasa.
- Dua teknik umum untuk mengkonversi data analog sehingga dapat dibawa melalui sinyal digital adalah modulasi kode pulsa dan modulasi delta. Modulasi kode pulsa mengubah sampel data analog menjadi nilai digital multi-bit. Modulasi Delta melacak data analog dan hanya mentransmisikan angka 1 atau 0, bergantung pada apakah data naik atau turun dalam periode waktu berikutnya.
- Kode data diperlukan untuk mengirimkan huruf, angka, simbol, dan karakter kontrol yang ditemukan dalam data teks. Tiga kode data penting adalah ASCII, EBCDIC, dan Unicode. Kode data EBCDIC menggunakan kode 8-bit dan memungkinkan 256 huruf, angka, dan simbol khusus yang berbeda. Mainframe IBM menggunakan kode EBCDIC. Kode data ASCII menggunakan kode 7-bit dan memungkinkan 128 huruf, angka, dan simbol khusus yang berbeda. ASCII adalah kode data paling populer di Amerika Serikat. Unicode adalah kode 16-bit yang mendukung lebih dari 110 bahasa dan kumpulan simbol berbeda dari seluruh dunia.

PERTANYAAN

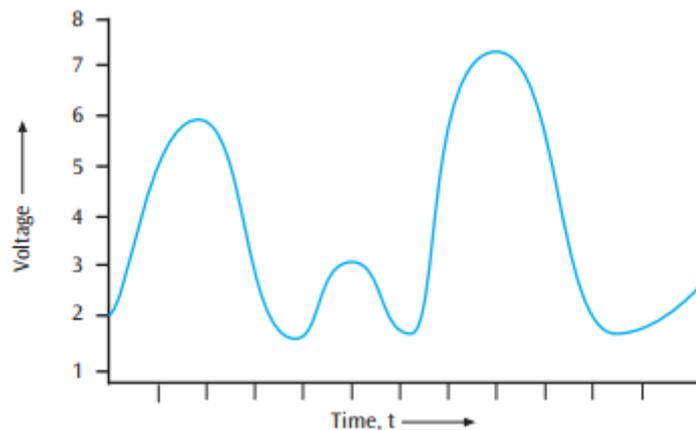
1. Apa perbedaan antara data dan sinyal?
2. Apa keunggulan utama sinyal digital dibandingkan sinyal analog?
3. Apa perbedaan antara sinyal kontinu dan sinyal diskrit?
4. Apa tiga komponen dasar dari semua sinyal?
5. Berapakah spektrum suatu sinyal?
6. Berapa bandwidth suatu sinyal?
7. Mengapa data analog harus dimodulasi menjadi sinyal analog?
8. Apa perbedaan kode diferensial seperti kode diferensial Manchester dengan kode nondiferensial seperti NRZ?

9. Apa yang dimaksud dengan sinyal yang melakukan self-clocking?
10. Apa definisi istilah “baud rate”?
11. Apa perbedaan baud rate dengan bit per detik?
12. Apa tiga jenis utama shift keying?
13. Apa perbedaan antara modulasi kode pulsa dan modulasi delta?
14. Apa yang dimaksud dengan sampling rate data analog?
15. Apa perbedaan EBCDIC, ASCII, dan Unicode?

LATIHAN

1. Berapa frekuensi dalam Hertz dari sinyal yang berulang 80.000 kali dalam satu menit? Berapa periodenya (panjang satu siklus penuh)?
2. Berapakah bandwidth suatu sinyal yang terdiri dari frekuensi dari 50 Hz hingga 500 Hz?
3. Gambarkan dalam bentuk grafik (seperti yang ditunjukkan pada Gambar 2-12) representasi tegangan dari pola bit 11010010 untuk skema pengkodean digital NRZ-L, NRZI, Manchester, differential Manchester, dan bipolar-AMI.
4. Berapa baud rate sinyal digital yang menggunakan differential Manchester dan memiliki kecepatan transfer data 2000 bps?
5. Tampilkan kode 4B/5B yang setara dengan string bit 1101 1010 0011 0001 1000 1001.
6. Berapa kecepatan transfer data dalam bps dari sinyal yang dikodekan menggunakan modulasi fase dengan delapan sudut fase berbeda dan baud rate 2000?
7. Jika modulasi amplitudo kuadratur digunakan untuk mengirimkan sinyal dengan baud rate 8000, berapa bit rate yang sesuai?
8. Gambarkan atau berikan contoh sinyal untuk masing-masing kondisi berikut: baud rate sama dengan bit rate, baud rate lebih besar dari bit rate, dan baud rate lebih kecil dari bit rate.
9. Sebuah sinyal dimulai dari titik X. Saat bergerak ke titik Y, sinyal tersebut kehilangan 8 dB. Di titik Y, sinyal diperkuat sebesar 10 dB. Saat sinyal bergerak ke titik Z, sinyal kehilangan 7 dB. Berapakah kekuatan dB sinyal di titik Z?
10. Pada soal sebelumnya, jika sinyal dimulai di titik X dengan kekuatan 100 watt, berapakah level daya sinyal di titik Z?
11. Gambarkan contoh sinyal (mirip dengan yang ditunjukkan pada Gambar 2-12) menggunakan NRZI dimana sinyal tidak pernah berubah selama 7 bit. Seperti apa bentuk pengkodean diferensial Manchester yang setara?
12. Tunjukkan pola gelombang sinus analog yang setara dari string bit 00110101 menggunakan penguncian pergeseran amplitudo, penguncian pergeseran frekuensi, dan penguncian pergeseran fasa.
13. Dua puluh empat sinyal suara harus dikirim melalui satu saluran telepon berkecepatan tinggi. Berapa bandwidth yang dibutuhkan (dalam bps) jika standar sampling rate analog-ke-digital digunakan dan setiap sampel diubah menjadi nilai 8-bit?

14. Mengingat sinyal analog yang ditunjukkan pada Gambar 2-32, berapakah nilai termodulasi kode pulsa 8-bit yang akan dihasilkan pada setiap waktu t ?
15. Dengan menggunakan sinyal analog dari Latihan 14 dan langkah delta yang panjangnya seperdelapan inci dan tinggi seperdelapan inci, berapakah keluaran modulasi delta? gambar modulasi delta, tunjukkan kebisingan beban berlebih pada lereng.
16. Dengan menggunakan kumpulan kode karakter EBCDIC, ASCII, dan Unicode, apa pengkodean biner dari pesan "Halo, dunia"?
17. Anda baru saja membuat sinyal termodulasi kode pulsa, tetapi ini bukan representasi yang baik dari data asli. Apa yang dapat Anda lakukan untuk meningkatkan keakuratan sinyal termodulasi?
18. Berapakah kerugian desibel suatu sinyal yang dimulai di titik A dengan kekuatan 2000 watt dan berakhir di titik B dengan kekuatan 400 watt?
19. Berapa kerugian desibel dari sinyal yang dimulai pada 50 watt dan mengalami kerugian 10 dB pada bagian kabel tertentu?
20. Berapakah hilangnya desibel suatu sinyal yang kehilangan separuh dayanya selama transmisi?



Gambar 2.32 Sinyal analog untuk Latihan 14

Latihan untuk bagian Detail:

21. Dengan menggunakan teorema Nyquist, hitung kecepatan transfer data dari suatu sinyal yang memiliki 16 level berbeda dan frekuensi 20.000 Hz.
22. Dengan menggunakan teorema Shannon, hitung kecepatan transfer data dengan informasi berikut:
 - a. frekuensi sinyal = 10.000 hz
 - b. daya sinyal = 5000 watt
 - c. daya kebisingan = 230 watt
23. Dengan menggunakan teorema Nyquist dan diberi frekuensi 5000 Hz dan kecepatan data 20.000 bps, berapa level sinyal (L) yang diperlukan untuk menyampaikan data ini?

Diskusikan Dengan Kelompok

1. Anda bekerja di perusahaan yang memiliki aplikasi jaringan untuk mengakses database profil perusahaan. Dari stasiun kerja komputer Anda, permintaan profil dikirim melalui jaringan area lokal perusahaan ke modem. Modem, menggunakan DSL, terhubung ke Internet dan akhirnya ke layanan database. Layanan database pada dasarnya adalah modem dan komputer mainframe. Buat tabel (atau gambar gambar) yang menunjukkan setiap kali data atau sinyal diubah ke bentuk berbeda dalam proses ini. Untuk setiap entri dalam tabel, tunjukkan tempat terjadinya konversi, bentuk informasi masuk, dan bentuk informasi keluar.
2. Sistem telepon dirancang untuk mengirimkan sinyal suara (4000 Hz). Ketika sinyal suara didigitalkan menggunakan modulasi kode pulsa, berapa laju pengambilan sampelnya, dan berapa tingkat kuantisasi yang digunakan? Berapa banyak data yang dihasilkan dalam satu detik? Apakah laju pengambilan sampel dan tingkat kuantisasinya sama seperti yang digunakan pada CD? Bisakah Anda memverifikasi jawaban Anda?
3. Jika saluran telepon dapat membawa sinyal dengan baud rate 6000 dan kita ingin mengirimkan data pada 33,600 bps, berapa banyak level sinyal berbeda yang diperlukan? Beginikah cara kerja modem 33.600 bps?
4. Apakah modem dan codec dapat digunakan secara bergantian? Pertahankan posisi Anda. (Modem mengubah data digital menjadi sinyal analog dan kembali ke data digital; codec mengubah data analog menjadi sinyal digital dan kembali ke data analog.)
5. Bab ini memperkenalkan skema pengkodean bipolar. Apa contoh skema pengkodean unipolar?
6. MegaCom adalah tipikal perusahaan dengan banyak pengguna, jaringan area lokal, akses Internet, dan sebagainya.

Seorang pengguna bekerja di rumah dan terhubung ke sistem email perusahaan. Gambarlah diagram linier koneksi dari komputer pribadi pengguna di rumah ke server email perusahaan di jaringan area lokal. Pada grafik linier ini, identifikasi setiap bentuk data dan sinyal. Apakah itu analog? Digital? Konversi data/sinyal apa yang terjadi? Di manakah konversi ini?

PROYEK LANGSUNG

1. Dengan menggunakan sumber dari perpustakaan atau Internet, tuliskan makalah setebal dua hingga tiga halaman yang menjelaskan bagaimana iPod atau pemutar CD melakukan konversi konten digital ke analog.
2. Ada lebih banyak skema pengkodean digital dibandingkan NRZ-L, NRZI, Manchester, differential Manchester, dan bipolar-AMI. Sebutkan tiga teknik pengkodean lainnya dan tunjukkan contoh bagaimana masing-masing teknik pengkodean.
3. Apa format pengkodean untuk televisi digital definisi tinggi yang baru? Apakah Amerika Serikat sudah menyepakati satu format, atau apakah ada beberapa format

lain? Apakah format ini sama dengan format yang digunakan di tempat lain di dunia? Menjelaskan.

4. Sistem telepon menggunakan skema pengkodean digital yang disebut B8ZS (diucapkan "bates"), yang merupakan variasi dari skema pengkodean bipolar-AMI. Bagaimana cara kerjanya? Mengapa ini digunakan? Tunjukkan contoh menggunakan string biner 01101100000000010.
5. Dapatkah Anda menemukan situs Web yang menunjukkan secara grafis hasil penambahan beberapa gelombang sinus untuk menghasilkan gelombang komposit seperti gelombang persegi atau gelombang gigi gergaji? Setelah Anda menemukan situs Web ini, gunakan alat online untuk membuat berbagai bentuk gelombang.
6. Berapa laju pengambilan sampel dan jumlah tingkat kuantisasi untuk iPod, pemutar CD, pemutar DVD-video, pemutar DVD-audio, dan pemutar Blu-ray?

BAB 3

MEDIA KONDUKTOR DAN NIRKABEL

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Uraikan ciri-ciri kawat twisted pair, termasuk kelebihan dan kekurangannya
- Uraikan perbedaan antara kabel twisted pair Kategori 1, 2, 3, 4, 5, 5e, 6, dan 7
- Jelaskan kapan kabel twisted pair berpelindung bekerja lebih baik daripada kabel twisted pair tidak berpelindung
- Uraikan ciri-ciri, kelebihan dan kekurangan kabel koaksial dan kabel serat optik
- Menguraikan karakteristik sistem gelombang mikro terestrial, termasuk kelebihan dan kekurangannya
- Menguraikan karakteristik sistem gelombang mikro satelit, termasuk kelebihan dan kekurangan serta perbedaan antara satelit orbit Bumi rendah, orbit Bumi tengah, orbit geosinkron, dan satelit orbit Bumi sangat elips
- Jelaskan dasar-dasar telepon seluler, termasuk semua sistem seluler generasi saat ini
- Uraikan karakteristik transmisi jarak pendek, termasuk Bluetooth
- Jelaskan karakteristik, kelebihan, dan kekurangan sistem nirkabel broadband dan berbagai teknik transmisi jaringan area lokal nirkabel
- Menerapkan kriteria pemilihan media berupa biaya, kecepatan, hak jalan, perluasan dan jarak, lingkungan, dan keamanan ke berbagai media dalam aplikasi tertentu

TIDAK yakin ponsel sudah menjadi bagian tak terpisahkan dari kehidupan sehari-hari? Mari kita periksa contoh berita utama dari Internet sehubungan dengan penggunaan telepon seluler.

Menurut beberapa angka terkini, pasar ponsel mencapai 5 miliar pelanggan pada tahun 2011. Menurut laporan AP, Anda sekarang dapat (jika Anda tidak memiliki uang receh di saku Anda) menggunakan ponsel Anda untuk mengisi meteran parkir di Coral Gables, Florida. Kota ini menjadi kota pertama yang menggunakan Cell-Park, sebuah metode pembayaran baru yang memungkinkan pengemudi untuk “menelepon” ke meteran dari ponsel mereka.

Anda cukup memasukkan nomor yang ditetapkan untuk tempat parkir Anda, dan meteran tidak akan kedaluwarsa sampai Anda menelepon lagi dan keluar. Nada dering ponsel yang meniru suara sepeda motor telah dibuat menjadi CD dan sangat populer sehingga penjualannya melebihi banyak lagu-lagu hits di tangga lagu Inggris. Ini adalah pertama kalinya nada dering masuk ke tangga lagu single dan mencapai posisi nomor satu di Inggris.

Sekarang hewan peliharaan Anda dapat memiliki ponselnya sendiri. Ponsel khusus sedang dibuat yang dapat dikenakan di leher anjing dan kucing. Ini memungkinkan pemilik hewan peliharaan untuk menelepon dan berbicara dengan hewan peliharaannya saat mereka

sedang bekerja atau berlibur. Ponsel ini juga dilengkapi GPS sehingga pemiliknya selalu mengetahui di mana hewan peliharaannya berada dan menemukannya jika mereka melarikan diri.

Dalam jajak pendapat yang dilakukan Joel Benenson, lebih dari 50 persen dari 1.013 remaja yang disurvei mengatakan mereka mengenal seseorang yang pernah menggunakan ponsel untuk berbuat curang di sekolah.

Apakah ponsel Anda merupakan aksesori yang diperlukan saat Anda keluar rumah?

Tahukah Anda teknologi nirkabel apa yang digunakan ponsel Anda?

Apa sajakah penerapan teknologi nirkabel selain telepon seluler?

3.1 PENDAHULUAN

Dunia jaringan komputer tidak akan ada jika tidak ada media yang digunakan untuk mentransfer data. Semua media komunikasi dapat dibagi menjadi dua kategori: (1) media fisik atau terkonduksi, seperti saluran telepon dan kabel serat optik, dan (2) media terpancar atau nirkabel, seperti telepon seluler dan sistem satelit. Media penghantar antara lain kawat twisted pair, kabel koaksial, dan kabel serat optik. Selain menyelidiki masing-masing hal tersebut, bab ini juga mengkaji tujuh kelompok dasar media nirkabel yang digunakan untuk transfer data:

- Gelombang mikro terestrial
- Transmisi satelit
- Sistem telepon seluler
- Layanan distribusi nirkabel broadband
- Bluetooth
- Sistem jaringan area lokal nirkabel
- Optik ruang bebas, ultra-wideband, inframerah, dan ZigBee

Urutan pembahasan topik nirkabel kira-kira sesuai dengan urutan popularitas teknologi tersebut.

Saat Anda membaca paragraf ini, pasti ada seseorang di suatu tempat yang sedang merancang material baru dan membuat peralatan baru yang lebih baik dari yang ada saat ini. Kecepatan dan jarak transmisi yang diberikan dalam bab ini akan terus berkembang. Harap ingat hal ini saat Anda mempelajari media.

Bab ini diakhiri dengan perbandingan seluruh jenis media, diikuti dengan beberapa contoh yang menunjukkan cara memilih media yang sesuai untuk aplikasi tertentu.

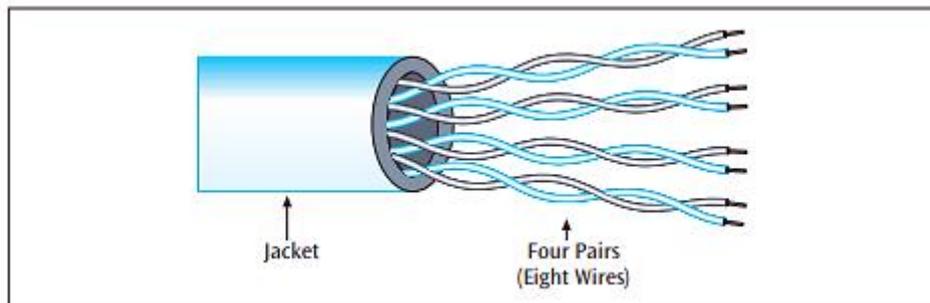
3.2 MEDIA YANG DILAKUKAN

Meskipun media yang dilakukan sudah ada sejak telepon itu sendiri (bahkan lebih lama lagi jika Anda memasukkan telegraf), hanya ada sedikit tambahan terbaru atau unik pada teknologi ini. Anggota terbaru dari keluarga media—kabel serat optik—mulai digunakan secara luas oleh perusahaan telepon pada tahun 1980an dan oleh perancang jaringan komputer pada tahun 1990an. Namun mari kita mulai pembahasan kita tentang tiga jenis

media konduksi yang ada dengan media tertua, paling sederhana, dan paling umum: kabel twisted pair.

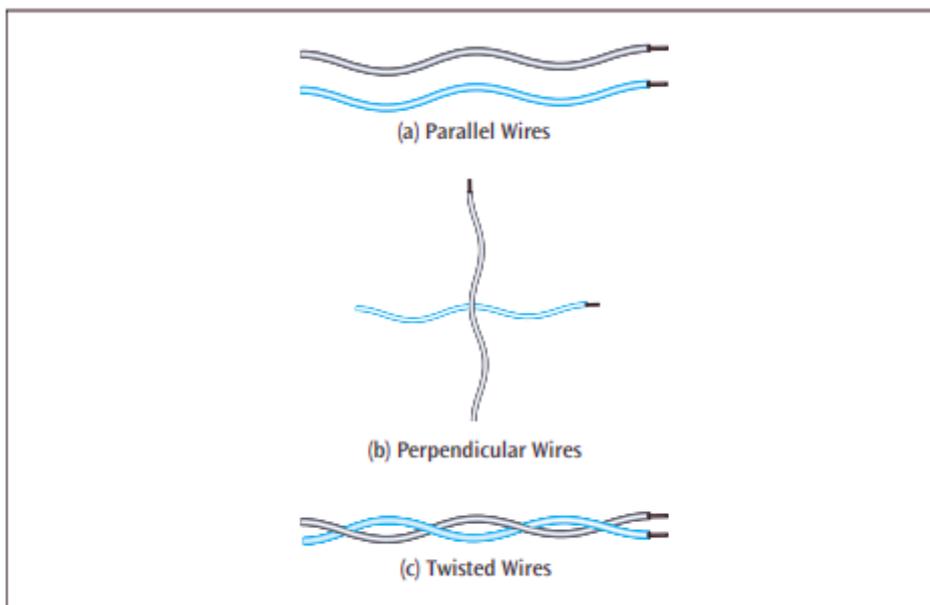
Kawat twisted pair

Istilah “twisted pair” hampir merupakan istilah yang keliru, karena jarang sekali kita menemukan sepasang kabel. Lebih sering, kabel twisted pair hadir sebagai dua atau lebih pasang kabel tembaga konduktor tunggal yang telah dipilin satu sama lain. Setiap kawat konduktor tunggal dibungkus dalam isolasi plastik dan dikabelkan dalam satu jaket luar, seperti yang ditunjukkan pada Gambar 3-1.



Gambar 3.1 Contoh kawat twisted pair empat pasang

Kecuali jika seseorang melepaskan selubung luarnya, Anda mungkin tidak akan melihat puntiran kabel, yang dilakukan untuk mengurangi jumlah interferensi yang dapat ditimbulkan oleh satu kabel pada kabel lainnya, sepasang kabel dapat menimbulkan pada pasangan kabel lainnya, dan kabel eksternal. sumber elektromagnetik dapat menimpa satu kabel secara berpasangan.



Gambar 3.2 (a) Kabel paralel; kemungkinan terjadinya crosstalk lebih besar (b) Kabel tegak lurus; lebih kecil kemungkinan terjadinya crosstalk (c) Kabel terpuntir; crosstalk berkurang karena kabel terus bersilangan pada sudut yang hampir tegak lurus

Anda mungkin ingat dua hukum penting dalam fisika: (1) Arus yang melewati kawat menciptakan medan magnet di sekitar kawat tersebut, dan (2) medan magnet yang melewati kawat menginduksi arus pada kawat tersebut. Oleh karena itu, arus atau sinyal pada satu kabel dapat menghasilkan arus atau sinyal yang tidak diinginkan, yang disebut crosstalk, pada kabel kedua. Jika kedua kabel dipasang sejajar satu sama lain, seperti ditunjukkan pada Gambar 3.2(a), peluang terjadinya crosstalk meningkat. Jika kedua kabel saling bersilangan dan membentuk sudut tegak lurus, seperti ditunjukkan pada Gambar 3.2(b), peluang terjadinya crosstalk berkurang. Meskipun tidak benar-benar menghasilkan sudut tegak lurus, pelintiran dua kabel di sekeliling satu sama lain, seperti ditunjukkan pada Gambar 3.2(c), setidaknya menjaga agar kabel tidak sejajar dan dengan demikian membantu mengurangi crosstalk.

Anda mungkin pernah mengalami crosstalk berkali-kali. Ingatkah saat Anda sedang berbicara di telepon dan mendengar percakapan yang samar-samar di latar belakang? Sambungan atau sirkuit telepon Anda mengalami crosstalk dari sirkuit telepon lain. Meskipun terlihat sederhana, kawat twisted pair sebenarnya hadir dalam berbagai bentuk dan variasi untuk mendukung berbagai aplikasi. Untuk membantu mengidentifikasi berbagai jenis kawat twisted pair, spesifikasi yang dikenal sebagai Kategori 1.7, disingkat CAT 1.7, telah dikembangkan. Pasangan terpilin kategori 1 adalah kabel telepon standar dan memiliki sedikit atau tanpa lilitan. Oleh karena itu, kebisingan elektromagnetik lebih merupakan masalah. Itu diciptakan untuk membawa suara atau data analog dengan kecepatan rendah (kurang dari atau sama dengan 9600 bps). Kabel twisted pair kategori 1 jelas tidak dirancang untuk kecepatan megabit saat ini dan tidak boleh digunakan untuk jaringan area lokal atau saluran telepon modern. Kabel twisted pair kategori 2 juga digunakan untuk sirkuit telepon dan beberapa LAN berkecepatan rendah tetapi memiliki beberapa puntiran, sehingga menghasilkan lebih sedikit noise. Pasangan terpilin kategori 2 kadang-kadang ditemukan pada jalur T-1 dan ISDN dan di beberapa instalasi sirkuit telepon standar. T-1 adalah sebutan untuk rangkaian telepon digital yang mentransmisikan suara atau data dengan kecepatan 1,544 Mbps. ISDN merupakan rangkaian telepon digital yang dapat mengirimkan suara atau data atau keduanya dari 64 kbps hingga 1,544 Mbps. (Bab Sebelas memberikan penjelasan yang lebih rinci tentang T-1.) Sekali lagi, kemajuan dalam kawat pasangan terpilin seperti penggunaan lebih banyak lilitan menyebabkan kawat Kategori 2 diganti dengan kawat berkualitas lebih tinggi, sehingga sangat sulit untuk menemukan siapa pun yang masih menjual kawat ini. Namun meskipun mereka menjualnya, Anda tidak akan pernah menggunakannya untuk jaringan modern.

Pasangan terpilin kategori 3 dirancang untuk mengirimkan data 10 Mbps melalui jaringan area lokal untuk jarak hingga 100 meter (328 kaki). (Perhatikan bahwa satuan yang biasanya digunakan untuk menentukan media konduksi adalah metrik bila diperlukan, padanan dalam bahasa Inggris akan disediakan.) Meskipun sinyal tidak secara ajaib berhenti pada jarak 100 meter, sinyal tersebut melemah (*attenuate*), dan tingkat kebisingan terus bertambah sehingga kemungkinan kesalahan transmisi kabel setelah 100 meter meningkat. Batasan tidak lebih dari 100 meter berlaku untuk jarak dari perangkat penghasil sinyal (sumber) ke perangkat penerima sinyal (tujuan). Perangkat penerima ini dapat menjadi tujuan

akhir atau pengulang. Repeater adalah perangkat yang menghasilkan sinyal baru dengan membuat replika yang sama persis dengan sinyal aslinya. Dengan demikian, twisted pair Kategori 3 dapat berjalan lebih jauh dari 100 meter dari sumbernya ke tujuan akhirnya, asalkan sinyalnya dibuat ulang setidaknya setiap 100 meter. Sebagian besar kabel Kategori 3 yang dijual saat ini digunakan untuk sirkuit telepon sederhana daripada instalasi jaringan komputer. Namun, mungkin ada beberapa instalasi jaringan komputer lama yang masih menggunakan kabel Kategori 3. Pemasangan kabel Kategori 3 baru untuk jaringan tidak disarankan.

Twisted pair kategori 4 dirancang untuk mengirimkan data 20 Mbps untuk jarak hingga 100 meter. Ini dibuat pada saat jaringan area lokal memerlukan kabel yang dapat mengirimkan data lebih cepat daripada kecepatan 10 Mbps Kategori 3. Kabel kategori 4 jarang, jika pernah, dijual lagi, dan pada dasarnya telah diganti dengan jenis kabel twisted yang lebih baru. pasangan.

Twisted pair kategori 5 dirancang untuk mengirimkan data 100 Mbps untuk jarak hingga 100 meter. (Secara teknis, Kategori 5 ditentukan untuk sinyal 100 MHz, namun karena sebagian besar sistem mengirimkan 100 Mbps melalui sinyal 100 MHz, 100 MHz setara dengan 100 Mbps.) Pasangan terpilin kategori 5 memiliki jumlah lilitan per inci yang lebih tinggi daripada kabel Kategori 1 hingga 4 dan, dengan demikian, menimbulkan lebih sedikit kebisingan.

Disetujui pada akhir tahun 1999, spesifikasi untuk pasangan terpilin Kategori 5e mirip dengan Kategori 5 karena kabel ini juga direkomendasikan untuk transmisi 100 Mbps (100 MHz) untuk jarak 100 meter. Banyak perusahaan yang memproduksi kabel Kategori 5e pada 125 MHz sepanjang 100 meter. Meskipun spesifikasi untuk kabel Kategori 1 hingga 5 sebelumnya hanya menjelaskan masing-masing kabel, spesifikasi Kategori 5e menunjukkan empat pasang kabel dan memberikan sebutan untuk konektor pada ujung kabel, kabel patch, dan komponen lain yang mungkin diperlukan. terhubung langsung dengan kabel. Jadi, sebagai spesifikasi yang lebih rinci daripada Kategori 5, Kategori 5e dapat mendukung jaringan area lokal berkecepatan 100-Mbps (dan lebih tinggi) dengan lebih baik. Lihat bagian Detail “Kabel Kategori 5e dan jaringan area lokal 1000-Mbps” untuk mempelajari bagaimana Kategori 5e dapat mendukung jaringan area lokal 1000-Mbps.

Twisted pair kategori 6 dirancang untuk mendukung transmisi data dengan sinyal setinggi 250 MHz untuk jarak 100 meter. Kabel ini memiliki spacer plastik di tengah kabel yang memisahkan pasangan terpilin dan selanjutnya mengurangi kebisingan elektromagnetik. Hal ini menjadikan kabel Kategori 6 pilihan yang baik untuk lari 100 meter di jaringan area lokal dengan kecepatan transmisi 250 hingga 1000 Mbps. Menariknya, kabel twisted pair Kategori 6 hanya berharga satu sen per kaki lebih mahal dibandingkan kabel twisted pair Kategori 5e. Oleh karena itu, dengan adanya pilihan kabel twisted pair Kategori 5, 5e, atau 6, Anda mungkin harus memasang Kategori 6 dengan kata lain, kabel dengan kualitas terbaik terlepas dari apakah Anda akan langsung memanfaatkan kecepatan transmisi yang lebih tinggi atau tidak.

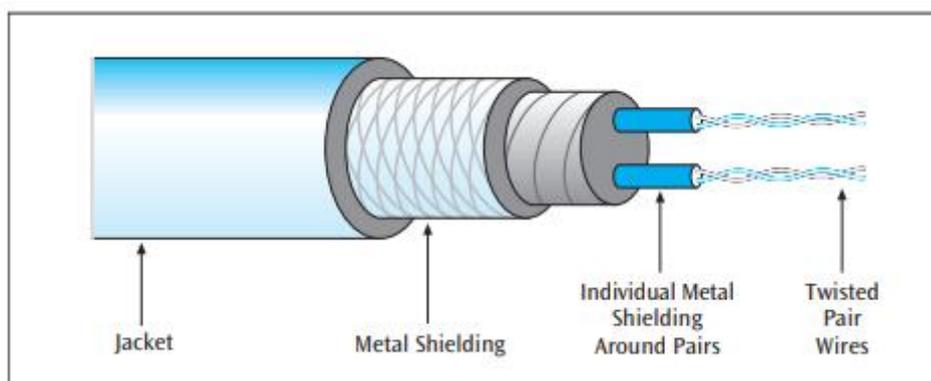
Twisted pair kategori 7 adalah tambahan terbaru pada keluarga twisted pair. Kabel kategori 7 dirancang untuk mendukung bandwidth 600 MHz untuk jarak 100 meter. Kabel

dilindungi dengan ketat setiap pasang kabel dilindungi oleh foil, dan seluruh kabel juga memiliki pelindung. Beberapa perusahaan sedang mempertimbangkan untuk menggunakan Kategori 7 untuk Gigabit dan 10-Gigabit Ethernet, namun saat ini harganya cukup tinggi lebih dari Rp. 10.000 per kaki.

Semua kabel yang dijelaskan sejauh ini kecuali kabel Kategori 7 dapat dibeli sebagai pasangan terpilin tanpa pelindung. Pasangan terpilin tanpa pelindung (UTP) adalah bentuk pasangan terpilin yang paling umum; tidak ada satu pun kabel dalam bentuk ini yang dibungkus dengan kertas logam atau jalinan. Sebaliknya, pasangan terpilin berpelindung (STP), yang juga tersedia dalam Kategori 5 hingga 6 (serta berbagai konfigurasi kabel), adalah bentuk di mana pelindung dililitkan pada masing-masing kabel secara terpisah, pada semua kabel secara bersamaan, atau keduanya. Pelindung ini memberikan lapisan isolasi tambahan dari interferensi elektromagnetik yang tidak diinginkan. Gambar 3-3 menunjukkan contoh kawat twisted pair berpelindung.

Kategori 5e Wire dan Jaringan Area Lokal 1000-Mbps

Jika kabel Kategori 5e dirancang untuk mendukung data 125-Mbps mampu mengirim 250 Mbps. Jawaban ini melibatkan trik kedua: transmisi sejauh 100 meter, bagaimana bisa digunakan di jaringan Gigabit Ethernet 1000 Mbps menggunakan skema pengkodean yang disebut jaringan area lokal 4D-PAM5 (juga dikenal sebagai Gigabit Ethernet)? Trik pertama (modulasi amplitudo pulsa). Sementara rincian dari 4D-PAM5 adalah dengan menggunakan empat pasang kabel Kategori 5e untuk lokal 1000-Mbps yang agak canggih dan di luar cakupan teks ini, anggap saja jaringan area (dibandingkan dua pasang dengan 100-Mbps area lokal itu adalah teknik yang menggunakan jaringan pengkodean data empat dimensi (4D). Dengan empat pasang, 250 Mbps dikirim melalui setiap pasang. Empat digabungkan dengan sinyal lima tingkat tegangan (PAM5). Kombinasi ini berpasangan dikalikan 250 Mbps sama dengan 1000 Mbps. Tapi itu masih tidak memungkinkan Gigabit Ethernet untuk mengirimkan 250 Mbps melalui sepasang kabel. Jelaskan bagaimana sepasang kabel yang dirancang untuk transmisi 125-Mbps adalah kabel Kategori 5e.



Gambar 3.3 Contoh kawat twisted pair berpelindung

Jika kabel pasangan terpilin harus melewati dinding, ruangan, atau bangunan yang terdapat interferensi elektromagnetik yang cukup untuk menyebabkan masalah kebisingan

yang besar, penggunaan kabel pasangan terpilin berpelindung dapat memberikan tingkat isolasi yang lebih tinggi dari interferensi tersebut dibandingkan kabel pasangan terpilin tidak berpelindung dan, dengan demikian, tingkat kesalahan yang lebih rendah. (Anda juga dapat mengalirkan kabel pasangan terpilin melalui saluran logam.) Interferensi elektromagnetik sering kali dihasilkan oleh motor besar, seperti yang ditemukan pada peralatan pemanas dan pendingin atau peralatan manufaktur.

Bahkan perlengkapan lampu neon menghasilkan interferensi elektromagnetik dalam jumlah yang nyata. Sumber daya yang besar juga dapat menghasilkan interferensi elektromagnetik dalam jumlah yang merusak. Oleh karena itu, umumnya bukan ide yang baik untuk mengikat kabel twisted pair ke saluran listrik yang melintasi ruangan atau dinding. Selain itu, meskipun kabel twisted pair berpelindung Kategori 5 hingga 6 telah meningkatkan isolasi kebisingan, Anda tidak dapat berharap untuk mendorongnya melewati batas 100 meter. Terakhir, bersiaplah untuk membayar mahal untuk twisted pair berpelindung. Bukan hal yang aneh untuk menghabiskan tambahan Rp. 10.000 per kaki untuk twisted pair berpelindung berkualitas baik. Sebaliknya, kabel twisted pair tanpa pelindung Kategori 5, 5e, dan 6 sering kali berharga antara Rp. 1.000-2.000 per kaki.

Tabel 3.1 Ringkasan karakteristik kabel twisted pair

UTP Category	Typical Use	Maximum Data Transfer Rate	Maximum Transmission Range	Advantages	Disadvantages
Category 1	Telephone wire	<100 kbps	5–6 kilometers (3–4 miles)	Inexpensive, easy to install and interface	Security, noise, obsolete
Category 2	T-1, ISDN	<2 Mbps	5–6 kilometers (3–4 miles)	Same as Category 1	Security, noise, obsolete
Category 3	Telephone circuits	10 Mbps	100 m (328 ft)	Same as Category 1, with less noise	Security, noise
Category 4	LANs	20 Mbps	100 m (328 ft)	Same as Category 1, with less noise	Security, noise, obsolete
Category 5	LANs	100 Mbps (100 MHz)	100 m (328 ft)	Same as Category 1, with less noise	Security, noise
Category 5e	LANs	250 Mbps per pair (125 MHz)	100 m (328 ft)	Same as Category 5. Also includes specifications for connectors, patch cords, and other components	Security, noise
Category 6	LANs	250 Mbps per pair (250 MHz)	100 m (328 ft)	Higher rates than Category 5e, less noise	Security, noise, cost
Category 7	LANs	600 MHz	100 m (328 ft)	High data rates	Security, noise, cost

Tabel 3-1 merangkum karakteristik dasar kabel twisted pair tak berpelindung. Ingatlah bahwa untuk tujuan kita, kabel pasangan terpilin berpelindung pada dasarnya memiliki kecepatan transfer data dan jangkauan transmisi yang sama dengan kabel pasangan terpilin tidak berpelindung tetapi berkinerja lebih baik di lingkungan yang bising. Perhatikan juga bahwa jarak transmisi dan kecepatan transfer yang tercantum pada Tabel 3-1 tidak dituliskan secara

jelas. Lingkungan yang bising cenderung memperpendek jarak transmisi dan kecepatan transfer.

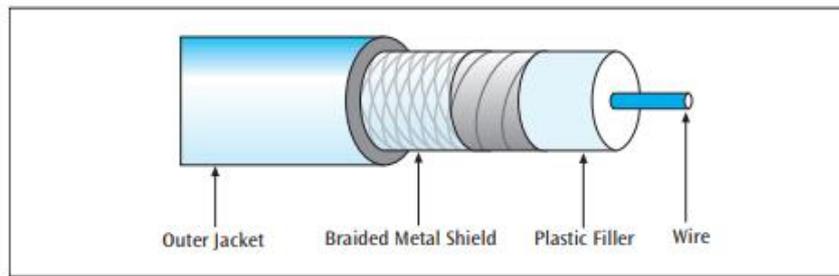
Lebih Banyak Karakteristik Twisted Pair

Saat Anda memilih kabel, Anda dapat menggunakan Kategori 5 hingga 7 yang tidak menyebarkan api dan asap berbahaya. Untuk memenuhi standar dan pelindung ini guna membuat beberapa perbedaan antara berbagai jenis kawat, jaket kawat terbuat dari bahan khusus; dan ini, dari kawat twisted pair. Selain mengetahui perbedaan-perbedaan ini, tentu saja Anda juga meningkatkan biaya kawat secara signifikan. Faktanya, kabel pleno perlu mempertimbangkan di mana kabel Anda akan ditempatkan dan berapa harganya terkadang dua kali lipat dari kabel twisted pair standar.

lebar seharusnya. Contohnya, saat dipasang antar ruangan. Jika, sebaliknya, kawat Anda akan melewati sebuah riser di dalam gedung, apakah kawat tersebut akan berjalan di dalam pleno atau melalui tabung logam berongga seperti saluran yang membentang di antara dinding lantai, anak tangga? Pleno adalah ruang di dalam bangunan yang dibuat dan langit-langit serta melingkupi masing-masing kabel maka api dan komponen bangunan serta dirancang untuk pergerakan asap berbahaya bukanlah masalah yang serius. Dalam hal ini, udara plastik standar dapat dihirup misalnya, ruang di atas plafon gantung. jaket bisa digunakan. Jenis kawat pasangan terpilin ini biasanya merupakan pleno A yang juga dapat menjadi jalan tersembunyi di antara ruangan tempat kabel diiklankan dan didiskusikan sehubungan dengan pemasangan kabel baru, ventilasi pemanas dan pendingin rumah, saluran telepon, dan kabel lainnya karena sebagian besar instalasi ini melibatkan layanan kabel berjalan. Kawat pleno dirancang sedemikian rupa sehingga jika terjadi kebakaran, kawat tersebut dapat melewati anak tangga.

Kabel koaksial

Kabel koaksial, dalam bentuknya yang paling sederhana, adalah kawat tunggal (biasanya tembaga) yang dibungkus dengan insulasi busa, dikelilingi oleh pelindung logam yang dikepang, dan kemudian ditutup dengan jaket plastik. Pelindung logam yang dikepang sangat baik dalam menghalangi sinyal elektromagnetik memasuki kabel dan menghasilkan kebisingan. Gambar 3.4 menunjukkan kabel koaksial dan pelindung logam yang dikepangnya. Karena sifat pelindungnya yang baik, kabel koaksial baik dalam membawa sinyal analog dengan rentang frekuensi yang luas. Dengan demikian, kabel koaksial dapat mentransmisikan saluran video dalam jumlah besar, seperti yang terdapat pada layanan televisi kabel yang dikirimkan ke rumah dan bisnis. Kabel koaksial juga telah digunakan untuk transmisi telepon jarak jauh, dalam kondisi yang jarang terjadi sebagai kabel dalam jaringan area lokal, dan sebagai penghubung antara terminal komputer dan komputer mainframe.

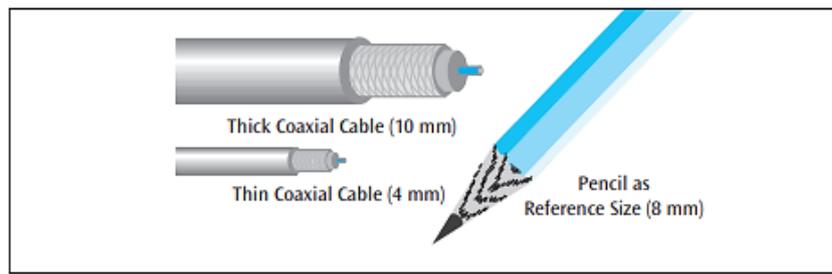


Gambar 3.4 Contoh kabel koaksial yang menunjukkan jalinan logam

Ada dua teknologi kabel koaksial utama dan dibedakan berdasarkan jenis sinyal yang dibawa masing-masing: baseband dan broadband. Teknologi koaksial baseband menggunakan sinyal digital dimana kabel hanya membawa satu saluran data digital. Aplikasi yang cukup umum untuk koaksial pita dasar adalah interkoneksi sakelar dalam jaringan area lokal. Dalam jaringan seperti itu, kabel baseband biasanya membawa satu sinyal 10 hingga 100 Mbps dan memerlukan repeater setiap beberapa ratus kilometer. Saat ini, kabel serat optik menggantikan kabel koaksial baseband sebagai metode pilihan untuk menghubungkan hub LAN.

Teknologi koaksial broadband biasanya mentransmisikan sinyal analog dan mampu mendukung banyak saluran data secara bersamaan. Pertimbangkan kabel koaksial yang mentransmisikan televisi kabel. Banyak perusahaan kabel menawarkan 100 saluran atau lebih. Setiap saluran atau sinyal menempati bandwidth sekitar 6 MHz. Ketika 100 saluran ditransmisikan bersama-sama, kabel koaksial mendukung sinyal komposit 100 6 MHz atau 600 MHz. Dibandingkan dengan kapasitas data kabel twisted pair dan kabel baseband, setiap saluran broadband cukup kuat, karena dapat mendukung jutaan bit per detik. Untuk mendukung rentang frekuensi yang luas, sistem kabel koaksial broadband memerlukan amplifier (ingat amplifikasi sinyal analog dari Bab Dua) kira-kira setiap tiga hingga empat kilometer. Meskipun pemisahan dan penggabungan sinyal broadband dan kabel dimungkinkan, ini adalah ilmu pasti yang sebaiknya diserahkan kepada spesialis di bidangnya. Oleh karena itu, banyak administrator jaringan sering mempekerjakan ahli dari luar untuk menginstal dan memelihara sistem broadband.

Selain dua kategori berbasis sinyal, kabel koaksial juga tersedia dalam berbagai ketebalan, dengan dua tipe fisik utama: kabel koaksial tebal dan kabel koaksial tipis, keduanya ditunjukkan pada Gambar 3.5. Kabel koaksial tebal memiliki ukuran diameter sekitar 6 hingga 18 mm (1/4 hingga 3/4 inci). Kabel koaksial tipis berdiameter sekitar 4 mm (kurang dari 1/4 inci). Dibandingkan dengan kabel koaksial tebal, yang biasanya membawa sinyal broadband, kabel koaksial tipis memiliki isolasi kebisingan terbatas dan biasanya membawa sinyal baseband. Kabel koaksial tebal memiliki ketebalan kebisingan yang lebih baik dan umumnya digunakan untuk transmisi data analog, seperti saluran video tunggal atau ganda. Beberapa kabel koaksial tebal sangat tebal dan kaku sehingga beberapa orang bercanda menyebutnya selang taman beku. Harga kabel koaksial tebal dan tipis bervariasi tergantung pada kualitas dan konstruksi kabel, tetapi biasanya harganya Rp. 8.000 hingga Rp. 12.000 per kaki, dan terkadang bahkan lebih tinggi.



Gambar 3.5 Contoh kabel koaksial tebal dan kabel koaksial tipis

Lebih Banyak Karakteristik Kabel Koaksial

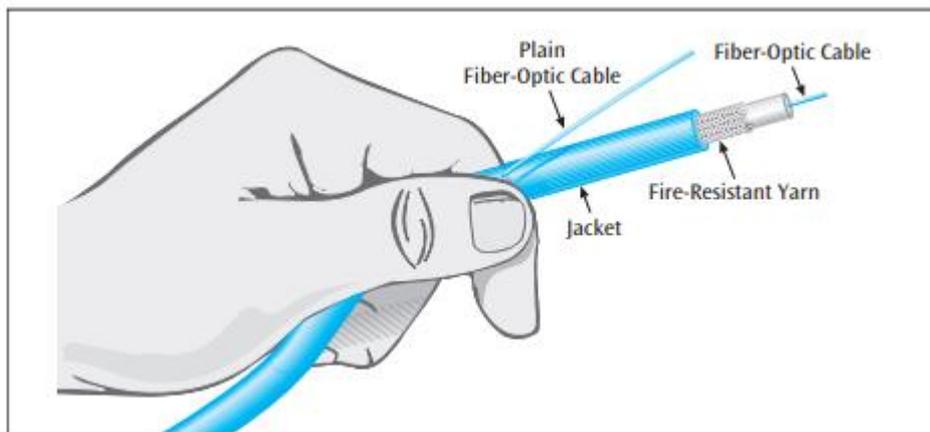
Karakteristik penting dari kabel koaksial adalah nilai ohmnya. Ohm adalah ukuran resistansi dalam suatu medium. Semakin tinggi nilai ohm, semakin besar hambatan pada kabel. Meskipun resistansi bukan merupakan perhatian utama ketika memilih kabel tertentu, nilai ohm secara tidak langsung penting karena kabel koaksial dengan nilai ohm tertentu bekerja lebih baik dengan jenis sinyal tertentu, dan juga dengan jenis aplikasi tertentu. Jenis kabel koaksial ditentukan oleh radio guide (RG), yaitu peringkat komposit yang memperhitungkan banyak karakteristik, termasuk ketebalan kawat, ketebalan isolasi, dan sifat listrik. Tabel 3.2 merangkum berbagai jenis kabel koaksial, nilai ohmnya, dan aplikasinya. Karakteristik lain dari kabel koaksial yang terkadang menjadi pertimbangan adalah apakah kabel yang melewati bagian tengah kabel koaksial itu beruntai tunggal atau dikepang. Kabel koaksial untai tunggal, sesuai dengan namanya, berisi satu kawat. Kabel koaksial yang dikepang terdiri dari banyak kabel halus yang dipilin satu sama lain, bertindak sebagai konduktor tunggal. Jika kawat dikepang, seringkali lebih murah dan lebih mudah ditekuk dibandingkan kawat tunggal, yang biasanya lebih tebal.

Tabel 3.2 Kabel koaksial yang umum, nilai ohm, dan aplikasinya

Type of Cable	Ohm Rating	Application/Comments
RG-6	75 Ohm	Cable television, satellite television, and cable modems
RG-8	50 Ohm	Older Ethernet local area networks; RG-8 is being replaced with RG-58
RG-11	75 Ohm	Broadband Ethernet local area networks and other video applications
RG-58	50 Ohm	Baseband Ethernet local area networks
RG-59	75 Ohm	Closed-circuit television; cable television (but RG-6 is better here)
RG-62	93 Ohm	Interconnection of IBM 3270 computer terminals

Kabel serat optik

Semua media yang dibahas sejauh ini mempunyai satu kelemahan besar: interferensi elektromagnetik. Interferensi elektromagnetik adalah distorsi elektronik yang dialami sinyal yang melewati kawat logam ketika medan magnet menyimpang melewatinya. Terkait dengan masalah ini adalah seperti yang telah Anda pelajari sebelumnya di bab ini, bahwa sinyal yang melewati kawat logam juga menghasilkan medan magnet dan dengan demikian menghasilkan interferensi elektromagnetik. Masalah terkait lainnya (dan kelemahan kabel twisted pair dan kabel koaksial) adalah seseorang dapat menyadap media ini yakni, memanfaatkan interferensi elektromagnetik ini dan mendengarkan data yang mengalir melalui kabel tanpa terdeteksi. Interferensi elektromagnetik dapat dikurangi dengan pelindung yang tepat, namun hal ini tidak dapat sepenuhnya dihindari kecuali Anda menggunakan kabel serat optik. Kabel serat optik (atau serat optik) adalah kabel kaca tipis, sedikit lebih tebal dari rambut manusia, dikelilingi oleh lapisan plastik. Ketika kabel serat optik dikemas menjadi kabel berinsulasi, kabel tersebut dikelilingi oleh benang Aramid dan jaket plastik yang kuat untuk melindunginya dari tekukan, panas, dan tekanan. Anda dapat melihat contoh kabel serat optik pada Gambar 3-6.



Gambar 3.6 Seseorang memegang kabel serat optik polos dan kabel serat optik dalam jaket berinsulasi

Bagaimana kabel kaca tipis mengirimkan data? Sumber cahaya, yang disebut dioda foto, ditempatkan pada ujung transmisi dan dengan cepat dinyalakan dan dimatikan untuk menghasilkan pulsa cahaya. Pulsa cahaya ini merambat ke bawah kabel kaca dan dideteksi oleh sensor optik yang disebut fotoreseptor di sisi penerima. Sumber cahaya dapat berupa dioda pemancar cahaya (LED) yang sederhana dan murah, seperti yang ditemukan di banyak kalkulator saku, atau laser yang lebih kompleks. Laser jauh lebih mahal dibandingkan LED, dan dapat menghasilkan kecepatan transmisi data yang jauh lebih tinggi. Kabel serat optik mampu mentransmisikan data lebih dari 100 Gbps (yaitu 100 miliar bit per detik!) dalam jarak beberapa kilometer. Karena banyak instalasi jaringan area lokal umum menggunakan sumber LED, transmisi serat optik di dunia nyata secara efektif dibatasi hingga 10 gigabit untuk jarak

300 meter. (Lihat bagian Detail “Karakteristik Lebih Lanjut Kabel Serat Optik” untuk diskusi tentang aplikasi serat optik LED dan laser.)

Selain menyediakan kecepatan transmisi data berkecepatan tinggi dan kesalahan rendah, kabel serat optik menawarkan sejumlah keunggulan lain dibandingkan kabel twisted pair dan kabel koaksial. Karena kabel serat optik melewatkan foton nonkonduktor listrik melalui media kaca, maka penyadapan hampir tidak mungkin dilakukan. Satu-satunya cara yang mungkin untuk menyadap jalur serat optik adalah dengan membobol jalur tersebut secara fisik, sebuah intrusi yang akan diketahui. Selain itu, karena kabel serat optik tidak dapat menghasilkan atau terganggu oleh interferensi elektromagnetik, tidak ada noise yang dihasilkan dari sinyal elektromagnetik asing. Meskipun kabel serat optik masih mengalami kebisingan saat pulsa cahaya memantul di dalam kabel kaca, kebisingan ini jauh lebih kecil dibandingkan kebisingan yang dihasilkan pada kawat logam dari kabel pasangan terpilin atau kabel koaksial. Kurangnya kebisingan yang signifikan adalah salah satu alasan utama kabel serat optik dapat mengirimkan data dalam jarak yang jauh.

Terlepas dari kelebihan yang luar biasa ini, kabel serat optik memiliki dua kelemahan kecil namun signifikan. Pertama, karena cara kerja pengaturan sumber cahaya dan fotoreseptor, pulsa cahaya hanya dapat merambat dalam satu arah. Oleh karena itu, untuk mendukung transmisi data dua arah diperlukan dua kabel serat optik. Karena alasan ini, sebagian besar kabel serat optik dijual dengan setidaknya dua (jika tidak lebih) untai serat individu yang digabungkan menjadi satu paket, seperti yang ditunjukkan pada Gambar 3-7.

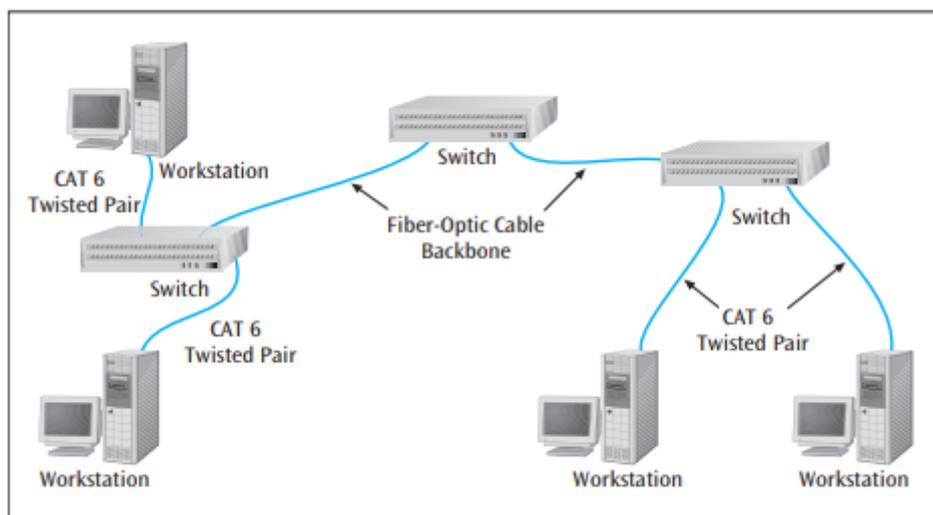


Gambar 3.7 Kabel serat optik dengan banyak helai serat

Kerugian kedua dari kabel serat optik adalah biayanya yang lebih tinggi, namun kelemahan ini perlahan-lahan menghilang. Misalnya, saat ini dimungkinkan untuk membeli kabel serat optik dupleks (dua untai) serbaguna dalam jumlah besar dengan harga sekitar \$0,50 per kaki (dibandingkan dengan membayar beberapa dolar per kaki beberapa tahun yang lalu), yang mendekati harga tersebut. Harga berbagai jenis kabel coaxial dan kabel twisted pair berpelindung. Jika Anda mempertimbangkan tingkat kesalahan yang lebih rendah dan tingkat

transmisi data yang lebih tinggi, kabel serat optik memang lebih murah, bahkan dibandingkan dengan kabel twisted pair yang murah.

Menariknya, bukan kabel serat optik itu sendiri yang mahal; mahalnya harga kabel disebabkan oleh perangkat keras yang mentransmisikan dan menerima pulsa cahaya di ujung kabel fiber. Namun situasi ini pun berubah. Mulai tahun 1999, harga dioda foto dan fotoreseptor mulai turun secara signifikan. Sebelum tahun 1999, kabel serat optik hanya digunakan sebagai tulang punggung kabel penghubung utama yang membentang dari satu ujung instalasi ke ujung lainnya dari suatu jaringan, dan menggunakan pasangan terpilin Kategori 5e atau 6 dari sambungan tulang punggung ke atas. ke stasiun kerja. Ilustrasi tulang punggung serat optik ditunjukkan pada Gambar 3-8.



Gambar 3.8 Tulang punggung serat optik dengan twisted pair CAT 6 berjalan ke stasiun kerja

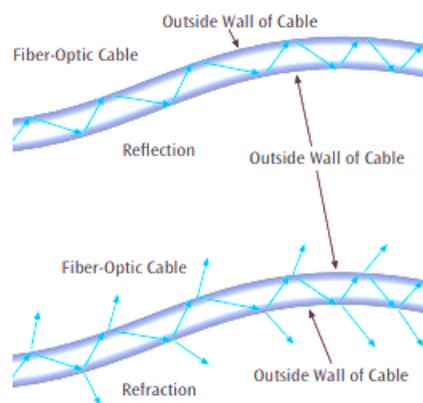
Serat Fotonik

Kabel serat optik, seperti yang baru saja kita lihat, adalah kabel kaca padat yang mengirimkan gelombang cahaya. Sayangnya, seiring dengan bertambahnya panjang kabel kacadan juga jarak yang harus ditempuh cahaya sinyal cahaya melemah (tersebar di dalam kaca) karena pemantulan dan pembiasan. (Lihat bagian Detail “Karakteristik Lebih Lanjut Kabel Serat Optik” untuk diskusi tentang refleksi dan refraksi.) Jenis media baru, serat fotonik, telah diperkenalkan yang secara virtual menghilangkan redaman ini. Kabel kaca ini mirip dengan kabel serat optik karena setipis rambut dan transparan. Namun perbedaan besarnya adalah kabel baru ini penuh dengan lubang. Jika Anda melihat penampang kabel serat fotonik, Anda akan melihat bahwa kaca tersebut memiliki pola sarang lebah. Sumber cahaya yang ditransmisikan melalui kabel sebenarnya berjalan melalui lubang-lubang yang hanya berisi udara. Karena cahaya yang merambat di udara bergerak tanpa hambatan, sinyalnya tidak menurun. Trik dengan serat fotonik adalah membuat lapisan yang mengelilingi kabel tidak menyerap cahaya. Untuk mengatasi masalah ini, para ilmuwan telah menciptakan permukaan reflektif yang bahkan lebih reflektif dibandingkan cermin. Diperkirakan setelah teknologi ini

disempurnakan, serat fotonik akan memiliki kecepatan dan jarak transmisi setidaknya 10 kali lipat dari kabel serat optik saat ini.

Lebih Banyak Karakteristik Kabel Serat Optik

Ketika cahaya dari suatu sumber dikirim melalui kabel serat optik, gelombang cahaya memantul di dalam kabel dan melewati kabel ke jaket pelindung luar. Ketika sinyal cahaya di dalam kabel memantul dari dinding kabel dan kembali ke kabel, hal ini disebut refleksi. Ketika sinyal cahaya berpindah dari inti kabel ke material di sekitarnya, hal ini disebut pembiasan. Gambar 3.9 menunjukkan perbedaan antara pemantulan dan pembiasan.



Gambar 3.9 Demonstrasi sederhana pemantulan dan pembiasan pada kabel serat optik

Cahaya dapat ditransmisikan melalui kabel serat optik menggunakan dua teknik dasar. Teknik pertama, yang disebut transmisi mode tunggal, memerlukan penggunaan kabel serat optik yang sangat tipis dan sumber cahaya yang sangat terfokus, seperti laser. Ketika laser ditembakkan pada serat yang sempit, cahayanya mengikuti sinar yang rapat, sehingga gelombang cahaya cenderung tidak memantul atau membias.

Dengan demikian, teknik ini memungkinkan sinyal yang sangat cepat dengan sedikit degradasi sinyal (dan dengan demikian lebih sedikit noise) dalam jarak jauh. Karena laser digunakan sebagai sumber cahaya, transmisi mode tunggal merupakan teknik yang lebih mahal dibandingkan teknik pensinyalan kabel serat optik kedua. Aplikasi apa pun yang melibatkan sejumlah besar data yang dikirimkan dengan kecepatan tinggi merupakan kandidat untuk transmisi mode tunggal.

Teknik pensinyalan kedua, disebut transmisi multimode, menggunakan kabel serat yang sedikit lebih tebal dan sumber cahaya yang tidak fokus, seperti LED. Karena sumber cahaya tidak fokus, gelombang cahaya mengalami lebih banyak pembiasan dan refleksi (yaitu kebisingan) saat merambat melalui kawat. Kebisingan ini mengakibatkan sinyal tidak dapat merambat sejauh atau secepat sinyal yang dihasilkan dengan teknik mode tunggal. Sejalan dengan itu, transmisi multimode lebih murah dibandingkan transmisi mode tunggal. Jaringan area lokal yang menggunakan kabel serat optik sering kali menggunakan transmisi multimode.

Teknik transmisi single mode dan multimode menggunakan kabel serat optik dengan karakteristik berbeda. Inti kabel serat optik mode tunggal memiliki lebar 8,3 mikron, dan bahan yang mengelilingi serat kelongsongnya memiliki lebar 125 mikron. Oleh karena itu,

kabel serat optik mode tunggal diberi label kabel 8.3/125. Inti kabel serat optik multimode umumnya memiliki lebar 62,5 mikron, dan kelongsongnya 125 mikron. Kabel serat optik multimode diberi label kabel 62,5/125. Ukuran kabel serat optik multimode lainnya termasuk 50/125 dan 100/140 mikron.

Tabel 3.3 Ringkasan karakteristik media yang dilakukan

Jenis Media yang Dilakukan	Penggunaan Khas	Kecepatan Data Maksimum	Jangkauan Transmisi Maksimum	Keuntungan	Kekurangan
Pasangan terpilih Kategori 1, 3	Sistem telepon	<2Mbps	5–6 kilometer (3–4 mil)	Murah, umum	Kebisingan, keamanan, usang
Pasangan terpilih Kategori 5, 5e, 6, 7	LAN	100–1000Mbps	100 m (328 kaki)	Murah, serbaguna	Kebisingan, keamanan
Kabel Koaksial Tipis (saluran tunggal baseband)	LAN	10Mbps	100 m (328 kaki)	Kebisingan rendah	Keamanan
Kabel Koaksial Tebal (multisaluran broadband)	LAN, TV kabel, telepon jarak jauh, hubungan sistem komputer jangka pendek	10–100Mbps	5–6 kilometer (3–4 mil) (dengan kecepatan data lebih rendah)	Kebisingan rendah, banyak saluran	Keamanan
Serat Optik LED	Data, video, audio, LAN	Gbps	300 meter (kira-kira 1000 kaki)	Aman, kapasitas tinggi, kebisingan rendah	Antarmuka mahal tetapi biayanya menurun
Laser Fiber-Optik	Data, video, audio, LAN, WAN, MAN	100 detik Gbps	100 kilometer (kira-kira 60 mil)	Aman, kapasitas tinggi, kebisingan sangat rendah	Antarmuka mahal

Tabel 3.3 merangkum media yang dilakukan dan dibahas dalam bab ini. Kabel twisted pair kategori 1 dan 3 telah dikelompokkan bersama karena biasanya digunakan untuk sistem telepon, sedangkan kabel kategori 5 hingga 7 dikelompokkan bersama karena biasanya digunakan untuk jaringan area lokal. Di hampir semua kasus, kecepatan data maksimum dan jangkauan transmisi maksimum adalah nilai tipikal dan bisa lebih kecil atau lebih besar, bergantung pada faktor lingkungan.

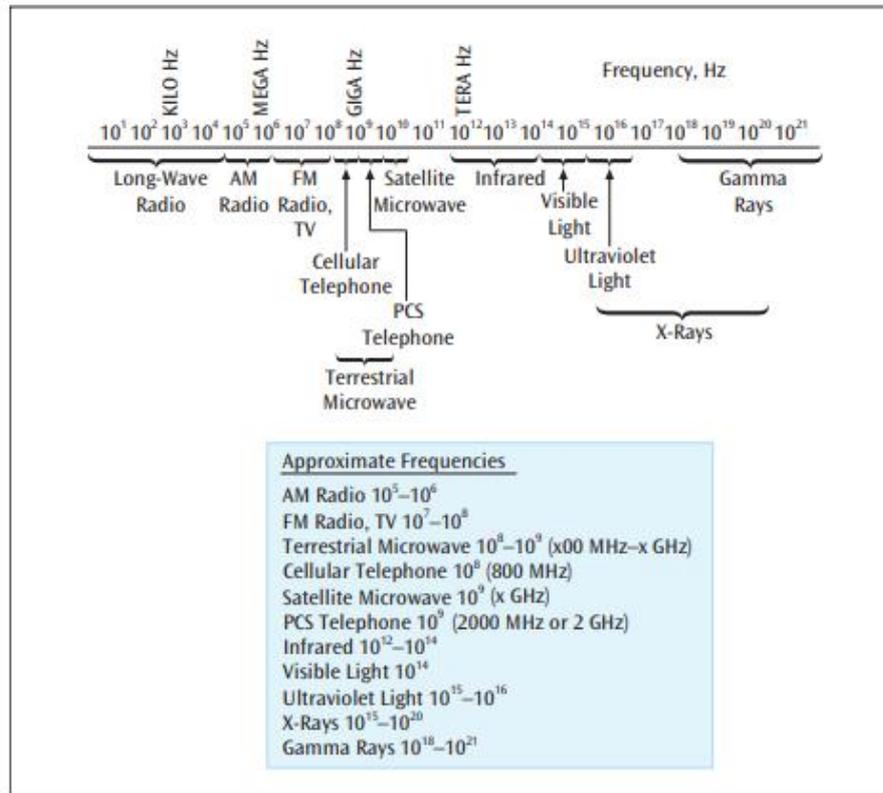
Sebelum kita meninggalkan topik media yang dikelola, mari kita perkenalkan satu isu penting terakhir yang berkaitan dengan media yang dikelola: isu hak jalan. Hak jalan adalah kemampuan hukum suatu bisnis atau seseorang untuk memasang kawat atau kabel di properti orang lain. Apabila suatu usaha hendak memasang media penghantar di antara dua bangunan, dan usaha itu tidak mempunyai tanah di antara bangunan-bangunan itu, maka usaha itu harus mendapat hak jalan dari pemilik tanah di antara itu. Hak ini mungkin berupa izin sederhana, tetapi mungkin juga melibatkan pembayaran. Seperti yang akan kita lihat di bagian berikut, transmisi nirkabel secara umum tidak harus berurusan dengan masalah jalur langsung. Hal ini sering kali memberikan keuntungan besar bagi media nirkabel dibandingkan media konduksi.

3.3 MEDIA NIRKABEL

Pengenalan bab ini mencantumkan tujuh jenis media nirkabel yang berbeda. Terlepas dari kenyataan bahwa setiap jenis media mungkin digunakan oleh aplikasi yang berbeda, dan rangkaian frekuensi yang berbeda sering kali ditetapkan untuk masing-masing media, semua media nirkabel menggunakan teknologi dasar yang sama: transmisi data menggunakan gelombang radio. (Sebenarnya, dalam semua jenis teknologi nirkabel ini, media sebenarnya yang harus dilalui oleh gelombang radio adalah udara atau ruang angkasa. Namun, untuk tujuan diskusi ini, kami akan memperluas istilah “media” untuk mencakup teknologi yang memancarkan gelombang radio. sinyal.) Mari kita kaji teknologi yang berkembang ini dan kemudian membahas masing-masing dari tujuh jenis media nirkabel, beserta karakteristik dasar dan area penerapannya.

Transmisi nirkabel menjadi populer pada tahun 1950an dengan radio AM, radio FM, dan televisi. Pada tahun 1962, transmisi dikirim melalui satelit pertama yang mengorbit, Telstar. Dalam 60 tahun atau lebih sejak transmisi nirkabel muncul, teknologi ini telah melahirkan ratusan, bahkan ribuan, aplikasi, beberapa di antaranya akan dibahas dalam bab ini.

Dalam transmisi nirkabel, berbagai jenis gelombang elektromagnetik digunakan untuk mengirimkan sinyal. Transmisi radio, transmisi satelit, cahaya tampak, cahaya inframerah, sinar-X, dan sinar gamma merupakan contoh gelombang elektromagnetik atau radiasi elektromagnetik. Secara umum, radiasi elektromagnetik adalah energi yang disebarkan melalui ruang dan, secara tidak langsung, melalui benda padat dalam bentuk gangguan medan listrik dan magnet yang semakin meningkat. Dalam kasus khusus, katakanlah, transmisi radio, energi ini dipancarkan dalam bentuk gelombang radio melalui percepatan elektron bebas, seperti yang terjadi ketika muatan listrik dilewatkan melalui kabel antena radio. Perbedaan mendasar antara berbagai jenis gelombang elektromagnetik adalah perbedaan panjang gelombang, atau frekuensinya, seperti yang ditunjukkan pada Gambar 3-10.



Gambar 3.10 Frekuensi gelombang elektromagnetik

Perhatikan bahwa semua jenis sistem transmisi seperti radio AM, radio FM, televisi, telepon seluler, gelombang mikro terestrial, dan sistem satelit semuanya terbatas pada pita frekuensi yang relatif sempit. Komisi Komunikasi Federal (FCC) menjaga kontrol ketat terhadap frekuensi yang digunakan oleh aplikasi apa. Kadang-kadang, FCC akan menetapkan rentang frekuensi yang tidak terpakai untuk aplikasi baru. Di lain waktu, FCC akan melelang frekuensi yang tidak terpakai kepada penawar tertinggi. Pemenang lelang kemudian diperbolehkan menggunakan frekuensi tersebut untuk memperkenalkan produk atau jasa tertentu. Penting untuk dicatat, bagaimanapun, bahwa hanya frekuensi tertentu yang tersedia untuk digunakan dalam aplikasi. Oleh karena itu, sangat penting bahwa setiap aplikasi menggunakan frekuensi yang ditetapkannya sebaik mungkin. Sistem telepon seluler, seperti yang akan kita lihat, memberikan contoh yang baik tentang bagaimana suatu aplikasi dapat menggunakan frekuensi yang ditetapkan secara efisien. Mari kita ingat proses alokasi frekuensi konservatif ini saat kita membahas delapan bidang sistem komunikasi nirkabel, dimulai dengan salah satu yang tertua: transmisi gelombang mikro terestrial.

Transmisi Gelombang Mikro Terestrial

Sistem transmisi gelombang mikro terestrial mengirimkan berkas sinyal radio yang sangat terfokus dari satu antena transmisi gelombang mikro berbasis darat ke antena transmisi gelombang mikro lainnya. Dua area penerapan gelombang mikro terestrial yang paling umum adalah komunikasi telepon dan pergaulan bisnis. Banyak perusahaan telepon menerapkan serangkaian antena, menempatkan kombinasi menara penerima dan pemancar setiap 15 hingga 30 mil. Sistem ini menyediakan layanan telepon dengan menjangkau wilayah

metropolitan serta intranegara bagian dan antar negara bagian. Bisnis juga dapat menggunakan gelombang mikro terestrial untuk menerapkan sistem telekomunikasi antar gedung perusahaan. Mempertahankan pengaturan seperti itu mungkin akan lebih murah dalam jangka panjang dibandingkan menyewa saluran telepon berkecepatan tinggi dari perusahaan telepon, yang memerlukan pembayaran bulanan berkelanjutan. Dengan microwave terestrial, setelah sistem dibeli dan dipasang, tidak diperlukan biaya layanan telepon.

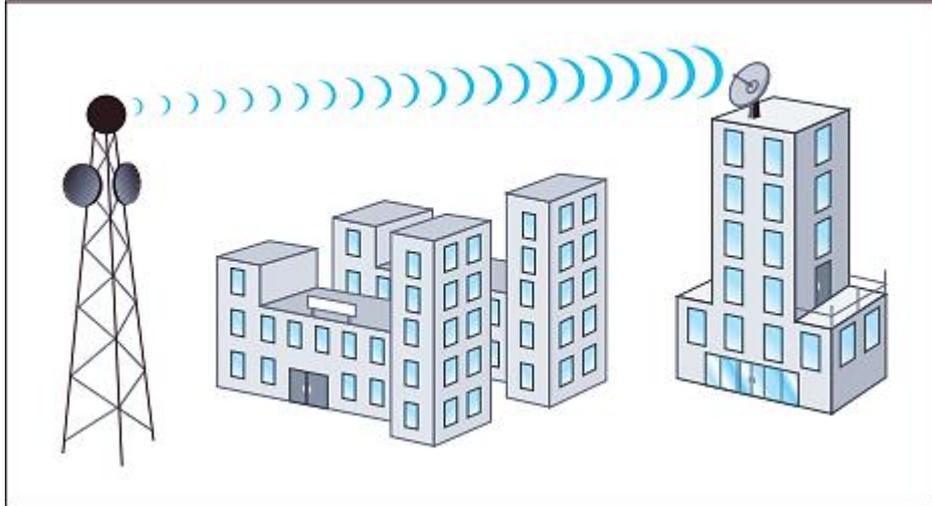
Mungkin nilai jual terbaik gelombang mikro terestrial adalah kemampuannya mengirimkan sinyal hingga ratusan juta bit per detik tanpa menggunakan kabel interkoneksi. Gambar 3.11 menunjukkan pemasangan antena gelombang mikro pada umumnya.



Gambar 3.11 Menara dan antena gelombang mikro pada umumnya

Transmisi gelombang mikro tidak mengikuti lengkungan bumi, juga tidak melewati benda padat, yang keduanya membatasi jarak transmisinya. Antena gelombang mikro menggunakan transmisi line-of-sight, artinya untuk menerima dan mengirimkan sinyal, setiap antena harus berhadapan dengan antena berikutnya (lihat Gambar 3.12). Banyak antena gelombang mikro terletak di atas menara yang berdiri bebas, dan jarak khas antara menara gelombang mikro kira-kira 15 hingga 30 mil. Semakin tinggi menaranya, semakin jauh kemungkinan jarak transmisinya. Jadi, menara yang terletak di perbukitan atau pegunungan, atau di atas gedung-gedung tinggi, dapat mengirimkan sinyal lebih jauh dari 30 mil. Faktor lain yang membatasi jarak transmisi adalah banyaknya objek yang mungkin menghalangi jalur transmisi sinyal. Bangunan, bukit, hutan, dan bahkan hujan lebat serta hujan salju semuanya mengganggu transmisi sinyal gelombang mikro. (Dengan asumsi tidak ada gangguan, dan

amplifier digunakan pada menara untuk meregenerasi sinyal, gelombang mikro terestrial dapat beroperasi pada jarak yang tidak terbatas.) Dengan mempertimbangkan keterbatasan ini, kelemahan gelombang mikro terestrial dapat mencakup hilangnya kekuatan sinyal (redaman) dan interferensi dari sinyal lain (intermodulasi), selain biaya sewa layanan atau pemasangan dan pemeliharaan antena.



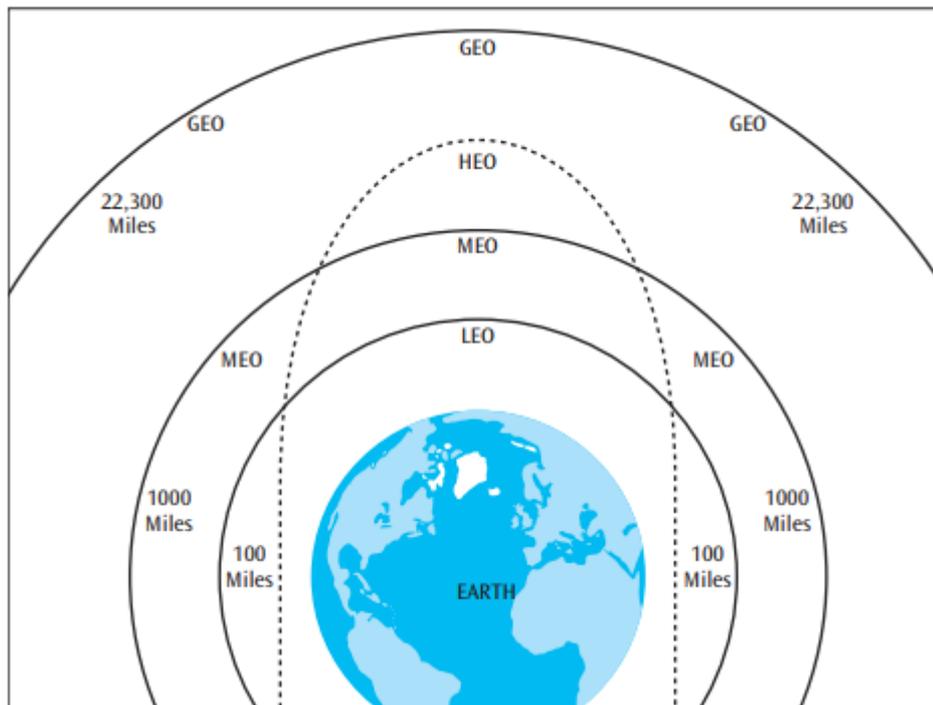
Gambar 3.12 Antena gelombang mikro di atas menara yang berdiri bebas mentransmisikan ke antena lain di atas gedung

Transmisi Gelombang Mikro Satelit

Sistem transmisi gelombang mikro satelit mirip dengan sistem gelombang mikro terestrial kecuali bahwa sinyal bergerak dari stasiun bumi di Bumi ke satelit dan kembali ke stasiun bumi lain di Bumi, sehingga mencapai jarak yang jauh lebih jauh dibandingkan transmisi garis pandang di Bumi. Faktanya, satelit yang terletak pada titik terjauh dari Bumi 36.000 kilometer atau 22.300 mil dapat menerima dan mengirim sinyal kira-kira sepertiga jarak mengelilingi Bumi. Sistem satelit juga dapat mengirimkan sinyal di tengah bumi dengan memantulkannya dari satu satelit ke satelit lainnya.

Salah satu cara untuk mengategorikan sistem satelit adalah berdasarkan seberapa jauh jarak satelit dari Bumi. Semakin dekat jarak satelit ke Bumi, semakin singkat waktu yang dibutuhkan untuk mengirim data ke satelit untuk uplink dan menerima data dari bumi satelit untuk downlink. Waktu transmisi dari stasiun bumi ke satelit dan kembali ke stasiun bumi disebut penundaan propagasi. Kerugian dari jarak yang lebih dekat ke Bumi adalah satelit harus terus menerus mengelilingi Bumi agar tetap berada pada orbitnya. Oleh karena itu, satelit-satelit ini terus bergerak dan akhirnya melewati cakrawala, sehingga merusak transmisi garis pandang. Satelit yang selalu berada pada titik yang sama di Bumi dapat digunakan untuk transfer data berkecepatan tinggi dalam jangka waktu lama. Sebaliknya, karena satelit yang dekat dengan Bumi tidak berada pada posisi yang sama di atas Bumi, satelit tersebut digunakan dengan aplikasi yang memerlukan periode transfer data yang lebih singkat, seperti sistem telepon seluler. Seperti yang ditunjukkan Gambar 3.13, satelit mengorbit Bumi dari

empat kemungkinan rentang: orbit Bumi rendah (LEO), orbit Bumi tengah (MEO), orbit Bumi geosinkron (GEO), dan orbit Bumi sangat elips (HEO).



Gambar 3.13 Bumi dan empat orbit Bumi: LEO, MEO, GEO, dan HEO

Satelit orbit rendah bumi (LEO) merupakan satelit yang paling dekat dengan bumi. Mereka dapat ditemukan sedekat 100 mil dari permukaan dan sejauh 1000 mil. Jumlah satelit yang mengorbit rendah Bumi berkembang pesat. Pada akhir abad ke-20, terdapat sekitar 300 satelit LEO. Pada tahun 2009, diperkirakan 420 satelit LEO berada di orbit. Satelit yang mengorbit rendah Bumi digunakan terutama untuk transfer nirkabel surat elektronik, jaringan telepon seluler di seluruh dunia, mata-mata, penginderaan jauh, dan konferensi video.

Salah satu proyek paling ambisius dan terkenal di akhir abad ke-20 adalah telepon satelit global dan jaringan paging genggam Iridium milik Motorola. Sistem Iridium awalnya dirancang menggunakan tujuh lapisan satelit LEO dengan 11 satelit di setiap lapisannya, atau total 77 satelit. Jaringan ini mendapatkan namanya dari unsur iridium, yang memiliki berat atom 77. Setelah beberapa pemikiran ulang, diputuskan bahwa sistem ini juga akan bekerja dengan enam lapisan dari 11 satelit, dan dengan demikian proyek ini diperkecil menjadi 66 satelit (namun namanya tidak diubah menjadi unsur yang sesuai disprosium—yang tampaknya tidak memiliki cincin yang sama). Bahkan dengan hanya 66 satelit yang bekerja, seseorang dapat, dari mana saja di bumi, menerima atau melakukan panggilan telepon dengan menggunakan telepon seluler Iridium. Sayangnya, pada musim panas 1999, sistem Iridium gagal menarik cukup banyak pelanggan, menyebabkan pemilik sistem menjual jaringan 66 satelit. Sistem ini masih beroperasi hingga saat ini dan disediakan bagi orang-orang yang membutuhkan layanan telepon di mana pun di dunia.

Satelit Middle-Earth-orbit (MEO) dapat ditemukan sekitar 1000 hingga 3000 mil dari Bumi. Pada akhir abad kedua puluh, sekitar 65 satelit MEO mengorbit bumi. Meskipun sistem satelit MEO tidak tumbuh dengan kecepatan yang sama dengan sistem LEO, pakar industri memperkirakan bahwa jumlah satelit MEO pada tahun 2005 mendekati 120.

Konfigurasi Satelit

Selain diklasifikasikan menjadi LEO, MEO, GEO, dan HEO, sistem satelit dapat dikategorikan menjadi tiga topologi dasar: fasilitas pengangkut curah, stasiun bumi multipleks, dan stasiun bumi pengguna tunggal. Gambar 3.14 mengilustrasikan masing-masing topologi ini.

Fasilitas Pengangkutan Massal

Gambar 3.14(a) menunjukkan bahwa dalam fasilitas pembawa massal, sistem satelit dan seluruh frekuensi yang ditugaskan dikhususkan untuk satu pengguna. Karena satelit mampu mentransmisikan data dalam jumlah besar dalam waktu yang sangat singkat, dan sistemnya sendiri mahal, hanya aplikasi berukuran besar yang secara ekonomis dapat membenarkan penggunaan eksklusif seluruh sistem satelit oleh satu pengguna. Misalnya, masuk akal bagi perusahaan telepon untuk menggunakan sistem satelit pembawa massal untuk mengirimkan ribuan panggilan telepon jarak jauh.

Sistem pembawa massal umumnya beroperasi pada pita 6/4-GHz (uplink 6-GHz, downlink 4-GHz) dan menyediakan bandwidth 500-MHz, yang dapat dipecah lebih lanjut menjadi beberapa saluran 40–50 MHz.

Stasiun Bumi Multipleks

Dalam sistem satelit stasiun bumi multipleks, stasiun bumi menerima masukan dari berbagai sumber dan dengan cara tertentu menjalin aliran data, baik dengan menetapkan frekuensi yang berbeda untuk sinyal yang berbeda atau dengan membiarkan sinyal yang berbeda untuk melakukan transmisi secara bergiliran. Gambar 3.14(b) menunjukkan diagram cara kerja sistem satelit stasiun bumi multipleks.

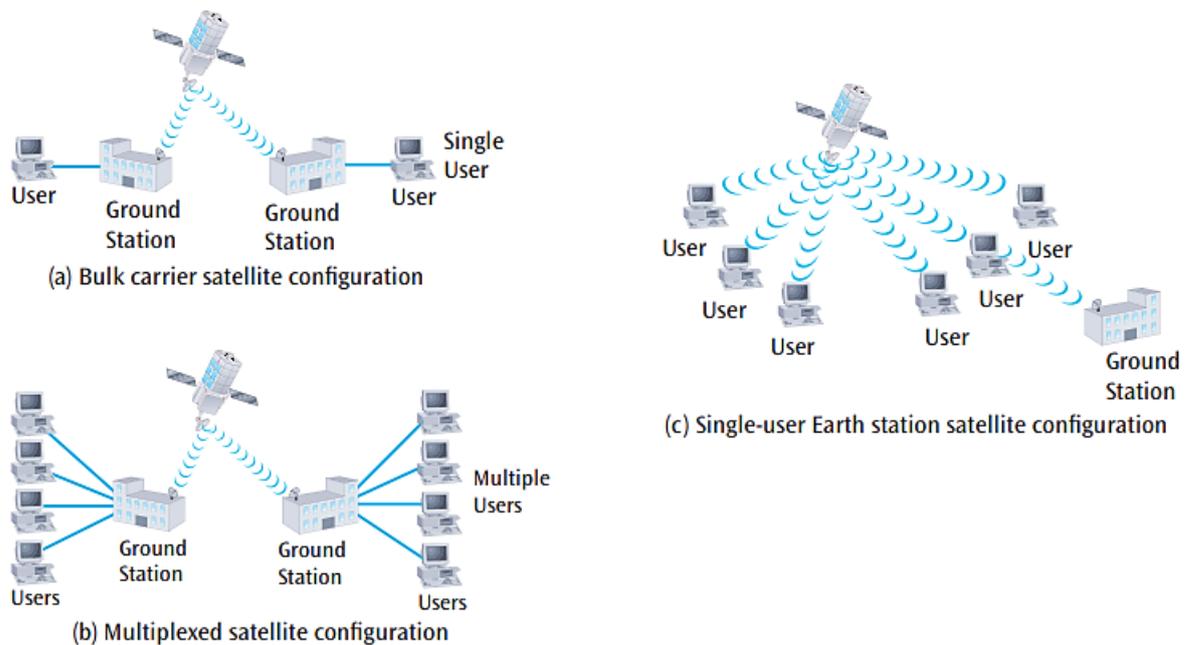
Bagaimana sistem satelit jenis ini memenuhi permintaan pengguna dan menetapkan slot waktu? Setiap pengguna dapat ditanyai secara bergantian apakah dia memiliki data untuk dikirimkan; namun karena begitu banyak waktu yang terbuang selama proses permintaan, teknik ini tidak layak secara ekonomi. Skenario siapa cepat dia dapat, di mana setiap pengguna bersaing dengan pengguna lainnya, juga merupakan rancangan yang sangat tidak efisien. Teknik yang tampaknya paling berhasil untuk menetapkan akses ke sistem satelit multipleks adalah sistem reservasi.

Dalam sistem reservasi, pengguna melakukan reservasi untuk slot waktu mendatang. Ketika slot waktu yang dipesan tiba, pengguna mengirimkan datanya ke sistem. Ada dua jenis sistem reservasi: reservasi terpusat dan reservasi terdistribusi. Dalam sistem reservasi terpusat, semua reservasi dikirim ke lokasi pusat, dan situs tersebut menangani permintaan masuk. Dalam sistem reservasi terdistribusi, tidak ada situs pusat yang menangani reservasi, namun pengguna individu mencapai kesepakatan mengenai urutan transmisi.

Stasiun Bumi Pengguna Tunggal

Dalam sistem satelit stasiun Bumi pengguna tunggal, setiap pengguna menggunakan stasiun bumi miliknya sendiri untuk mengirimkan data ke satelit. Gambar 3.14(c) menunjukkan konfigurasi satelit stasiun bumi pengguna tunggal. Sistem Very Small Aperture Terminal (VSAT) adalah contoh sistem satelit stasiun Bumi pengguna tunggal dengan stasiun bumi sendiri dan antena kecil (lebar dua hingga enam kaki).

Di antara semua stasiun bumi pengguna terdapat satu stasiun master yang biasanya terhubung ke sistem komputer mirip mainframe. Stasiun bumi berkomunikasi dengan komputer mainframe melalui satelit dan stasiun induk. Pengguna akhir VSAT memerlukan unit dalam ruangan, yang terdiri dari transceiver yang menghubungkan sistem komputer pengguna dengan parabola luar (unit luar ruangan). Transceiver ini, yang berukuran kecil, mengirimkan sinyal ke dan menerima sinyal dari satelit LEO melalui parabola. VSAT mampu menangani sinyal data, suara, dan video di sebagian besar permukaan bumi.



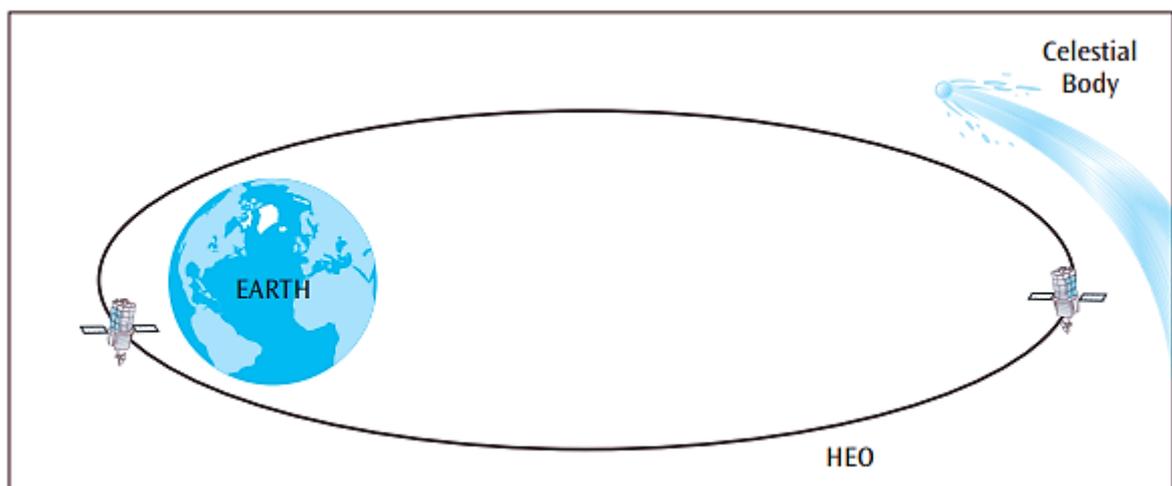
Gambar 3.14 Fasilitas pembawa massal, stasiun bumi multipleks, dan konfigurasi sistem satelit stasiun bumi pengguna tunggal

Satelit orbit Bumi Tengah digunakan terutama untuk aplikasi navigasi permukaan sistem penentuan posisi global. Sistem penentuan posisi global (global positioning system) merupakan sistem yang kompleks, namun ada baiknya kita melihat sekilas cara kerjanya. Sistem penentuan posisi global (GPS) adalah sistem 24 satelit yang diluncurkan oleh Departemen Pertahanan AS dan digunakan untuk mengidentifikasi lokasi di Bumi. Dengan melakukan triangulasi sinyal dari setidaknya empat satelit GPS (masing-masing menyediakan koordinat arah X, Y, Z, dan waktu), unit penerima dapat menentukan lokasinya saat ini dalam jarak beberapa meter di mana pun di Bumi. Banyak perusahaan sekarang memproduksi perangkat GPS genggam dan otomotif, yang akurat dalam jarak beberapa meter, dan produsen mobil besar menawarkan mobil dengan GPS bawaan sehingga pelanggan mereka dapat mengakses petunjuk arah mengemudi dan bahkan lokasi pompa bensin terdekat saat

mengemudi di kendaraan mereka. mobil. Sistem ini juga memungkinkan produsen untuk menentukan, jika pengemudi hilang atau mengalami kecelakaan, lokasi mobilnya di mana pun di negara tersebut.

Satelit Geosynchronous-Earth-orbit (GEO) ditemukan 36.000 kilometer (22.300 mil) dari Bumi dan selalu ditempatkan pada titik yang sama di Bumi (di suatu tempat di atas khatulistiwa). Dengan demikian, dua stasiun bumi dapat melakukan transmisi terus menerus dari Bumi ke satelit dan kembali ke Bumi. Satelit geosynchronous-orbit bumi paling sering digunakan untuk relay sinyal untuk siaran, kabel, dan televisi langsung; meteorologi; operasi intelijen pemerintah; dan telepon seluler maritim. Keuntungan utama satelit GEO adalah kapasitasnya untuk mengirimkan transmisi massal berkecepatan tinggi dan dalam jumlah besar yang dapat mencakup hingga sepertiga permukaan bumi. Perusahaan yang mengoperasikan satelit GEO dapat menyerahkan seluruh sumber daya transmisinya ke satu klien atau dapat berbagi waktu satelit dengan banyak klien. Penggunaan sistem satelit GEO oleh satu klien memerlukan biaya yang mahal dan biasanya melibatkan transfer data dalam jumlah besar. Diperkirakan 360 satelit GEO berada di orbit pada akhir tahun 2009.

Sistem satelit keempat yang memiliki sifat unik adalah satelit yang sangat elips (HEO), yang digunakan oleh pemerintah untuk memata-matai (melalui fotografi satelit) dan oleh lembaga ilmiah untuk mengamati benda langit. Satelit HEO mengikuti pola elips, seperti yang ditunjukkan pada Gambar 3-15. Saat satelit berada pada perigee (titik terdekat dengan Bumi), satelit akan mengambil foto Bumi. Ketika satelit mencapai apogee (titik terjauh dari Bumi), satelit mengirimkan data ke stasiun bumi. Pada puncaknya, satelit juga dapat memotret objek di luar angkasa.



Gambar 3.15 Diagram satelit orbit Bumi yang sangat elips

Satelit dan sistem gelombang mikro terestrial juga dapat dikategorikan berdasarkan frekuensi transmisi sistem, atau pita satelit. Semua sistem transmisi radio, seperti satelit, gelombang mikro berbasis darat, serta sistem televisi dan radio, memancarkan sinyalnya dalam pita transmisi yang disetujui FCC. Misalnya, pita radio menurut definisi ITU (International Telecommunication Union) adalah sebagai berikut:

Nomor Pita	Simbol	Frekuensi	Penggunaan Umum
4	VLF (frekuensi sangat rendah)	3–30kHz	Sistem navigasi radio
5	LF (frekuensi rendah)	30–300 kHz	Suar radio
6	MF (frekuensi sedang)	300kHz–3MHz	radio pagi
7	HF (frekuensi tinggi)	3–30MHz	radio CB
8	VHF (frekuensi sangat tinggi)	30–300MHz	TV VHF, radio FM
9	UHF (frekuensi sangat tinggi)	300MHz–3GHz	TV UHF, ponsel, pager
10	SHF (frekuensi super tinggi)	3–30GHz	Satelit
11	EHF (frekuensi sangat tinggi)	30–300GHz	Satelit, sistem radar

Banyak perangkat yang mengirimkan sinyal menggunakan pita radio di atas mengirimkan sinyalnya secara siaran, di mana sinyal tersebut merambat keluar dari menara transmisi ke segala arah. Sebaliknya, sebagian besar gelombang mikro terestrial dan sistem satelit mengirimkan sinyalnya dalam jalur garis pandang yang sempit dan sering dikategorikan berdasarkan pita radar. IEEE dan NATO telah menetapkan pita radar berikut:

Pita Radar	Frekuensi	Penggunaan Umum
L	~1–2GHz	GPS, penggunaan pemerintah, ponsel GSM
S	2–4GHz	Sistem cuaca, sistem radio satelit digital
C	4–8GHz	Sistem satelit komersial
X	~7–12,5GHz	Beberapa satelit komunikasi, cuaca
Ku	12–18GHz	NASA, stasiun televisi remote ke stasiun
KA	18–40GHz	Satelit komunikasi
V	50–75GHz	Tidak banyak digunakan
W	75–111GHz	Lain-lain (militer, sistem radar mobil)

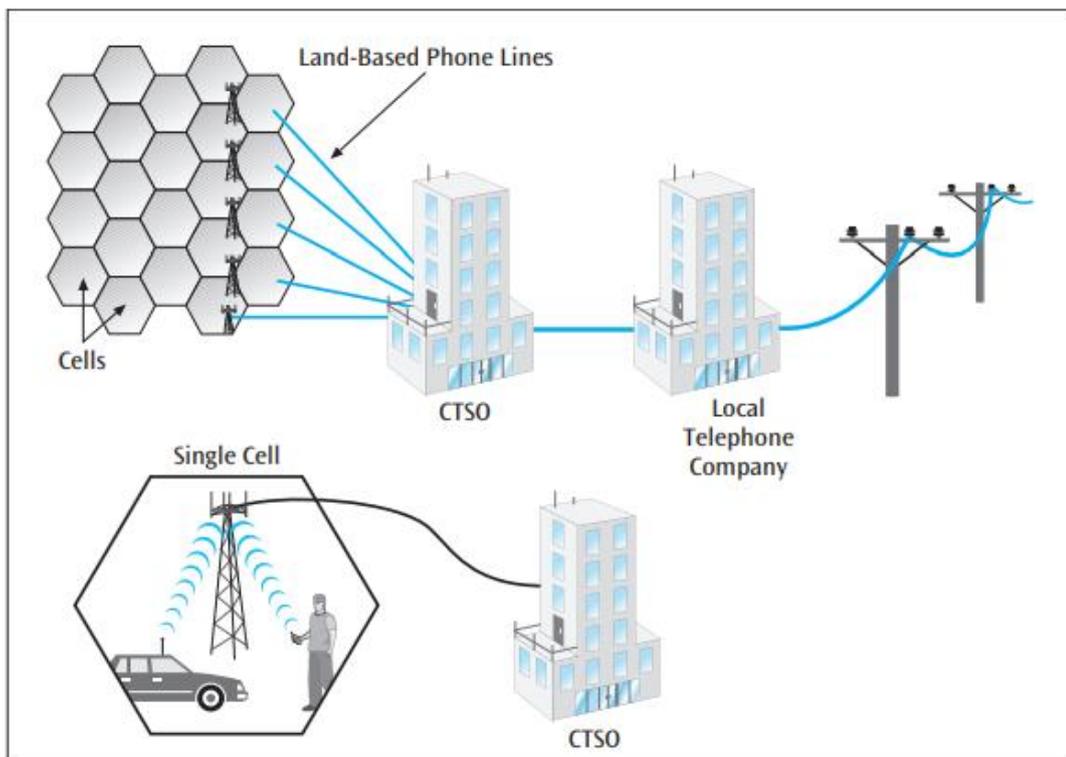
Perhatikan tumpang tindih antara dua konvensi penamaan. Pita radio SHF (3–30 GHz) berbagi frekuensi yang sama dengan pita radar L dan S (masing-masing 1–2 GHz dan 2–4 GHz).

Handphone

Teknologi nirkabel lain yang menggunakan gelombang radio adalah sistem telepon seluler, atau telepon seluler. Lima generasi dasar sistem telepon seluler telah diciptakan sejauh ini: telepon seluler analog generasi pertama; Layanan Komunikasi Pribadi (PCS) digital generasi kedua; generasi ketiga (yang menariknya diberi label generasi 2.5), yang melihat konvergensi sinyal data dengan sinyal suara; generasi ketiga (3G), yang melibatkan kecepatan transfer data lebih tinggi; dan ponsel generasi keempat (4G) saat ini. Selama tahun 1980an dan 1990an, banyak orang membawa pager sebagai sarana untuk tetap berhubungan dengan bisnis atau keluarga mereka. Pada pergantian abad, ketika telepon seluler semakin populer, penggunaan pager menurun, dan dalam beberapa tahun terakhir, bahkan dapat dikatakan bahwa telepon seluler telah menggantikan pager. Telepon seluler telah menjadi begitu populer sehingga, menurut Forrester Research, sebuah kelompok pengawas telekomunikasi, pada bulan Februari 2011, 81 persen orang dewasa memiliki telepon seluler, dan 25 persen

dari seluruh rumah tangga di AS hanya memiliki telepon seluler dan tidak memiliki telepon seluler. telepon rumah.21q

Istilah “ponsel” menimbulkan pertanyaan menarik: Apa arti istilah “sel” atau “seluler”? Untuk menjawab pertanyaan ini, Anda perlu mencermati jaringan radio interaktif yang ada pada tahun 1990-an, sebelum telepon seluler menjadi populer: Improved Mobile Telephone Service (IMTS). IMTS hanya mengizinkan 12 pengguna secara bersamaan dalam satu kota. Alasan mengapa begitu sedikit pengguna secara bersamaan telah disebutkan sebelumnya dalam bab ini: FCC hanya menyediakan sejumlah frekuensi radio untuk aplikasi tertentu. Saat pengguna berbicara dengan pengguna lain, diperlukan dua saluran. Satu saluran untuk transmisi satu arah, dan saluran kedua untuk arah sebaliknya. Setiap saluran memerlukan rentang frekuensi yang cukup untuk membawa sinyal suara. Untuk mendukung prospek ratusan dan ribuan pengguna secara bersamaan dalam wilayah metropolitan, diperlukan rentang frekuensi yang sangat luas. FCC tidak dapat mengalokasikan frekuensi sebanyak ini ke satu aplikasi, sehingga menciptakan alternatif dengan membagi negara menjadi lebih dari 700 wilayah layanan seluler (MSA), atau pasar. Setiap pasar, yang biasanya mencakup seluruh wilayah metropolitan, dipecah lagi menjadi sel-sel yang berdekatan (seperti yang ditunjukkan pada sudut kiri atas Gambar 3-16). Perhatikan bagaimana sel-selnya membentuk pola seperti sarang lebah.



Gambar 3-16 Satu pasar ponsel dibagi menjadi beberapa sel

Ukuran sel dapat berkisar dari radius setengah mil hingga radius 50 mil. Terletak di persimpangan setiap sel adalah pemancar/penerima berdaya rendah, yang sering ditempatkan pada menara yang berdiri sendiri (lihat Gambar 3-17). Tidak lama setelah

menara-menara ini mulai bermunculan di lingkungan sekitar, warga mulai mengeluhkan keberadaannya. Akibatnya, perusahaan telepon seluler menjadi kreatif dalam menyamarkan antena mereka di bagian atas dan samping gedung serta di dalam menara gereja, dan bahkan mendesainnya dalam bentuk pohon (lihat Gambar 3-18).



Gambar 3-18 Menara telepon seluler yang menyamar sebagai pepohonan

Telepon seluler di dalam sel berkomunikasi dengan menara seluler, yang selanjutnya dihubungkan ke kantor peralihan telepon seluler (CTSO) melalui saluran telepon. CTSO kemudian dihubungkan ke sistem telepon lokal. Jika ponsel berpindah dari satu sel ke sel lainnya, CTSO melepaskan koneksi dari satu sel ke sel lainnya.

Karena setiap sel menggunakan transmisi berdaya rendah, kecil kemungkinannya bahwa transmisi dalam satu sel tertentu akan mengganggu transmisi dalam sel lain yang jaraknya lebih dari satu atau dua sel. Jadi, hanya sel yang berdekatan yang perlu menggunakan rangkaian frekuensi berbeda. Hasilnya, frekuensi yang digunakan dalam sebuah sel dapat digunakan kembali di sel lain, sehingga memungkinkan lebih banyak koneksi simultan di suatu pasar dibandingkan frekuensi yang tersedia.

Di setiap sel, setidaknya satu saluran, saluran pengaturan, bertanggung jawab atas pengaturan dan pengendalian panggilan. Segera setelah telepon seluler dihidupkan, telepon mengunci saluran pengaturan dan mengirimkan nomor identifikasi selulernya (MIN). Perusahaan telepon seluler menerima MIN dan mengidentifikasi telepon tertentu (dan pengguna). Sekarang jaringan telepon seluler mengetahui di mana sel pengguna berada. Setiap beberapa detik, telepon seluler mengirimkan ulang MIN-nya, untuk berjaga-jaga jika telepon tersebut benar-benar bergerak.

Pada sistem telepon seluler generasi sebelumnya, perusahaan telepon seluler hanya dapat mengetahui nomor telepon seluler di mana Anda berada. Ia tidak dapat menentukan dengan tepat di mana Anda berada di sel tersebut. Tak lama setelah tahun 2000, FCC meminta perusahaan telepon seluler untuk merancang sistem yang dapat menentukan lokasi pasti telepon seluler. Salah satu ide di balik fitur ini adalah memungkinkan layanan darurat menemukan lokasi pengguna ponsel jika pengguna meminta layanan 911. FCC memberi waktu kepada perusahaan telepon seluler hingga akhir tahun 2005 untuk mengaktifkan 95 persen telepon seluler mereka dengan chip GPS sehingga dalam situasi darurat, perusahaan telepon seluler dapat menemukan lokasi telepon seluler dan penggunanya dalam jarak 100 kaki. Tentu saja, tidak semua perusahaan telepon seluler dapat memenuhi persyaratan ini dan beberapa di antaranya didenda. Saat ini, semua perusahaan telepon seluler dapat menawarkan layanan ini.

Ponsel, ketika mencoba melakukan panggilan, mentransfer nomor telepon yang dihubungi beserta identifikasi lainnya, seperti MIN ponsel, ke CTSO melalui saluran pengaturan. Akun pengguna diperiksa keabsahannya, dan jika tagihan telepon telah dibayar, CTSO memberikan saluran ke sambungan tersebut. Ponsel kemudian melepaskan saluran pengaturan, mengambil saluran yang ditetapkan, dan mulai melakukan panggilan telepon.

Apa yang terjadi ketika seseorang mencoba menelepon ponsel? Karena perusahaan telepon seluler mengetahui (jika telepon dihidupkan) di mana telepon seluler berada, maka perusahaan telepon seluler mengirimkan ID telepon seluler di dalam satu sel tersebut. Ketika ID dikenali oleh ponsel, ponsel mencoba mengambil saluran pengaturan sel lokal. Ketika saluran pengaturan disita, telepon seluler mengirimkan sinyal ke CTSO, CTSO memverifikasi nomor ID seluler, saluran ditetapkan ke telepon seluler, dan panggilan masuk tersambung.

Saat ini, sejumlah teknologi telepon seluler beroperasi di Amerika Serikat. Advanced Mobile Phone Service (AMPS) adalah sistem telepon seluler generasi pertama; itu mencakup hampir seluruh Amerika Utara dan ditemukan di lebih dari 35 negara lainnya. AMPS menggunakan teknologi multipleksing pembagian frekuensi (dibahas secara rinci di Bab Lima), yang beroperasi seperti transmisi televisi. AMPS adalah perangkat seluler yang setara dengan "sistem telepon lama biasa" (POTS). Tidak ada lagi perusahaan seluler AS yang menawarkan layanan AMPS. Layanan Telepon Seluler Digital-Advanced (D-AMPS) adalah layanan telepon seluler analog yang setara dengan digital. Ia menggunakan teknologi multiplexing pembagian waktu (juga dibahas dalam Bab Lima) selain multiplexing pembagian frekuensi dan memberikan kejelasan dan keamanan sinyal yang lebih baik daripada AMPS. Karena D-AMPS dimulai dengan multiplexing pembagian frekuensi dan kemudian menambahkan teknik

multiplexing pembagian waktu, sistem telepon seluler analog dapat ditingkatkan ke D-AMPS—suatu peningkatan yang meningkatkan kejelasan sinyal, fitur keamanan, jumlah layanan khusus yang ditawarkan, dan jumlah saluran yang tersedia per sel. Sebagian besar penyedia layanan seluler telah meningkatkan ponsel AMPS mereka ke layanan D-AMPS untuk bersaing dengan layanan digital yang lebih baru.

Kategori teknologi telepon seluler berikutnya adalah Personal Communications Services (PCS), yang tidak bergantung pada teknik analog lama. Sistem ini dianggap sebagai ponsel generasi kedua. Telepon seluler PCS disetujui oleh FCC pada tahun 1993, dan sistem telepon seluler PCS pertama muncul di Washington, D.C., pada bulan November 1995. Sejak itu, tiga teknologi PCS yang bersaing (dan tidak kompatibel) telah muncul. Teknologi PCS pertama menggunakan bentuk multiplexing pembagian waktu yang disebut teknologi Time Division Multiple Access (TDMA) untuk membagi saluran pengguna yang tersedia berdasarkan waktu, memberikan setiap telepon seluler yang melakukan transmisi waktu singkat untuk melakukan transmisi. Teknologi PCS yang kedua menggunakan teknologi Code Division Multiple Access (CDMA), yang menyebarkan transmisi sinyal ponsel pada rentang frekuensi yang luas, menggunakan nilai matematika. CDMA didasarkan pada teknologi spektrum tersebar, yang akan diperkenalkan pada Bab Dua Belas. Teknologi PCS yang ketiga adalah Global System for Mobile (GSM) Communications, yang menggunakan bentuk teknologi TDMA yang berbeda.

Setelah PCS, layanan telepon seluler generasi berikutnya seharusnya menjadi generasi ketiga, namun karena sejumlah alasan (yang paling jelas, fakta bahwa layanan ini mewakili peningkatan kecil dalam teknologi dibandingkan dengan generasi sebelumnya), layanan telepon seluler industri telepon menjulukinya generasi 2,5. Ponsel generasi 2,5 mampu menerima dan mengirimkan data digital antara ponsel dan penyedia layanan Internet. Dengan menggunakan ponsel yang memiliki layar kecil, pengguna dapat mendownload sejumlah kecil informasi dari Internet. Contoh jenis data yang dapat diunduh mencakup harga saham, cuaca, skor olahraga, petunjuk arah perjalanan, dan informasi berbasis teks bervolume rendah lainnya. Banyak ponsel juga memiliki kamera internal, dan pengguna dapat mengirim gambar dari satu ponsel ke ponsel lainnya.

Untuk mendukung aliran data teks dan gambar yang lebih intensif bandwidth pada generasi 2.5, protokol baru untuk transmisi data dengan kecepatan lebih tinggi dikembangkan. Secara khusus, jaringan GSM diubah menjadi General Packet Radio Service (GPRS) yang dapat mengirimkan data pada 30 kbps hingga 40 kbps. Jaringan CDMA diubah menjadi bentuk CDMA terbaru yang disebut CDMA2000 1xRTT (Teknologi Transmisi Radio satu operator). Teknologi terbaru ini mampu mentransmisikan data dengan kecepatan 50 kbps hingga 75 kbps.

Teknologi telepon seluler generasi berikutnya dimulai pada awal tahun 2005 dan sebenarnya mewakili generasi ketiga. Untuk mendukung peningkatan kebutuhan bandwidth untuk mengunggah dan mengunduh teks dan gambar melalui telepon seluler, sistem GPRS diubah menjadi teknologi Universal Mobile Telecommunication System (UMTS). UMTS mampu mendukung kecepatan data hilir 220 kbps hingga 320 kbps. Sistem 1xRTT diubah

menjadi teknologi yang disebut 1xEV (1 x Enhanced Version)—khususnya, versi 1xEV yang disebut Evolution Data Only (EV-DO). Sistem EV-DO mampu mendukung kecepatan data hilir 300 kbps hingga 500 kbps. Sistem generasi keempat, yang mulai muncul pada tahun 2010, saat ini didasarkan pada teknologi LTE (Long Term Evolution) atau WiMAX (akan dibahas segera). Bahkan ada yang berpendapat bahwa LTE yang muncul di beberapa ponsel saat ini belum 4G, melainkan mendekati. LTE Advanced, yang belum diproduksi pada musim panas 2011, akan dianggap sebagai 4G sejati. Bingung? Anda tidak sendiri.

Sistem Nirkabel Broadband dan WiMax

Sistem nirkabel broadband, juga dikenal sebagai loop lokal nirkabel atau nirkabel titik tetap, adalah salah satu teknik terbaru untuk menyampaikan layanan Internet ke rumah dan bisnis. Sistem ini melewati loop lokal perusahaan telepon (saluran telepon terakhir antara kantor pusat telepon dan rumah atau bisnis) dengan mentransmisikan suara, data, dan video melalui frekuensi radio yang sangat tinggi. Seperti yang ditunjukkan Gambar 3-19, penyedia layanan nirkabel broadband (broadband switching center) menerima transmisi broadband baik dari sistem satelit atau koneksi Internet berkecepatan tinggi. Transmisi broadband ini kemudian dikirim ke satu atau lebih antena transmisi lokal (base station). Bisnis dan rumah kemudian menerima transmisi ini dengan antena parabola, yang mengubah sinyal menjadi sinyal yang sesuai untuk komputer atau jaringan komputer.

Pembelahan Saluran Antar Sel

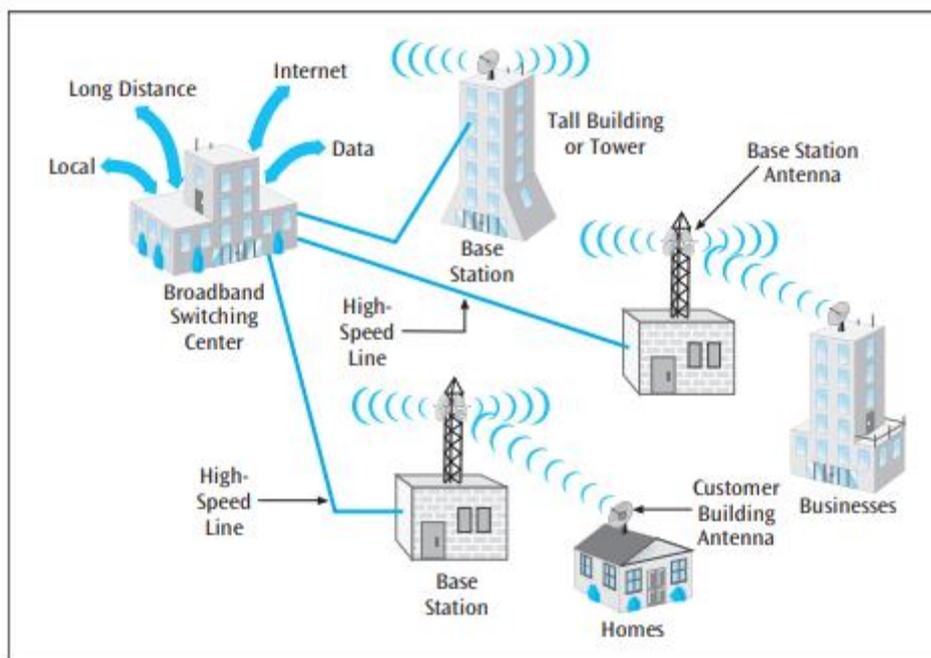
Untuk mendapatkan pemahaman yang lebih baik tentang bagaimana frekuensi dibagi di antara sel-sel sistem telepon seluler, mari kita lihat contoh sederhana: sistem telepon seluler generasi pertama. Sistem telepon seluler AMPS dan D-AMPS mengalokasikan salurannya menggunakan rentang frekuensi dalam spektrum 800–900 MHz. Lebih tepatnya, rentang 824–849 MHz digunakan untuk menerima sinyal dari telepon seluler (uplink), sedangkan rentang 869–894 MHz digunakan untuk mentransmisikan sinyal ke telepon seluler (downlink). Dalam wilayah metropolitan, kedua pita frekuensi ini memungkinkan sekitar 50 MHz di mana sinyal dapat ditransmisikan. Pita frekuensi ini dibagi lagi menjadi sub-pita 30 kHz yang disebut saluran. Pembagian spektrum menjadi saluran-saluran sub-band dicapai melalui Frekuensi Division Multiple Access (FDMA), dimana setiap saluran ditetapkan (seperti halnya televisi dan radio) serangkaian frekuensi berbeda untuk ditransmisikan.

Sebanyak 1666 saluran tersedia untuk transmisi sinyal di wilayah metropolitan (50 MHz dibagi 30 kHz per saluran menghasilkan 1666 saluran). Untuk melakukan percakapan dua arah pada telepon seluler, diperlukan dua saluran: satu untuk uplink dan satu lagi untuk downlink. Karena setiap percakapan memerlukan dua saluran, 833 (1666 saluran dibagi dua) koneksi dua arah tersedia di wilayah metropolitan. Selain itu, FCC mengizinkan hingga dua operator yang bersaing untuk menawarkan layanan telepon seluler AMPS di wilayah metropolitan mana pun. Dengan demikian, 416 koneksi per operator (833 koneksi dibagi 2 operator) per wilayah metropolitan tersedia untuk digunakan. Akhirnya, 416 koneksi ini dibagi ke seluruh sel di wilayah metropolitan. Dengan demikian, wilayah metropolitan seperti New York City dapat memiliki dua perusahaan telepon seluler, masing-masing hanya menawarkan 416 panggilan telepon secara bersamaan untuk seluruh kota. Untungnya, ada satu langkah

penting lagi. Ingatlah bahwa sel-sel di suatu area membentuk pola sarang lebah (pola sarang lebah tersebut bagus di atas kertas, namun tidak begitu rapi di kehidupan nyata), dan rangkaian frekuensi dapat digunakan kembali. Karena hanya frekuensi dalam sel yang berdekatan yang unik, perusahaan telepon seluler mengelompokkan tujuh sel menjadi satu. Jadi, hanya diperlukan tujuh set frekuensi; rumpun tujuh sel berikutnya dapat menggunakan kembali tujuh set frekuensi ini. Hal ini mengakibatkan 59 koneksi dua arah per sel (416 dibagi 7) per operator tersedia di wilayah metropolitan. 59 koneksi ini semakin dikurangi dengan fakta bahwa beberapa saluran di setiap sel digunakan untuk pengaturan panggilan.

Meskipun 59 koneksi AMPS yang tersedia per sel tampaknya bukan jumlah yang besar dibandingkan dengan jumlah total pengguna telepon seluler di suatu wilayah, ingatlah fakta berikut:

- Pengguna telepon seluler dalam suatu seluler tidak semuanya menggunakan telepon mereka secara bersamaan.
- Sel bisa berukuran sekecil setengah mil.
- Ada beberapa penyedia layanan untuk sistem AMPS dan D-AMPS.



Gambar 3-19 Konfigurasi nirkabel broadband di wilayah metropolitan

Dua teknologi transmisi nirkabel pita lebar diperkenalkan pada pergantian abad ke-21—Layanan Distribusi Multipoint Lokal (LMDS) dan Layanan Distribusi Multisaluran Multipoint (MMDS)—namun keduanya sudah ketinggalan zaman. Sebagai gantinya adalah teknologi baru: WiMax.

WiMax adalah teknologi transmisi nirkabel broadband yang didasarkan pada serangkaian standar IEEE. Misalnya, teknologi WiMax yang dirancang untuk memberikan akses Internet berkecepatan tinggi ke rumah dan usaha kecil sehingga bersaing dengan DSL dan modem kabel disebut IEEE 802.16a. IEEE 802.16a beroperasi pada spektrum 2–11 GHz,

menyediakan koneksi line-of-sight dan non-line-of-sight, dan dapat mentransfer data hingga 70 Mbps sejauh 30 mil.

Teknologi WiMax lainnya, IEEE 802.16c, dirancang untuk beroperasi pada spektrum 10–66 GHz dan hanya beroperasi secara saling berhadapan. IEEE 802.16d (terkadang disebut IEEE 802.16–2004) menggabungkan revisi 802.16a dan 802.16c menjadi satu standar. IEEE 802.16e merupakan revisi dari standar 802.16.

Standar yang menyediakan koneksi berkecepatan tinggi untuk perangkat yang bergerak lambat, seperti saat seseorang sedang berjalan atau berkendara di jalan perumahan dan menggunakan ponsel berkemampuan WiMax. Karena 802.16 awalnya dirancang untuk perangkat tetap, namun revisi 802.16e bukanlah standar optimal untuk perangkat bergerak secara umum. Yang lebih disukai adalah standar IEEE 802.20, yang dirilis pada tahun 2008. Standar IEEE 802.20, yang dibuat khusus untuk perangkat seluler berkecepatan tinggi—dalam hal ini, “kecepatan tinggi” mengacu pada kecepatan data dan kecepatan pergerakan perangkat dapat mengalaminya saat terhubung. IEEE 802.20 dapat beroperasi dengan perangkat yang bergerak hingga 180 mil per jam, secara efektif melakukan handoff (pengalihan dari satu rangkaian frekuensi transmisi ke rangkaian berikutnya), dan dapat mengirimkan data dalam kisaran ratusan kbps hingga lebih dari satu juta bit per detik. Namun ada juga pengerjaan pada standar WiMax lainnya: IEEE 802.16n. Spesifikasi ini diperkirakan akan menghadirkan koneksi tetap 10 Gbps dan koneksi seluler 1 Gbps. Ini mungkin juga disebut WiMax 3.0.

Bluetooth

Protokol Bluetooth—yang diambil dari nama pejuang Viking Harald Bluetooth, yang menyatukan Denmark dan Norwegia pada abad kesepuluh—adalah teknologi nirkabel yang menggunakan frekuensi radio berdaya rendah dan jarak pendek untuk berkomunikasi antara dua perangkat atau lebih. Lebih tepatnya, Bluetooth menggunakan pita ISM (Industri, Ilmiah, Medis) 2,45 GHz dan biasanya dibatasi pada jarak antara 10 cm dan 10 meter (masing-masing setara dengan sekitar 4 inci dan 30 kaki). Tidak seperti inframerah, Bluetooth mampu melakukan transmisi melalui benda bukan logam. Dengan demikian, perangkat yang memancarkan sinyal Bluetooth dapat dibawa dalam saku, tas, atau tas kerja. Selain itu, Bluetooth dapat mentransfer data dengan kecepatan yang cukup tinggi. Standar Bluetooth pertama mampu mencapai kecepatan transfer data hingga sekitar 700 kbps. Standar kedua meningkatkan kecepatan data menjadi lebih dari 2 Mbps.

Bluetooth juga dapat berkomunikasi antar beberapa perangkat. Misalnya, pertimbangkan lingkungan kantor dengan banyak komputer, printer, mesin faks, dan mesin fotokopi. Dengan Bluetooth, setiap perangkat dapat mengirim sinyal ke perangkat lain atau ke satu titik—misalnya, untuk menunjukkan petunjuk layanan seperti “kertas habis” atau “toner hampir habis”. Jaringan kecil seperti ini dengan delapan perangkat atau kurang disebut piconet. Istilah lain untuk piconet adalah personal area network atau PAN, yang telah kami perkenalkan di Bab Satu. Beberapa piconet dapat dihubungkan untuk membentuk sebuah scatternet.

Aspek paling menarik dari Bluetooth adalah daftar aplikasi yang mendapat manfaat dari teknologi transmisi jarak pendek tersebut. Aplikasi ini meliputi:

- Transmisi nirkabel antara pemutar musik portabel dan headset
- Transmisi antara personal digital Assistant (PDA) dan komputer lain
- Transmisi antara perangkat periferal dan komputer
- Transmisi nirkabel antara PDA dan mobil, rumah, atau tempat kerja

Untuk menghargai potensi kekuatan teknologi Bluetooth, pertimbangkan contoh berikut yang lebih deskriptif: Anda dapat secara otomatis menyinkronkan semua pesan email antara PDA Anda dan komputer desktop/laptop Anda; saat Anda mendekati mobil Anda, PDA Anda akan memberitahu mobil untuk membuka kunci pintunya dan mengubah radio ke stasiun favorit Anda; saat Anda berjalan ke pintu depan rumah Anda, PDA Anda akan menginstruksikan rumah Anda untuk membuka kunci pintu depan, menyalakan lampu, dan menyalakan sistem hiburan, dan saat Anda duduk dalam pertemuan bisnis, PDA/laptop Anda akan melakukannya kirimkan presentasi slide Anda secara nirkabel ke proyektor dan catatan Anda ke PDA/laptop masing-masing peserta.

Meskipun mempunyai banyak dukungan, Bluetooth relatif lambat dalam mempengaruhi pasar. Teknologi Bluetooth saat ini masih mengalami masalah dalam mendapatkan beberapa (lebih dari dua) perangkat untuk menyinkronkan data satu sama lain. Jarak transmisi yang pendek yaitu 10 meter (30 kaki) juga dipandang oleh banyak orang sebagai suatu kerugian. Meskipun dimungkinkan (dalam kondisi khusus) untuk mengirimkan sinyal Bluetooth hingga 100 meter (328 kaki), hal ini memerlukan baterai yang lebih kuat untuk perangkat transmisi dan dapat meningkatkan masalah interferensi. Meski demikian, Bluetooth merupakan teknologi yang tentunya perlu diwaspadai dan dipahami.

Jaringan Area Lokal Nirkabel

Meskipun jaringan area lokal akan dibahas secara rinci di Bab Tujuh, mungkin ada gunanya memperkenalkan bentuk jaringan area lokal nirkabel sekarang, sementara kita membahas berbagai jenis sistem nirkabel. Standar jaringan area lokal nirkabel pertama diperkenalkan pada tahun 1997 oleh IEEE dan disebut IEEE 802.11. IEEE 802.11 mampu mendukung kecepatan data hingga 2 Mbps dan memungkinkan workstation nirkabel hingga jarak beberapa ratus kaki untuk berkomunikasi dengan titik akses. Jalur akses ini adalah koneksi ke bagian kabel dari jaringan area lokal. Pada tahun 1999, IEEE menyetujui protokol 11-Mbps baru, IEEE 802.11b. Protokol ini juga dikenal sebagai fidelitas nirkabel (Wi-Fi) dan mentransmisikan data dalam rentang frekuensi 2,4 GHz. Setelah 802.11b ada dua protokol lagi: 802.11a dan 802.11g. IEEE 802.11a mentransmisikan data dengan kecepatan hingga 54 Mbps (secara teoritis 54 Mbps namun kenyataannya sekitar setengahnya) menggunakan frekuensi dalam rentang 5-GHz. 802.11g juga mentransmisikan data dengan kecepatan hingga 54 Mbps (teoretis) tetapi menggunakan frekuensi yang sama—2,4 GHz—seperti 802.11b. Karena 802.11b dan 802.11g berbagi rentang frekuensi yang sama, 802.11g lebih menarik dibandingkan 802.11a bagi pengguna yang telah menginstal 802.11b dan ingin mengupgrade sistemnya. Awalnya, 802.11a disebut Wi-Fi5, namun istilah tersebut tidak lagi digunakan.

Protokol LAN nirkabel keempat yang disetujui pada akhir tahun 2009 adalah IEEE 802.11n. Standar ini mampu mendukung sinyal 100Mbps antar perangkat nirkabel dan menggunakan banyak antena untuk mendukung beberapa aliran data independen. Semua protokol ini—802.11a, 802.11b, 802.11g, dan 802.11n—kini disebut Wi-Fi.

Optik Ruang Bebas, Ultra-Wideband, Inframerah, dan ZigBee

Empat teknologi nirkabel tambahan yang layak disebutkan adalah optik ruang bebas, transmisi ultra-wideband, inframerah, dan ZigBee. Optik ruang bebas menggunakan laser, atau, dalam beberapa kasus, perangkat transmisi inframerah, untuk mengirimkan data antara dua bangunan dalam jarak pendek, seperti di seberang jalan. Kecepatan transfer data dengan teknologi ini bisa mencapai 1,25 Gbps, dan kecepatan yang lebih tinggi mungkin terjadi di masa depan. Namun, salah satu masalah utama dengan optik ruang bebas adalah kabut. Laser kehilangan kekuatannya saat ditransmisikan melalui kabut. Oleh karena itu, jika kabut tebal, jarak transmisi dapat dikurangi menjadi kurang dari 50 meter (150 kaki). Kilau, (seperti gelombang berkilauan yang Anda lihat di atas trotoar pada hari yang panas)” pergerakan bangunan, penyerapan oleh molekul air yang tersuspensi di udara, dan penghalang sementara seperti burung yang menghalangi sinar dapat mengurangi kecepatan data efektif optik ruang bebas. Meskipun demikian, optik ruang bebas adalah solusi menarik untuk aplikasi kabel non-konduksi berkecepatan tinggi.

Media nirkabel kedua adalah ultra-wideband. Sistem ultra-wideband mengirimkan data melalui rentang frekuensi yang luas dibandingkan membatasi transmisi pada pita frekuensi yang sempit dan tetap. Aspek yang menarik tentang transmisi pada rentang frekuensi yang luas adalah bahwa beberapa frekuensi tersebut digunakan oleh sumber lain, seperti sistem telepon seluler. Jadi apakah sinyal ultra-wideband mengganggu sinyal dari sumber lain? Pendukung ultra-wideband mengklaim bahwa, meskipun rentang frekuensi yang luas digunakan, ultra-wideband mentransmisikan pada tingkat daya yang cukup rendah sehingga sumber lain tidak terpengaruh. Penentang ultra-wideband berpendapat bahwa hal ini tidak benar—bahwa transmisi ultra-wideband memang mempengaruhi sumber lain dan, oleh karena itu, harus dikontrol dengan hati-hati. Terlepas dari masalah interferensi ini, ultra-wideband mampu mendukung kecepatan hingga 100 Mbps, namun pada jarak kecil seperti yang ditemukan di jaringan area lokal nirkabel.

Transmisi inframerah adalah bentuk khusus transmisi radio yang menggunakan sinar cahaya terfokus pada rentang frekuensi inframerah (1012–1014 MHz). Bekerja seperti perangkat kendali jarak jauh yang digunakan untuk mengoperasikan pesawat televisi, sinar informasi inframerah terfokus ini dikirim dari pemancar ke penerima melalui transmisi garis pandang. Biasanya perangkat ini hanya berjarak sekitar tiga hingga sepuluh kaki (satu hingga tiga meter), namun sistem inframerah yang dapat mentransmisikan hingga satu setengah mil memang ada.

Sistem transmisi inframerah sering dikaitkan dengan komputer laptop, komputer genggam, perangkat periferal seperti printer dan mesin faks, kamera digital, dan bahkan

permainan elektronik genggam anak-anak. Transmisi inframerah bekerja dengan baik dalam aktivitas berikut:

- Mengirimkan dokumen dari komputer laptop Anda ke printer atau modem
- Pertukaran file kecil seperti kartu nama antar komputer genggam
- Sinkronisasi buku telepon elektronik dan penjadwal
- Mengambil catatan bank dari anjungan tunai mandiri 24 jam dengan berjalan mendekati mesin dan mengarahkan perangkat genggam seperti PDA ke terminal

Dalam masing-masing contoh ini, pemancar dan penerima berada dalam ruangan yang sama atau berjarak dekat, dan kecepatan transfer data biasanya tidak lebih cepat dari 4 Mbps. Ada sistem inframerah yang dapat mentransfer data dengan kecepatan hingga 16 Mbps.

Meskipun Asosiasi Data Inframerah (IrDA) memimpin dalam standarisasi teknologi inframerah dan memasukkan inframerah ke dalam banyak bidang aplikasi, masih dipertanyakan apakah inframerah akan berkembang jauh melampaui penerapan yang ada saat ini. Bluetooth saat ini merupakan pesaing terkuat inframerah dan tampaknya memenangkan perang nirkabel khusus ini.

ZigBee adalah teknologi nirkabel yang relatif baru yang didukung oleh standar IEEE 802.15.4. Ini telah dirancang untuk transmisi data antara perangkat yang lebih kecil, sering kali tertanam, yang memerlukan kecepatan transfer data rendah (20–250 Kbps) dan konsumsi daya yang rendah. Misalnya, Aliansi ZigBee menyatakan bahwa ZigBee ideal untuk aplikasi seperti otomatisasi rumah dan gedung (pemanas, pendingin, keamanan, penerangan, dan detektor asap dan CO), kontrol industri, pembacaan meter otomatis, serta penginderaan dan pemantauan medis. Ia beroperasi pada pita radio ISM dan hanya memerlukan sedikit dukungan perangkat lunak dan daya yang sangat kecil. Faktanya, konsumsi daya sangat rendah sehingga beberapa pemasok mengklaim bahwa perangkat mereka yang dilengkapi ZigBee akan bertahan beberapa tahun dengan baterai aslinya.

Aspek menarik dari ZigBee adalah bagaimana perangkat mampu menjaga konsumsi daya tetap rendah. Teknik pertama yang digunakan adalah komunikasi mesh. Dengan menggunakan komunikasi mesh, semua perangkat tidak mengirimkan secara langsung ke satu penerima. Sebaliknya, setiap perangkat mengirimkan sinyalnya ke perangkat ZigBee terdekat berikutnya, yang kemudian meneruskan sinyal ini ke perangkat berikutnya. Pada akhirnya, penerima tujuan akan tercapai dan suatu tindakan akan dilakukan. Karena jarak transmisi biasanya lebih pendek dalam konfigurasi mesh, lebih sedikit daya yang diperlukan untuk mengirimkan sinyal.

Kedua, perangkat yang mendukung ZigBee tidak perlu terus-menerus berkomunikasi dengan perangkat lain. Saat tidak mengirimkan sinyal ke penerima, perangkat dapat masuk ke mode tidur. Ketika seseorang atau sesuatu mengaktifkan perangkat dengan ZigBee, sirkuit ZigBee akan aktif, mengirimkan sinyal, dan kemudian kembali ke mode tidur.

Karena banyak orang bingung membedakan ZigBee dengan Bluetooth, akan menarik untuk melihat apakah keduanya bertahan. Keduanya harus bertahan karena masing-masing menargetkan area aplikasi yang berbeda: Bluetooth adalah yang terbaik dalam menggantikan

kabel untuk jarak pendek, sementara ZigBee akan baik dalam mengirimkan sinyal berkecepatan rendah pada jarak pendek hingga menengah.

Tabel 3.4 merangkum media nirkabel yang dibahas di sini, termasuk penggunaan umum, kecepatan transfer data maksimum, jangkauan transmisi maksimum, kelebihan dan kekurangan masing-masing.

Tabel 3.4 Ringkasan media nirkabel

Jenis Media Nirkabel	Penggunaan Khas	Kecepatan Transfer Data Maksimum	Jangkauan Transmisi Maksimum	Keuntungan	Kekurangan
Gelombang Mikro Terrestrial	Telekomunikasi jarak jauh, gedung ke gedung	100s-Mbps	20-30 mil	Andal, kecepatan tinggi, volume tinggi	Jangka panjang, mahal untuk diterapkan, saling berhadapan.
Satelit LEO	Komunikasi seperti e-mail, paging, jaringan telepon seluler di seluruh dunia, mata-mata, penginderaan jauh, konferensi video	100s-Mbps	Tergantung pada jumlah satelit	Transfer berkecepatan tinggi, jarak sangat lebar, beberapa aplikasi tidak mahal	Beberapa aplikasi mahal, interferensi
Satelit MEO	Sistem navigasi permukaan bergaya GPS	100s-Mbps	Tergantung pada jumlah satelit	Transfer kecepatan tinggi, jarak jauh	Mahal untuk disewa, ada gangguan
GEO Satelit	Relai sinyal untuk televisi kabel dan langsung	100s-Mbps	Sepertiga keliling bumi (8000 mil)	Jarak yang sangat jauh, kecepatan tinggi, dan volume tinggi	Mahal untuk disewa, ada gangguan
Satelit HEO	Pengawasan global, aplikasi ilmiah	100s-Mbps	Variabel	Variabilitas jarak	Mahal
Seluler (AMPS dan D-AMPS)	Telepon seluler	19,2 kbps	Setiap sel: Radius 0,5-50 mil, tetapi cakupannya nasional	Aplikasi yang tersebar luas dan murah	Kebisingan
PCS	Telepon seluler	9,6 kbps	Setiap sel: radius 0,5-25 mil	Digital, kebisingan rendah	Kecepatan data lambat
GPRS, 1xRTT	Telepon seluler	30-75kbps	Sel fach: radius 0,5-25 mil	Digital, kebisingan rendah	Kecepatan data lambat
UMTS	Telepon seluler	320kbps	Setiap sel: radius 0,5-25 mil	Digital, kebisingan rendah	
EV-DO	Telepon seluler	500kbps	Setiap sel: radius 0,5-25 mil	Digital, kebisingan rendah	
Inframerah	Transfer data jarak pendek	16Mbps	1,5 mil	Cepat, murah, aman	Jarak pendek, saling berhadapan
WIMAX	Akses Internet nirkabel	30Mbps	30 mil	Kecepatan tinggi	

Bluetooth	Perpindahan jarak pendek	722kbps	30 kaki (10 meter)	Protokol universal	Jarak Terbatas
LAN nirkabel	Jaringan area lokal	100Mbps	< 328 kaki (< 100 meter)	Kasus penggunaan relatif	Beberapa standar
Optik Ruang Bebas	Transfer jarak pendek dan berkecepatan tinggi	45Mbps	1000s fcct (100s meter)	Kecepatan tinggi	Garis pandang, dipengaruhi oleh kabut
Pita lebar ultra	Transfer jarak pendek dan berkecepatan tinggi	100Mbps	<328 kaki (100 meter)	Kecepatan tinggi, tidak terbatas pada frekuensi tetap	Dapat mengganggu sumber lain
ZigBee	Transfer jarak pendek hingga menengah, kecepatan rendah	250 KBps	Jarak tak terbatas (mesh)	Daya rendah	Kecepatan transfer rendah

Sekarang setelah Anda memahami kategori dan jenis media nirkabel dan media konduksi yang tersedia, Anda perlu mempertimbangkan kriteria lain untuk membuat keputusan tentang media mana yang akan dipilih.

3.4 KRITERIA PEMILIHAN MEDIA

Saat merancang atau memperbaiki jaringan komputer, memilih satu jenis media dibandingkan yang lain merupakan masalah penting. Proyek berbasis jaringan komputer mempunyai kinerja yang buruk dan bahkan mungkin gagal karena keputusan yang buruk mengenai jenis media yang tepat. Selain itu, perlu dicatat bahwa harga pembelian dan biaya pemasangan untuk media tertentu seringkali merupakan biaya terbesar yang terkait dengan jaringan komputer. Setelah waktu dan uang dihabiskan untuk memasang media tertentu, sebuah bisnis harus menggunakan media yang dipilih selama beberapa tahun untuk menutup biaya awal tersebut. Singkatnya, pemilihan media tidak boleh dianggap enteng. Dengan asumsi Anda memiliki pilihan untuk memilih media, Anda harus mempertimbangkan banyak kriteria pemilihan media sebelum membuat pilihan akhir. Faktor utama yang harus Anda pertimbangkan dalam keputusan Anda meliputi biaya, kecepatan, perluasan dan jarak, lingkungan, dan keamanan. Pembahasan berikut akan mempertimbangkan faktor-faktor ini sehubungan dengan kabel twisted pair, kabel koaksial, kabel serat optik, gelombang mikro terestrial, gelombang mikro satelit, sistem seluler, inframerah, WiMax, Wi-Fi, dan Bluetooth.

Yang terakhir, jangan lupa tentang jalur kanan dan garis pandang. Right-of-way melibatkan kemampuan untuk menempatkan kabel fisik di atas properti umum atau milik pribadi orang lain. Jika Anda tidak memiliki jalur yang benar, Anda tidak dapat memasang kabel apa pun. Line-of-sight berhubungan dengan sinyal nirkabel. Beberapa bentuk sinyal nirkabel hanya dapat beroperasi bila pemancar dan penerima berada dalam jarak pandang satu sama lain.

Biaya

Biaya dikaitkan dengan semua jenis media, dan terdapat berbagai jenis biaya. Misalnya, kabel twisted pair umumnya lebih murah dibandingkan kabel serat optik dan kabel

koaksial. Namun, untuk membuat keputusan pemilihan yang hemat biaya, penting untuk mempertimbangkan lebih dari sekedar biaya awal kabel— Anda juga harus mempertimbangkan biaya perangkat pendukung yang memulai dan mengakhiri kabel, biaya pemasangan, dan harga / rasio kinerja. Misalnya, kawat twisted pair biasanya merupakan media yang paling murah untuk dibeli. Setiap kabel biasanya diakhiri dengan soket modular kecil yang mirip dengan soket yang menghubungkan telepon ke soket telepon di dinding. Dongkrak modular ini sebagian besar terbuat dari plastik dan sangat murah, masing-masing hanya berharga beberapa sen. Pemasangan twisted pair biasanya mudah dilakukan, namun biayanya bisa sangat mahal tergantung pada lingkungan pemasangan tertentu dan siapa yang melakukan pemasangan.

Sebagai perbandingan, kabel koaksial seringkali merupakan kabel yang lebih mahal untuk dibeli, terkadang harganya lebih dari Rp. 15.000 per kaki. Konektor yang mengakhiri kabel koaksial sebagian besar terbuat dari logam dan sedikit lebih mahal dibandingkan konektor twisted pair. Memasang kabel koaksial juga sedikit lebih sulit daripada kabel twisted pair.

Kabel serat optik, jika dibeli dengan dua konduktor dan dalam jumlah besar, lebih mahal daripada kabel twisted pair tetapi biayanya sebanding dengan kabel koaksial. Konektor yang mengakhiri kabel serat optik, seperti disebutkan sebelumnya, lebih mahal dibandingkan kabel twisted pair atau kabel koaksial. Yang lebih penting lagi, jika Anda perlu menyambungkan kabel serat optik ke kabel atau perangkat non-serat optik, kenaikan biayanya bahkan lebih besar lagi karena Anda harus mengubah gelombang cahaya menjadi sinyal listrik dan sebaliknya. Meskipun biaya pemasangan ketiga media yang dilakukan tidak selalu berbeda secara signifikan, namun seringkali yang terkait dengan kabel serat optik adalah yang paling mahal. Namun pertimbangkan rasio harga/kinerja kabel serat optik dibandingkan dengan kabel twisted pair dan kabel koaksial. Meskipun fiber mungkin sedikit lebih mahal untuk dibeli dan dipasang, fiber memiliki kemampuan transmisi terbesar dengan tingkat kebisingan yang paling sedikit. Mana yang lebih penting: menghemat uang untuk pembelian suatu media, atau memiliki media yang mampu menghasilkan kecepatan transmisi yang sangat tinggi?

Sistem gelombang mikro terestrial yang menjangkau jarak jauh dan sistem satelit merupakan media yang mahal, mengingat biaya menara gelombang mikro dan satelit. Namun sangat sedikit perusahaan yang memasang menara sendiri dan meluncurkan satelitnya sendiri. Sebaliknya, sebagian besar perusahaan menyewa waktu dari perusahaan lain yang berspesialisasi dalam sistem gelombang mikro. Mempertimbangkan opsi sewa, dan fakta bahwa sistem gelombang mikro dapat mengirimkan aliran data dengan cepat, beberapa perusahaan mungkin menemukan solusi gelombang mikro yang lebih murah dibandingkan solusi berbasis kabel. Sistem gelombang mikro milik swasta, yang dipasang di gedung-gedung perusahaan, jauh lebih murah dibandingkan sistem gelombang mikro dan satelit terestrial dengan area luas. Mengingat biaya pemasangan kabel (dengan asumsi Anda dapat memasangnya), sistem gelombang mikro jarak pendek mungkin, dalam situasi tertentu, juga

menawarkan alternatif yang masuk akal untuk memasang kabel atau menyewa waktu dari penyedia layanan.

Dalam banyak kasus, tidak mungkin memasang kabel Anda sendiri. Misalnya, jika Anda memiliki dua gedung yang dipisahkan oleh jalan umum, Anda mungkin tidak memiliki cara untuk menyambungkan kabel dari satu gedung ke gedung lainnya. Sekalipun ada jalan di atas atau di bawah tanah yang bisa dilalui kabel, apakah Anda pemilik jalan itu? Dengan kata lain, Anda mungkin tidak mempunyai hak untuk memasang kabel. Jika jalur tersebut bukan milik Anda, apakah pemilik jalur tersebut akan mengizinkan Anda memasang kabel melalui jalur tersebut? Dan jika ya, berapa biayanya bagi Anda? Jika tidak mungkin atau tidak layak untuk memasang kabel Anda sendiri, Anda dapat mempertimbangkan beberapa bentuk transmisi nirkabel. Atau, Anda dapat mempertimbangkan untuk menghubungi penyedia layanan telekomunikasi lokal (seperti perusahaan telepon lokal) untuk mengetahui opsi apa saja yang tersedia (lebih lanjut mengenai hal ini di Bab Sebelas).

Setiap jenis media memiliki tambahan biaya pemeliharaan. Akankah jenis kawat tertentu bertahan selama x tahun jika terkena lingkungan tertentu? Ini adalah pertanyaan yang sulit untuk dijawab, namun sebaiknya ditanyakan kepada perusahaan yang memasok media tersebut. Meskipun mudah untuk menelusuri katalog dan mempelajari biaya awal suatu jenis kabel tertentu, lebih sulit untuk menentukan biaya pemeliharaan dalam dua, lima, atau sepuluh tahun ke depan. Seringkali, terlalu fokus pada biaya awal menghambat pengambil keputusan dalam memperhitungkan biaya pemeliharaan jangka panjang dan, oleh karena itu, mempertimbangkan jenis media yang lebih baik.

Kecepatan

Untuk mengevaluasi media dengan benar, Anda perlu mempertimbangkan dua jenis kecepatan: kecepatan transmisi data dan kecepatan propagasi. Kecepatan transmisi data adalah jumlah bit per detik yang dapat ditransmisikan. Bit maksimum per detik untuk media tertentu bergantung secara proporsional pada bandwidth efektif media tersebut, jarak yang harus ditempuh data, dan lingkungan yang harus dilalui media tersebut (noise). Jika salah satu persyaratan jaringan yang Anda rancang adalah kecepatan transmisi data minimal yang dapat diterima, maka media yang Anda pilih harus mendukung kecepatan tersebut. Masalah ini mungkin terdengar sepele, namun menjadi rumit karena sulitnya memprediksi pertumbuhan jaringan. Meskipun media yang dipilih mungkin mendukung tingkat lalu lintas tertentu saat ini, media tersebut mungkin tidak dapat mendukung penambahan pengguna baru atau aplikasi baru di masa mendatang. Oleh karena itu, perencanaan yang matang untuk pertumbuhan di masa depan diperlukan untuk mendapatkan dukungan jaringan yang tepat (kita akan membahas masalah ini secara lebih rinci di Bab Tiga Belas). Masalah penting lainnya yang perlu dipertimbangkan adalah meskipun teknologi tertentu menunjukkan kecepatan transmisi data, kecepatan tersebut mungkin bukan throughput data yang sebenarnya. Misalnya, LAN nirkabel IEEE 802.11a dan 802.11g menawarkan kecepatan transmisi data sebesar 54 Mbps, namun kenyataannya, pengguna merasakan kecepatan transfer data kira-kira setengah dari nilai ini. Hal ini, seperti yang akan kita lihat di bab selanjutnya, disebabkan oleh noise, interferensi, dan sinyal lemah.

Kecepatan propagasi adalah kecepatan pergerakan sinyal melalui suatu medium. Kecepatan propagasi media serat optik sangat mendekati kecepatan cahaya, dan media nirkabel sebenarnya merambat dengan kecepatan cahaya, yaitu 186.000 mil per detik (3.108 meter per detik). Untuk media penghantar listrik (twisted pair dan kabel koaksial), kecepatan rambatnya kira-kira dua pertiga kecepatan cahaya, atau 124.000 mil per detik (2.108 meter per detik). Meskipun kecepatan ini tampak cukup cepat untuk sebagian besar aplikasi, perlu diingat bahwa waktu yang diperlukan untuk mengirim sinyal ke satelit di orbit luar Bumi dan kembali penundaan propagasi kira-kira 0,25 hingga 0,75 detik, tergantung pada jarak sebenarnya ke satelit, satelit dan jumlah perangkat yang harus dilewati sinyal. Jika Anda mentransfer data dari satu negara ke negara lain, Anda mungkin ingin mempertimbangkan media dengan penundaan propagasi yang lebih rendah.

Perluasan dan Jarak

Media tertentu lebih mudah melakukan ekspansi. Kabel twisted pair lebih mudah untuk diperluas dibandingkan kabel koaksial atau kabel serat optik, dan kabel koaksial lebih mudah untuk diperluas dibandingkan kabel serat optik. Kabel koaksial lebih sulit untuk diperluas dibandingkan kabel twisted pair karena jenis konektor pada ujung kabel. Konektor serat optik bahkan lebih rumit lagi, dan menyambungkan dua potong kabel serat optik memerlukan latihan dan seperangkat alat yang tepat.

Pertimbangan terkait perluasan lainnya adalah bahwa sebagian besar bentuk twisted pair hanya dapat beroperasi pada jarak 100 meter (328 kaki) sebelum sinyal memerlukan regenerasi. Beberapa bentuk sistem kabel koaksial dapat berjalan lebih jauh (mil), dan kabel serat optik dapat diperpanjang hingga bermil-mil sebelum regenerasi sinyal diperlukan. Gelombang mikro terestrial yang dimiliki oleh swasta memiliki tingkat transmisi yang tinggi, namun jika piringan gelombang mikro dipasang di gedung-gedung perusahaan, maka jarak antara gedung-gedung tersebut tidak boleh lebih dari 20 hingga 30 mil. Selain itu, pengaturan ini hanya akan berfungsi jika bangunannya tinggi dan tidak ada penghalang, misalnya bangunan lain, yang menghalangi. Sistem seluler tersebar luas dan terus berkembang. Teknologi baru seperti telepon seluler generasi keempat dan WiMax menjanjikan kemampuan untuk diperluas. Kebetulan, ketika berbicara tentang teknologi nirkabel, penting untuk tidak membingungkan berbagai bidang aplikasi. Bluetooth dan inframerah hanya untuk jarak pendek. Wi-Fi dirancang untuk jaringan area lokal dan memiliki jangkauan maksimum beberapa ribu kaki (setara dengan beberapa ratus meter). WiMax dirancang untuk akses Internet berkecepatan tinggi pada jarak hingga 30 mil. Ponsel generasi ketiga seperti UMTS mampu mentransfer data dalam jumlah ratusan kbps, dan ponsel generasi keempat akan mencapai jutaan bit per detik.

Saat mempertimbangkan perluasan, jangan lupakan masalah hak jalan. Jika Anda mencoba memasang kabel melintasi tanah yang bukan milik Anda, Anda harus mendapatkan izin dari pemilik tanah. Terkadang izin tersebut tidak diberikan, dan terkadang Anda mungkin mendapatkan izin namun harus membayar biaya berulang kepada pemilik tanah.

Jika Anda berharap untuk menciptakan sistem yang dapat berkembang di masa depan, ada baiknya mempertimbangkan penggunaan media yang dapat berkembang dengan biaya

yang wajar. Namun perlu diperhatikan bahwa perluasan suatu sistem, sering kali, lebih ditentukan oleh desain sistem dan penggunaan peralatan elektronik pendukung dibandingkan dengan pemilihan jenis media.

Lingkungan

Faktor lain yang harus diperhatikan dalam proses pemilihan media adalah lingkungan. Banyak jenis lingkungan yang berbahaya bagi media tertentu. Lingkungan industri dengan mesin berat menghasilkan radiasi elektromagnetik yang dapat mengganggu kabel yang tidak terlindung dengan baik. Jika pemasangan kabel Anda mungkin dilakukan melalui lingkungan yang bising secara elektromagnetik, Anda harus mempertimbangkan untuk menggunakan kabel berpelindung atau kabel serat optik.

Transmisi nirkabel juga dapat terganggu oleh gangguan elektromagnetik dan interferensi dari transmisi lain. Bintik matahari, meskipun jarang terjadi, dapat mengganggu transmisi satelit. Karena begitu banyak orang kini mengandalkan layanan nirkabel untuk suara, data, dan paging, surat kabar sering kali memperingatkan masyarakat ketika aktivitas bintik matahari diperkirakan tinggi. Perlu dicatat bahwa transmisi gelombang mikro dan optik ruang bebas dapat terhambat oleh cuaca buruk. Sebelum memilih media, penting untuk mengetahui lingkungan yang diinginkan dari media tersebut dan menyadari bagaimana lingkungan ini dapat mempengaruhi atau mengganggu transmisi.

Keamanan

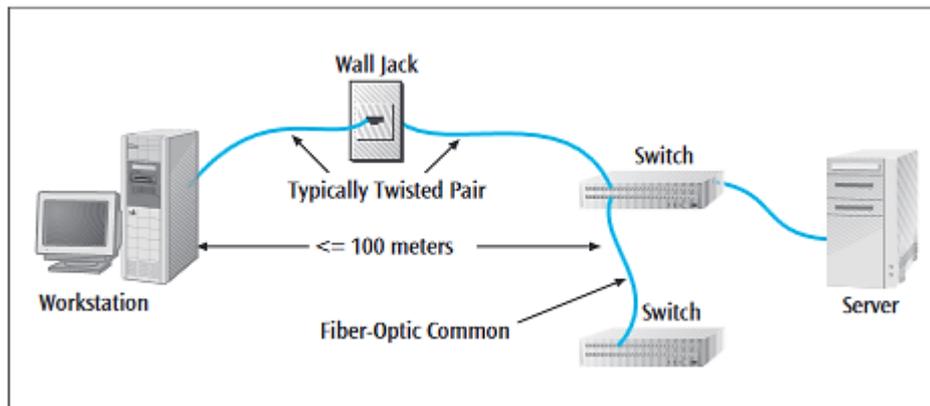
Jika data harus aman selama transmisi, penting agar medianya tidak mudah disadap. Semua media penghantar, kecuali kabel serat optik, dapat disadap dengan mudah, artinya seseorang dapat “mendengarkan” sinyal elektromagnetik yang melewati kabel tersebut. Komunikasi nirkabel juga dapat disadap, namun jauh lebih mudah untuk menyadap transmisi siaran nirkabel seperti jaringan area lokal nirkabel dibandingkan sistem nirkabel pancaran sempit seperti gelombang mikro. Untungnya, ada cara untuk meningkatkan keamanan data baik pada media konvensional maupun nirkabel. Perangkat lunak enkripsi dan dekripsi dapat digunakan dengan media konduksi. Teknologi spektrum tersebar dapat diterapkan pada komunikasi nirkabel, membuatnya tahan terhadap intersepsi. Teknologi enkripsi, dekripsi, dan spread spektrum akan dibahas secara rinci di Bab Dua Belas.

Sekarang kita telah membahas berbagai jenis media dan kriteria pemilihan, mari kita mengalihkan perhatian kita pada cara kerja media nirkabel dan terkonduksi dalam suatu jaringan.

3.5 DUA CONTOH AKSI MEDIA YANG DILAKUKAN

Mari kita pertimbangkan pengkabelan untuk jaringan area lokal. Gambar 3-20 menunjukkan situasi umum di mana stasiun kerja mikrokomputer yang terhubung ke jaringan area lokal harus terlebih dahulu terhubung ke perangkat seperti switch. Sakelar adalah perangkat yang menghubungkan beberapa stasiun kerja dan meneruskan sinyal transmisi dari stasiun kerja mana pun ke stasiun kerja lainnya (Bab Tujuh dan Delapan membahas sakelar secara lebih rinci). Dalam instalasi biasa, kecil kemungkinannya bahwa kabel yang meninggalkan stasiun kerja langsung menuju ke sakelar. Sebaliknya, kabel yang keluar dari

bagian belakang komputer mikro terlebih dahulu disambungkan ke soket dinding di ruangan tempat komputer mikro berada. Soket dinding ini adalah perangkat pasif, titik koneksi sederhana antara dua rangkaian kabel yang tidak menghasilkan kembali sinyal pada kabel.



Gambar 3-20 Contoh situasi pengkabelan yang melibatkan stasiun kerja dan jaringan area lokal

Untuk memilih media yang tepat untuk koneksi ini, Anda harus mempertimbangkan dua masalah utama: jarak kabel dan kecepatan data. Untuk memperhitungkan jarak kabel dalam situasi ini, Anda harus mempertimbangkan jarak total dari bagian belakang komputer mikro ke saklar. Jika jarak ini kurang dari 100 meter (328 kaki), Anda dapat mempertimbangkan untuk menggunakan twisted pair untuk menghubungkan komputer mikro ke saklar. Jika kabel tidak melewati lingkungan yang bising, maka Anda dapat mempertimbangkan untuk menggunakan kabel twisted pair tanpa pelindung, kabel yang paling murah dan termudah untuk digunakan. Jika Anda dapat berasumsi bahwa kecepatan data koneksi tidak akan melebihi 1000 Mbps, koneksi tersebut seharusnya dapat didukung menggunakan empat pasang Kategori 5e atau Kategori 6.

Namun, jika kecepatan data lebih tinggi dari 1000 Mbps, Anda mungkin ingin mempertimbangkan alternatif selain twisted pair. Kabel serat optik adalah pilihan yang baik untuk kecepatan transmisi data lebih dari 1000 Mbps, namun biayanya lebih mahal daripada sambungan twisted pair. Selain itu, karena kabel serat optik merupakan kabel satu arah dan aliran data antara stasiun kerja dan saklar bersifat dua arah, maka diperlukan dua kabel serat optik.

Dalam hal ini, karena kecepatan data antara workstation mikro dan switch adalah 100 Mbps atau kurang, twisted pair tanpa pelindung Kategori 5e atau 6 akan menjadi pilihan yang dapat diterima (Kategori 7 akan menjadi pengeluaran yang tidak perlu pada saat ini). Kabel serat optik juga merupakan pilihan yang masuk akal, karena dapat beradaptasi dengan kecepatan transmisi yang lebih tinggi di masa depan.

Bagaimana dengan pemasangan kabel koneksi antara switch dan titik berikutnya di jaringan area lokal (biasanya switch lain)? Jika jarak antara kedua saklar melebihi panjang 100 meter atau jika kabel melewati lingkungan yang bising, seperti ruang mekanis pemanas

dan pendingin, sebaiknya gunakan kabel selain kabel twisted pair. Dalam keadaan ini, Anda akan mempertimbangkan kabel koaksial yang sangat bagus atau, lebih baik lagi, kabel serat optik untuk menghubungkan kedua sakelar. Mengapa Anda harus mempertimbangkan kabel serat optik yang lebih mahal? Perbedaan harga antara kabel koaksial dan kabel serat optik jauh lebih kecil dibandingkan perbedaan kinerjanya. Oleh karena itu, masuk akal untuk memilih kabel terbaik dan memasang kabel serat optik.

Pada contoh kedua, mari kita pertimbangkan skenario di mana sebuah perusahaan mempunyai dua bangunan yang jaraknya kira-kira 1 mil. Perusahaan ingin mengirimkan data antara dua gedung secara rutin dengan kecepatan hingga 100 Mbps. Apa yang Anda rekomendasikan sebagai jenis media interkoneksi terbaik? Sebelum kita mempertimbangkan segala bentuk media yang dilakukan, kita perlu mengajukan pertanyaan: Apakah properti di antara dua bangunan tersebut milik perusahaan? Mari kita berasumsi bahwa hal tersebut tidak terjadi (kemungkinan besar terjadi). Perusahaan mungkin ingin mempertimbangkan untuk menggunakan bentuk transmisi nirkabel, seperti gelombang mikro terestrial atau optik ruang bebas (dengan asumsi tidak ada struktur intervensi), atau menghubungi perusahaan telepon dan menanyakan apakah layanan transmisi data 100 Mbps cocok untuk digunakan. tersedia yang akan menghubungkan kedua bangunan tersebut.

Jika properti di antara kedua bangunan tersebut adalah milik perusahaan, maka pemilihan media yang dilakukan masih sulit. Media penghantar manakah yang mampu mendukung 100 Mbps untuk jarak 1 mil? Kabel serat optik akan memenuhi persyaratan tersebut, namun bagaimana perusahaan akan memasang kabel tersebut—di bawah tanah dalam bentuk pipa atau terowongan, atau overhead pada beberapa jenis tiang telepon? Kedua solusi tersebut akan memakan biaya yang cukup mahal kecuali jika infrastruktur untuk mendukung kabel serat optik baru sudah ada. Memasang kawat di dalam gedung lebih mudah daripada mencoba memasangnya di antara gedung, namun tidak ada tugas yang sederhana. Karena memasang suatu media itu mahal dan berjangka panjang, perencanaan dan pengambilan keputusan yang cermat sangat penting sebelum proyek dapat dimulai.

Mari kita pertimbangkan masing-masing kriteria pemilihan media yang diterapkan pada solusi dua bangunan ini:

- **Biaya**—Fiber optik merupakan pilihan media yang paling mahal namun sepadan dengan biayanya, mengingat kebutuhan permasalahannya. Beberapa bentuk nirkabel mungkin merupakan alternatif yang baik, selain menghubungi perusahaan telepon lokal untuk mendapatkan solusi yang disarankan.
- **Kecepatan**—Fiber-optik, twisted pair, dan kabel koaksial akan mendukung persyaratan kecepatan yang diperlukan, begitu juga dengan microwave dan optik ruang bebas.
- **Perluasan dan Jarak**—Jarak satu mil menghilangkan pertimbangan kabel twisted pair dan koaksial. Jalan yang benar jelas merupakan masalah dalam kasus ini. Jika Anda tidak memiliki hak jalan, Anda tidak dapat memasang kabel Anda sendiri.
- **Lingkungan**—Kabel serat optik tidak boleh terpengaruh oleh lingkungan. Jika solusi nirkabel diterapkan, jarak pandang dan cuaca bisa menjadi dua hambatan serius.

- **Keamanan**—Sistem serat optik harus aman dari penyadapan.

Kesimpulannya, pemasangan kabel antara dua bangunan sering kali tidak dapat dilakukan karena masalah hak jalan atau pembatasan jarak maksimum. Ketika media yang digunakan tidak dapat digunakan, sejumlah pilihan nirkabel harus dipertimbangkan. Bahkan jika media yang digunakan dapat digunakan, solusi nirkabel mungkin terbukti lebih ekonomis dalam jangka panjang. Seringkali, solusi untuk menghubungkan beberapa bisnis melibatkan perusahaan telepon, seperti yang akan kita lihat di bab selanjutnya.

3.6 CONTOH MEDIA NIRKABEL

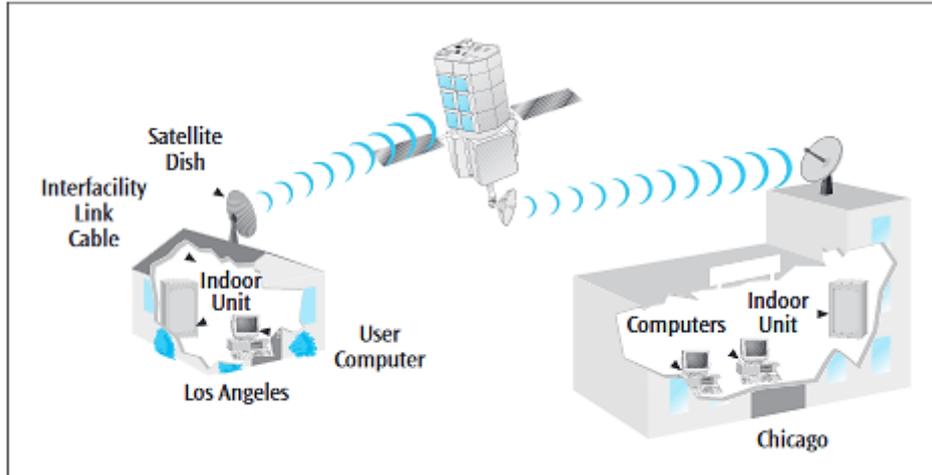
Di rumah Anda, Anda memiliki beberapa komputer, masing-masing di ruangan berbeda. Setiap komputer mempunyai printer ink-jet yang cukup murah, dan hanya satu komputer yang memiliki akses ke Internet. Anda ingin menghubungkan kedua komputer ke Internet dan membeli printer laser yang bagus untuk digunakan bersama oleh keduanya. Untuk melakukan hal ini, Anda perlu menghubungkan komputer-komputer, namun menarik kabel melalui dinding dan lantai sepertinya bukan pilihan yang menarik. Bagaimana dengan nirkabel? Anda dapat membeli kartu antarmuka jaringan nirkabel yang menggunakan salah satu protokol IEEE 802.11 dan membuat jaringan area lokal nirkabel.

Anda mungkin juga ingin mempertimbangkan untuk mengganti perangkat yang ada, seperti printer dan pemindai, dengan perangkat yang mendukung Wi-Fi. Dengan menggunakan Wi-Fi, Anda akan dapat mengurangi ketergantungan pada kabel yang mengalir dari stasiun kerja ke periferal dan, dengan demikian, meningkatkan fleksibilitas Anda dalam menemukan lokasi peralatan. Kita akan membahas topik jaringan area lokal rumah (sering disebut instalasi Small Office/Home Office, atau SOHO) secara lebih rinci di bab selanjutnya.

Sebagai contoh kedua, mari kita perhatikan DataMining Corporation, sebuah organisasi besar yang memiliki kantor utama di Chicago dan kantor kedua di Los Angeles. DataMining mengumpulkan data dari toko kelontong dari setiap pembelian yang dilakukan oleh setiap pelanggan. Dengan menggunakan data ini, perusahaan mengekstraksi tren pengeluaran dan menjual informasi ini ke bisnis lain yang memasarkan barang yang dapat dijual. Data dikumpulkan di kantor Chicago dan dikirimkan ke kantor Los Angeles, di mana data tersebut disimpan dan kemudian diambil. Oleh karena itu, terdapat kebutuhan untuk mengirimkan data dalam jumlah besar antara kedua situs secara terus-menerus.

Saat ini, DataMining menyewa layanan telepon antara Chicago dan Los Angeles, namun tagihan teleponnya tinggi. Perusahaan berusaha mengurangi biaya dan mempertimbangkan alternatif selain layanan telepon sewaan. Bentuk layanan telepon lainnya juga tersedia, namun hal ini baru akan diperkenalkan pada Bab Sebelas. Anggap saja DataMining telah memeriksa bentuk layanan lain ini dan menganggapnya mahal—sehingga perlu mempertimbangkan alternatif lain. DataMining telah menemukan bahwa sejumlah perusahaan dapat menyediakan berbagai tingkat layanan komunikasi satelit. Misalnya, Hughes Network Systems dapat menyediakan internetworking jaringan area lokal, transfer gambar multimedia, koneksi suara interaktif, transfer data interaktif dan batch, serta layanan siaran video dan komunikasi data. Karena DataMining terutama tertarik pada transmisi data

dua arah, maka DataMining mempertimbangkan layanan komunikasi data dua arah yang ditawarkan oleh Hughes melalui sistem satelit VSAT. Seperti yang ditunjukkan pada Gambar 3-21, layanan data dua arah ini memerlukan instalasi parabola stasiun Bumi individual di setiap lokasi perusahaan DataMining.



Gambar 3-21 Solusi satelit VSAT untuk DataMining Corporation

Setiap stasiun Bumi terdiri dari dua bagian: unit dalam ruangan dan unit luar ruangan. Unit outdoor terdiri dari parabola dan biasanya dipasang di atap gedung. Ukuran parabola bergantung pada kecepatan data yang digunakan dan jangkauan satelit yang diperlukan. Unit luar ruangan dihubungkan ke unit dalam ruangan melalui satu kabel penghubung antar fasilitas. Unit dalam ruangan memiliki satu atau lebih port yang dapat dihubungkan dengan peralatan pemrosesan data perusahaan.

Pemeliharaan dan dukungan untuk layanan VSAT ini disediakan oleh perusahaan satelit selama 24 jam per hari, 7 hari seminggu, dan mencakup konfigurasi peralatan, pelaporan status sistem, alokasi bandwidth, pengunduhan semua informasi yang diperlukan, perangkat lunak, dan pengiriman personel lapangan jika diperlukan.

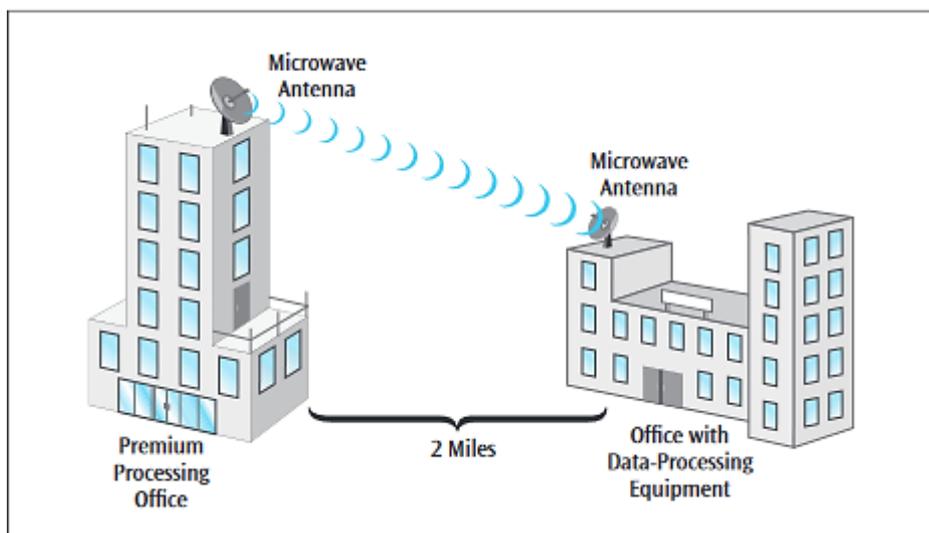
DataMining Corporation telah memutuskan untuk menginstal sistem satelit VSAT. Sebagai rangkuman, mari kita pertimbangkan masing-masing kriteria pemilihan media yang diterapkan pada solusi VSAT:

- **Biaya**—Sistem VSAT relatif mahal, namun memberikan kecepatan transfer data yang tinggi dengan keandalan yang tinggi.
- **Kecepatan**—Sistem VSAT dapat mendukung kecepatan transfer data yang diperlukan oleh Data-Mining Corporation.
- **Perluasan dan Jarak**—Sistem satelit dapat dengan mudah menjangkau dari Chicago hingga Los Angeles. Jalan yang benar tidak menjadi masalah dalam kasus ini.
- **Lingkungan**—Sistem satelit dapat terganggu oleh gaya elektromagnetik yang kuat, yang dapat menjadi masalah. Jika DataMining tidak dapat mentolerir gangguan layanan apa pun, DataMining mungkin ingin mempertimbangkan untuk memasang sistem cadangan jika sistem VSAT gagal untuk sementara waktu.

- **Keamanan**—Sistem satelit VSAT sulit untuk dicegat karena pancaran transmisi yang dikirim antara stasiun bumi dan satelit kecil. Selain itu, aliran data dapat dienkripsi.

Perusahaan kedua, Perusahaan Asuransi Amerika, memiliki dua kantor, keduanya berlokasi di Peoria, Illinois. Kantor pertama menampung seluruh pembayaran premi, dan kantor kedua berisi peralatan pengolah data utama. American Insurance perlu mentransfer informasi premi yang dikumpulkan ke pusat pemrosesan data setiap malam. Kedua kantor tersebut berjarak sekitar dua mil, namun tidak mungkin menjalankan kabel milik perusahaan melalui properti publik dan properti pribadi. Beberapa bentuk sistem telepon mungkin memberikan solusi yang masuk akal, namun American Insurance tertarik untuk berinvestasi pada sistemnya sendiri dan ingin menghindari biaya telepon bulanan yang berulang karena biaya tersebut, pada suatu saat, akan melebihi biaya pemasangan sistemnya sendiri.

ProNet adalah perusahaan yang menawarkan sistem gelombang mikro terestrial pribadi yang dapat mentransfer suara pribadi, data jaringan area lokal, konferensi video, dan gambar resolusi tinggi antar situs jarak jauh hingga jarak 15 mil. Gambar 3-22 menunjukkan pengaturan komunikasi gelombang mikro yang khas seperti yang diatur antara dua kantor perusahaan American Insurance.



Gambar 3-22 Komunikasi gelombang mikro antara gedung perusahaan American Insurance

Mari kita pertimbangkan masing-masing kriteria pemilihan media yang diterapkan pada solusi gelombang mikro terestrial ProNet:

- **Biaya**—Sistem ProNet pada awalnya mahal ketika peralatan dibeli, namun setelah itu, American harus membayar hanya untuk pemeliharaan.
- **Kecepatan**—Sistem ProNet dapat mendukung kecepatan transfer data yang diperlukan oleh American Insurance.
- **Perluasan dan Jarak**—Sistem gelombang mikro terestrial dapat mentransmisikan hingga jarak 15 mil. Kedua gedung perusahaan berjarak dua mil. Jalan yang benar tidak menjadi masalah dalam kasus ini.

- **Lingkungan**—Sistem gelombang mikro dapat terganggu oleh gaya elektromagnetik yang kuat dan cuaca buruk. Namun ProNet menyatakan bahwa sistemnya tidak terpengaruh oleh kabut atau salju, dan memberikan tingkat keandalan dan ketersediaan layanan sebesar 99,97 persen.
- **Keamanan**—Sistem gelombang mikro terestrial dapat disadap, namun aliran data dapat dienkripsi.

American Insurance akan secara serius mempertimbangkan untuk menggunakan sistem gelombang mikro terestrial ProNet, karena sistem ini lebih baik dibandingkan dengan sistem lain dan memenuhi tujuan perusahaan dalam hal kepemilikan pribadi, tingkat transfer yang tinggi, dan biaya berulang yang rendah.

RINGKASAN

- Semua media komunikasi data dapat dibagi menjadi dua kategori dasar: (1) media fisik atau terkonduksi, seperti kabel, dan (2) media terpancar atau nirkabel, seperti sistem satelit.
- Tiga jenis media penghantar adalah kabel twisted pair, kabel koaksial, dan kabel serat optik.
- Kabel pasangan terpilin dan kabel koaksial keduanya merupakan kabel logam dan dapat terkena interferensi elektromagnetik. Kabel serat optik adalah kawat kaca dan tahan terhadap interferensi elektromagnetik; oleh karena itu, ia mengalami tingkat kebisingan yang lebih rendah dibandingkan kabel twisted pair dan koaksial.
- Kabel serat optik mempunyai kecepatan transmisi dan kinerja jarak jauh terbaik dibandingkan semua media yang dihantarkan karena (1) memiliki tingkat kebisingan yang lebih rendah, dan (2) sinyal cahaya tidak melemah secepat sinyal listrik.
- Ada beberapa kelompok dasar media nirkabel: transmisi gelombang mikro terestrial, transmisi satelit, sistem telepon seluler, transmisi inframerah, WiMax, Bluetooth, Wi-Fi, optik ruang bebas, ultra-wideband, dan ZigBee.
- Setiap teknologi nirkabel dirancang untuk aplikasi tertentu. Kecepatan transfer data, jarak transmisi, kelebihan dan kekurangan harus dipertimbangkan untuk masing-masingnya.
- Saat mencoba memilih media tertentu untuk suatu aplikasi, ada baiknya membandingkan media yang berbeda menggunakan lima kriteria berikut: biaya, kecepatan, kemampuan untuk diperluas dan jarak, jalur yang tepat, lingkungan, dan keamanan.

PERTANYAAN TINJAUAN

1. Mengapa kawat twisted pair disebut twisted pair?
2. Bagaimana crosstalk terjadi pada kabel twisted pair?
3. Untuk tujuan apa kawat twisted pair Kategori 5e, 6, dan 7 digunakan?
4. Apa kelebihan dan kekurangan pasangan terpilin berpelindung?
5. Apa keunggulan utama kabel koaksial dibandingkan kabel twisted pair?
6. Apa perbedaan antara kabel koaksial baseband dan kabel koaksial broadband?
7. Mengapa kabel serat optik kebal terhadap interferensi elektromagnetik?

8. Apa kelebihan dan kekurangan kabel serat optik?
9. Apa perbedaan antara gelombang mikro terestrial dan gelombang mikro satelit?
10. Berapa jarak rata-rata untuk transmisi gelombang mikro terestrial?
11. Benda apa saja yang dapat mengganggu transmisi gelombang mikro terestrial?
12. Sebutkan beberapa kegunaan umum gelombang mikro terestrial.
13. Apa saja empat tingkat orbit sistem satelit?
14. Sebutkan beberapa area penerapan umum untuk setiap sistem satelit tingkat orbit.
15. Bagaimana urutan kejadian yang terjadi ketika seseorang melakukan panggilan dari telepon seluler?
16. Apa fungsi kantor peralihan telepon seluler?
17. Apa perbedaan utama antara sistem seluler AMPS dan D-AMPS?
18. Apa perbedaan utama antara sistem seluler AMPS (atau D-AMPS) dan telepon seluler PCS yang lebih baru?
19. Apa perbedaan antara Layanan telepon seluler generasi 2,5 seperti GPRS dan 1xRTT, dan layanan telepon seluler UMTS yang lebih baru seperti 1xEV dan EV-DO?
20. Apa yang dimaksud dengan saling berhadapan?
21. Untuk apa protokol WiMax digunakan?
22. Apa kelebihan IEEE 802.20 dibandingkan IEEE 802.16e?
23. Transmisi inframerah dapat digunakan untuk jenis aplikasi apa?
24. Apa kelebihan dan kekurangan utama ZigBee?
25. Layanan nirkabel broadband mendukung aplikasi apa?
26. Apa kelebihan dan kekurangan utama Bluetooth?
27. Sebutkan tiga kemungkinan penerapan Bluetooth.
28. Apa sajakah protokol jaringan area lokal nirkabel yang berbeda?
29. Dalam situasi apa Anda dapat menggunakan optik ruang kosong?
30. Apa saja jenis biaya media yang dilakukan?
31. Apa perbedaan antara kecepatan transmisi data dan kecepatan propagasi?
32. Apa yang dimaksud dengan jalan yang benar?

LATIHAN TAMBAHAN

1. Tabel 3-1 menunjukkan kabel Kategori 1 memancarkan sinyal sejauh 5 hingga 6 kilometer (3 hingga 4 mil) namun Kategori 5e hanya sejauh 100 meter (328 kaki). Apakah ini berarti Kategori 1 adalah kabel terbaik untuk transmisi jarak jauh? Menjelaskan.
2. Sebutkan tiga contoh crosstalk yang tidak melibatkan kabel dan sinyal listrik. (Petunjuk: Lihatlah sekeliling Anda.)
3. Karakteristik apa dari pasangan terpilin tak berpelindung Kategori 5e/6 yang membuatnya menjadi kawat penghantar yang paling umum digunakan?
4. Dapatkah Anda mengirimkan sinyal video melalui kabel twisted pair? Menjelaskan. Pastikan untuk mempertimbangkan beberapa skenario.

5. Perusahaan TV kabel lokal sedang mempertimbangkan untuk melepas seluruh kabel koaksial dan menggantinya dengan kabel serat optik. Buatlah daftar keuntungan dan kerugian dari rencana ini.
6. Perusahaan TV kabel lokal telah berubah pikiran. Sekarang akan mengganti semua kabel koaksial yang ada dengan kabel twisted pair unshielded. Buatlah daftar keuntungan dan kerugian dari rencana ini.
7. Urutkan lima contoh media berikut secara berurutan dari kecepatan transmisi data tertinggi hingga kecepatan transmisi data terendah: twisted pair, kabel koaksial, kabel serat optik, gelombang mikro, dan satelit.
8. Dengan menggunakan lima contoh media yang sama dari latihan sebelumnya, urutkan kelima media tersebut berdasarkan transmisi yang paling berisik hingga transmisi yang paling sedikit berisik.
9. Dengan menggunakan lima contoh media yang sama dari latihan sebelumnya, urutkan kelima media tersebut dari transmisi yang paling aman hingga transmisi yang paling tidak aman.
10. Gelombang mikro terestrial merupakan transmisi garis pandang. Benda apa saja yang cukup tinggi untuk mengganggu gelombang mikro terestrial?
11. Perusahaan Anda mempunyai dua kantor yang berjarak kira-kira 1 mil. Data perlu ditransfer antara dua kantor dengan kecepatan hingga 100 Mbps. Buatlah daftar solusi sebanyak mungkin untuk menghubungkan kedua bangunan tersebut. Apakah setiap solusi secara teknis layak dilakukan? Layak secara finansial? Layak secara politis? Pertahankan posisi Anda.
12. Mengingat sinyal satelit bergerak dengan kecepatan cahaya, berapa lama waktu yang dibutuhkan sinyal untuk berpindah dari Bumi ke satelit dalam orbit geosinkron dan kembali ke Bumi? Tunjukkan perhitungannya.
13. Berapa lama waktu yang dibutuhkan sinyal untuk mencapai satelit di orbit rendah Bumi? Tunjukkan perhitungannya.
14. Anda sedang berjalan di jalan, dan ponsel Anda berdering. Urutan kejadian apa yang memungkinkan seseorang dengan telepon konvensional menghubungi Anda melalui ponsel Anda?
15. Teknologi nirkabel apa yang dapat mentransmisikan melalui benda padat? Teknologi nirkabel mana yang tidak bisa?
16. Anda berbicara di ponsel saat berpindah dari satu ponsel ke ponsel lainnya. Akankah ponsel Anda menggunakan rangkaian frekuensi yang sama di sel baru seperti yang digunakan di sel sebelumnya? Menjelaskan.
17. Mengapa sistem telepon seluler hanya memerlukan tujuh set frekuensi di wilayah metropolitan?
18. Apa potensi masalah serius saat menggunakan asisten digital pribadi dan Bluetooth untuk membuka kunci pintu secara nirkabel? Menjelaskan.
19. Sebuah perusahaan di komunitas Anda mulai menawarkan layanan WiMax untuk akses Internet. Perusahaan menjanjikan unduhan 2 Mbps. Jika perusahaan

- memperkirakan bahwa layanan baru ini akan menarik 2000 pelanggan, berapakah bandwidth yang diperlukan untuk mendukung layanan ini?
20. Layanan T-1 yang ditawarkan oleh perusahaan komunikasi suara dan data mampu mendukung transfer data berkelanjutan sebesar 1,5 Mbps melalui kabel telepon berkualitas tinggi. Apa kelebihan dan kekurangan layanan tersebut dibandingkan layanan seperti WAP, Bluetooth, dan microwave terrestrial?
 21. Anda sedang mempertimbangkan untuk mengganti sistem transmisi gelombang mikro terrestrial dengan sistem optik ruang bebas. Apa keuntungan dan kerugian melakukan hal ini?

DISKUSI KAN DENGAN KELOMPOK ANDA

1. Kumpulkan dan beri label pada sampel sebanyak mungkin jenis media yang dilakukan, dan tampilkan dengan rapi pada selembar karton.
2. Dengan menggunakan Internet, temukan spesifikasi teknis dari dua jenis kabel yang berbeda.
3. Berapa banyak jenis media yang ada di bisnis atau sekolah Anda? Bagaimana cara penggunaannya? Gambarlah diagram kasar yang menunjukkan perkiraan lokasi dan jenis kawat.
4. Dengan menggunakan sumber apa pun, selidiki perusahaan yang dapat menawarkan layanan gelombang mikro di wilayah Anda. Laporkan jenis aplikasi apa yang dapat didukung, peralatan apa yang diperlukan, di mana peralatan tersebut akan ditempatkan, dan layanan apa yang ditawarkan perusahaan ini.
5. Dengan menggunakan sumber apa pun, selidiki perusahaan yang dapat menawarkan layanan satelit VSAT di wilayah Anda. Laporkan jenis aplikasi apa yang dapat didukung, peralatan apa yang diperlukan, di mana peralatan tersebut akan ditempatkan, dan layanan apa yang ditawarkan perusahaan ini.
6. Apakah ada orang di daerah Anda yang menawarkan layanan WiMax? Jika ya, tulis ringkasan satu halaman yang mencakup fitur utama layanan.
7. Berapa banyak perusahaan telepon seluler yang menawarkan layanan di wilayah Anda? Apakah layanannya D-AMPS atau PCS? Kalau PCS apakah CDMA, TDMA, atau GSM? Apakah itu GPRS atau CDMA2000 1xRTT? Apakah itu UMTS atau EV-DO? Bagaimana dengan LTE atau WiMax? Apakah perusahaan mempunyai perkiraan jumlah pelanggan saat ini? Apakah mereka tahu berapa banyak sel yang ada di pasar Anda?
8. Apakah twisted pair Kategori 8 sudah ada? Apakah ada kebutuhan akan kawat seperti itu? Gunakan sumber kertas atau Internet untuk menemukan jawabannya.
9. Dengan menggunakan sumber luar, seperti Internet atau perpustakaan, tentukan ketinggian menara gelombang mikro terrestrial. Jika tinggi menara dinaikkan 10 meter, berapa jarak transmisi yang dapat dicapai menara tersebut?
10. Menggunakan komputer laptop dengan kartu LAN nirkabel terpasang, temukan LAN nirkabel di kampus Anda, lalu buat peta jaringan tersebut.

BAB 4

MEMBUAT KONEKSI

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Sebutkan empat komponen dari semua standar antarmuka
- Diskusikan pengoperasian dasar standar antarmuka USB
- Kenali perbedaan antara koneksi half-duplex dan full-duplex
- Sebutkan keunggulan standar antarmuka FireWire, Thunderbolt, SCSI, iSCSI, InfiniBand, dan Fibre Channel
- Menguraikan karakteristik antarmuka data link asynchronous, synchronous, dan isochronous
- Identifikasi karakteristik pengoperasian koneksi terminal-ke-mainframe dan mengapa koneksi tersebut unik dibandingkan dengan jenis koneksi komputer lainnya

MENGHUBUNGKAN PERANGKAT PERIPHERAL ke komputer tidak pernah menjadi tugas yang mudah. Antarmuka antara komputer dan periferal rumit dan mengandung banyak lapisan perangkat keras dan perangkat lunak. Para ahli di bidangnya telah bekerja selama bertahun-tahun untuk menyederhanakan proses interkoneksi, dan Universal Serial Bus memimpin sebagai salah satu pesaing terbaik untuk standar antarmuka universal.

Sayangnya, standar antarmuka baru jarang berfungsi sebagaimana mestinya pada percobaan pertama. Salah satu contoh paling klasik terjadi selama Pameran Komputer COMDEX Spring 98, di mana CEO Microsoft Corporation Bill Gates dan rekannya, dalam upaya untuk mendemonstrasikan Windows 98 yang akan segera dirilis dan antarmuka Universal Serial Bus-nya, mencoba untuk menghubungkan pemindai halaman ke komputer saat komputer dihidupkan. Terlepas dari kenyataan bahwa Universal Serial Bus dan Windows 98 dirancang untuk menerima periferal secara otomatis setiap kali mereka terhubung, komputer Gates tidak menerima perangkat tersebut dan crash. Untuk menyenangkan penonton, Gates dengan cepat menjawab, *“Itulah sebabnya kami belum mengirimkan Windows 98.”*

Apa yang terlibat dalam menghubungkan komputer ke perangkat lain?

Apakah antarmuka begitu sulit sehingga bahkan para spesialis pun mengalami kesulitan?

Apakah kita benar-benar perlu mengetahui apa yang terjadi di tingkat antarmuka?

4.1 PENDAHULUAN

Komputer tidak akan ada gunanya jika kita tidak dapat menghubungkannya dengan apa pun. Bayangkan, jika Anda mau, sebuah komputer tanpa monitor untuk melihat keluaran dan tanpa keyboard untuk memasukkan data. Banyak orang juga merasa bahwa komputer mereka tidak akan berguna jika tidak ada cara untuk menghubungkan komputer ke printer,

atau jika mereka tidak dapat menghubungkannya ke modem DSL untuk berselancar di Internet atau mengakses sistem komputer jarak jauh. Banyak orang di dunia korporat bergantung hampir secara eksklusif pada interkoneksi antara komputer mereka dan jaringan area lokal perusahaan. Melalui interkoneksi ini mereka dapat mengakses database perusahaan, email, Internet, dan aplikasi perangkat lunak lainnya. Sadar akan ekspektasi konsumen seperti ini, produsen komputer dan komputer terus-menerus menciptakan perangkat baru untuk interkoneksi ke komputer. Perangkat periferal ini antara lain mencakup perangkat pemutaran musik (seperti iPod), pemindai dokumen, kamera digital, dan kamera video.

Menghubungkan perangkat periferal ke komputer bisa menjadi tugas yang menantang. Berbagai tingkat perangkat keras dan perangkat lunak harus disetujui sepenuhnya sebelum komputer dapat “berbicara” dengan perangkat, atau sebaliknya. Pertanyaan seperti berikut ini perlu diselesaikan: Apakah konektor di ujung kabel yang berasal dari perangkat kompatibel dengan konektor di bagian belakang komputer? Akankah sifat kelistrikan kedua perangkat tersebut kompatibel? Meskipun jawaban atas pertanyaan-pertanyaan ini adalah ya, pertanyaan lain tetap ada: Akankah komputer dan perangkat “berbicara dalam bahasa yang sama”? Menghubungkan komputer ke perangkat lain memiliki banyak kendala dan kendala.

Untuk lebih memahami interkoneksi antara komputer dan perangkat periferal, Anda harus terlebih dahulu memahami konsep antarmuka. Dianggap terutama sebagai aktivitas lapisan fisik, antarmuka adalah proses yang kompleks dan relatif teknis yang sangat bervariasi tergantung pada jenis perangkat, komputer, dan koneksi yang diinginkan antara perangkat dan komputer.

Kita akan memeriksa empat komponen dasar antarmuka—listrik, mekanis, fungsional, dan prosedural—dan kemudian memperkenalkan beberapa standar antarmuka yang lebih umum, seperti Universal Serial Bus, FireWire, Thunderbolt, SCSI, iSCSI, InfiniBand, dan Saluran Fibre.

Namun, menghubungkan komputer ke perangkat memerlukan lebih dari sekadar menyelesaikan koneksi pada lapisan fisik. Penting juga untuk menentukan pengemasan data saat ditransfer antara komputer dan perangkat. Secara umum, konfigurasi dasar kemasan ini ditentukan oleh standar lapisan data link. Oleh karena itu, kita akan memeriksa tiga konfigurasi lapisan data link yang populer: koneksi asinkron, koneksi sinkron, dan koneksi isokron.

Terakhir, kita akan memeriksa hubungan antara terminal dan komputer mainframe. Karena terminal merupakan perangkat yang relatif tidak cerdas, komputer mainframe menciptakan dialog unik yang disebut polling, yang meminta terminal untuk melihat apakah ia mempunyai data untuk dikirimkan ke mainframe.

Namun pertama-tama mari kita mulai dengan dasar-dasar menghubungkan komputer ke perangkat lain.

4.2 INTERFACING KOMPUTER KE PERANGKAT PERIPHERAL

Kebanyakan orang akan setuju bahwa komputer adalah alat yang luar biasa. Alat ini mampu melakukan berbagai macam operasi terutama karena dua fakta penting: komputer dapat diprogram, dan dapat terhubung ke berbagai perangkat input/output, atau periferal. Koneksi ke periferal sering disebut antarmuka, dan proses menyediakan semua interkoneksi yang tepat antara komputer dan periferal disebut interfacing. Anda tidak dapat mendiskusikan antarmuka tanpa membahas standar. Kita akan membahas berbagai jenis koneksi, dan setiap koneksi akan memiliki banyak kemungkinan lapisan standar antarmuka. Menghubungkan perangkat ke komputer dianggap sebagai aktivitas lapisan fisik karena berhubungan langsung dengan sinyal analog, sinyal digital, dan komponen perangkat keras.

Mari kita mulai diskusi kita tentang antarmuka dengan menjelajahi karakteristik umum standar antarmuka dan kemudian memeriksa fitur-fitur khusus dari standar antarmuka yang sangat populer—Universal Serial Bus—dan beberapa antarmuka berkecepatan tinggi yang lebih baru.

Karakteristik standar antarmuka

Bertahun-tahun yang lalu, produsen dan pengguna komputer dan periferal menyadari bahwa jika satu perusahaan membuat komputer dan perusahaan lain membuat perangkat periferal, peluang keduanya untuk dapat “berbicara” satu sama lain sangat kecil. Oleh karena itu, berbagai organisasi mulai menciptakan antarmuka standar antara perangkat seperti komputer dan modem. Namun, karena terdapat begitu banyak lingkungan transmisi dan antarmuka yang berbeda, satu standar saja tidak cukup. Hasilnya, ratusan standar telah diciptakan. Meskipun demikian, semua standar antarmuka mempunyai dua karakteristik dasar: Telah dibuat dan disetujui oleh organisasi pembuat standar yang dapat diterima, dan dapat terdiri dari satu hingga empat komponen, yang masing-masing akan dibahas segera. Organisasi utama yang terlibat dalam pembuatan standar adalah:

- Persatuan Telekomunikasi Internasional (ITU), sebelumnya Komite Konsultatif Telegraf dan Telepon Internasional (CCITT)
- Asosiasi Industri Elektronik (EIA) yang kini sudah tidak ada lagi
- Institut Insinyur Listrik dan Elektronika (IEEE)
- Organisasi Internasional untuk Standardisasi (ISO)
- Institut Standar Nasional Amerika (ANSI)

Seringkali, masing-masing perusahaan terburu-buru untuk memasarkan produknya sehingga mereka akan menciptakan produk baru yang menggunakan protokol antarmuka yang tidak standar. Meskipun ada keuntungan pemasaran yang pasti untuk menjadi yang pertama menawarkan teknologi baru, ada juga kerugian besar jika menggunakan protokol antarmuka yang belum disetujui oleh salah satu organisasi pembuat standar tersebut. Misalnya, segera setelah perusahaan Anda memperkenalkan produk barunya, salah satu organisasi pembuat standar mungkin membuat protokol baru yang menjalankan fungsi yang sama dengan protokol non-standar Anda, dan hal ini mungkin menyebabkan produk perusahaan Anda menjadi usang. Dalam dunia teknologi komputer yang berubah dengan cepat, menciptakan produk yang sesuai dengan standar antarmuka yang disetujui adalah hal yang sulit namun

sangat disarankan. Kadang-kadang, sebuah perusahaan akan membuat protokol yang, meskipun bukan standar resmi, menjadi sangat populer sehingga perusahaan lain mulai menggunakannya. Dalam hal ini, protokol dianggap sebagai standar *de facto*. Misalnya, sistem operasi Microsoft untuk komputer pribadi bukanlah standar resmi. Meskipun demikian, sekitar 90 persen dari seluruh komputer pribadi menggunakan sistem operasi Microsoft, sehingga menjadikan sistem operasi desktop Windows sebagai standar *de facto*.

Karakteristik dasar kedua dari standar antarmuka adalah komposisinya. Standar antarmuka dapat terdiri dari empat bagian, atau komponen, yang semuanya berada pada lapisan fisik: komponen listrik, komponen mekanis, komponen fungsional, dan komponen prosedural. Semua standar yang ada saat ini membahas satu atau lebih komponen-komponen ini. Komponen kelistrikan berhubungan dengan voltase, kapasitansi saluran, dan masalah kelistrikan lainnya. Komponen kelistrikan standar antarmuka terutama merupakan tanggung jawab teknisi, dan oleh karena itu kami tidak akan membahasnya secara mendetail. Komponen mekanis berkaitan dengan item seperti deskripsi konektor atau konektor. Pertanyaan yang biasanya diajukan oleh komponen mekanis meliputi: Apa ukuran dan bentuk konektor? Berapa banyak pin yang ditemukan pada konektor? Bagaimana susunan pinnya? Komponen fungsional menjelaskan fungsi setiap pin (yang disebut sebagai rangkaian jika Anda juga memperhitungkan sinyal yang berjalan melalui pin dan kabel) yang digunakan dalam antarmuka tertentu. Komponen prosedural menjelaskan bagaimana sirkuit tertentu digunakan untuk melakukan suatu operasi. Meskipun komponen fungsional dari standar antarmuka mungkin, misalnya, menggambarkan dua sirkuit, seperti Permintaan untuk Mengirim dan Hapus untuk Mengirim, komponen prosedural akan menjelaskan bagaimana kedua sirkuit ini digunakan sehingga komputer dapat mentransfer data ke periferal, dan sebaliknya.

Standar antarmuka awal

Antarmuka USB saat ini merupakan bentuk antarmuka komputer pribadi yang paling populer dan mungkin akan tetap seperti itu selama beberapa waktu. Namun tidak selalu seperti itu. Mari kita perkenalkan secara singkat salah satu standar antarmuka sebelumnya hanya untuk memberi Anda titik referensi mengenai sejauh mana kemajuannya. Antarmuka RS-232, yang dibuat pada tahun 1962, adalah contoh klasik dari salah satu antarmuka awal. Karena popularitasnya, RS-232 telah berevolusi—bukannya menjadi usang—selama bertahun-tahun, dan inkarnasinya saat ini diberi nama EIA-232F (juga dikenal sebagai TIA-232-F). Lebih tepatnya, EIA-232F adalah standar antarmuka untuk menghubungkan komputer atau terminal (atau DTE) ke modem tingkat suara (atau DCE) untuk digunakan pada sistem telekomunikasi publik analog. (Dalam terminologi antarmuka modem, ujung komputer [atau terminal] dari sebuah antarmuka disebut sebagai peralatan terminasi data [DTE], sedangkan modem disebut sebagai peralatan komunikasi data [DCE].)

Perlu dicatat bahwa antarmuka EIA-232F adalah apa yang kami sebut koneksi dupleks penuh. Koneksi full-duplex adalah koneksi dimana pengirim dan penerima dapat mengirimkan secara bersamaan. Hal ini dimungkinkan dengan EIA-232F karena terdapat satu kabel untuk transmisi dan kabel terpisah untuk penerima. Beberapa sistem, karena berbagai alasan, hanya

memperbolehkan satu pihak atau pihak lain (yaitu pengirim atau penerima) untuk mengirimkan pada satu waktu. Jenis koneksi ini, seperti yang akan kita lihat sebentar lagi, adalah contoh koneksi setengah dupleks.

Meskipun standar EIA-232F berumur panjang, nampaknya standar antarmuka lain pada dasarnya telah menggantikannya. Meskipun demikian, EIA-232F adalah contoh klasik dari standar antarmuka, dan studinya memberikan gambaran menarik tentang cara kerja komunikasi antara komputer dan perangkat. Sekarang mari kita lihat standar antarmuka yang menggantikan EIA-232F.

Bus Serial Universal (USB)

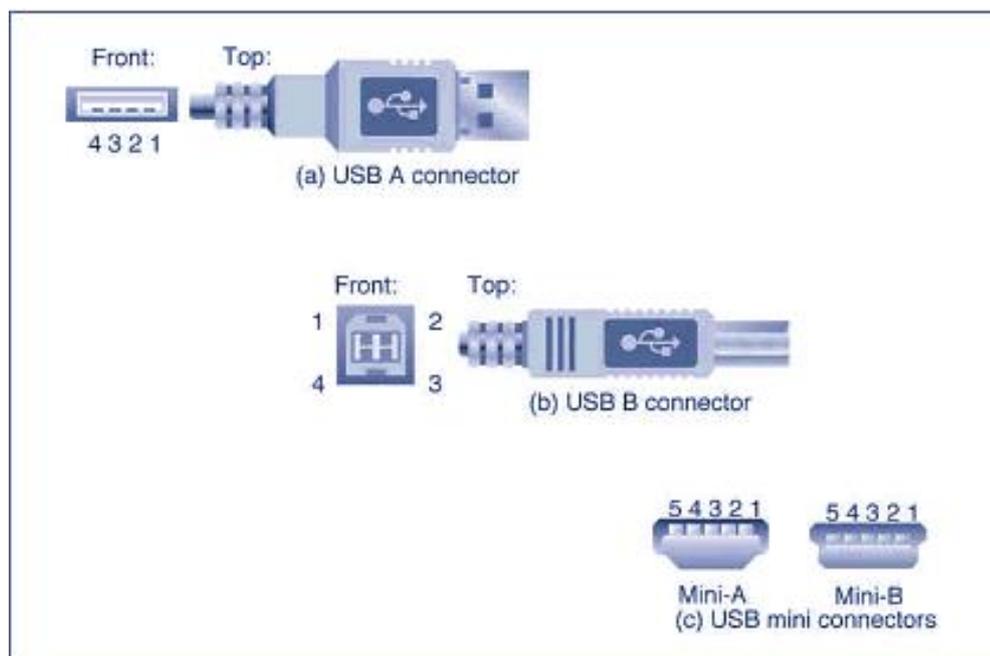
Universal Serial Bus (USB) adalah standar modern untuk menghubungkan berbagai jenis perangkat perifer ke komputer. Lebih tepatnya, USB adalah antarmuka digital yang menggunakan konektor (colokan) standar untuk semua perangkat berjenis serial dan paralel. Karena USB menyediakan antarmuka digital, maka tidak perlu mengubah sinyal digital komputer mikro menjadi sinyal analog untuk ditransfer melalui sambungan. Seperti yang mungkin Anda ingat dari Bab Dua, sistem yang menjalani konversi digital-ke-analog atau analog-ke-digital biasanya memiliki lebih banyak noise pada sinyalnya sebagai akibat dari konversi tersebut. USB menghindari munculnya kebisingan tersebut. Selain itu, USB adalah kabel yang relatif tipis dan hemat ruang untuk digunakan di berbagai perangkat dapat ditambahkan dan dihapus saat komputer dan perifer aktif—fitur yang membuat USB hot pluggable. Gagasan di balik hot plugging adalah bahwa perifer cukup dicolokkan dan dihidupkan, dan komputer harus secara dinamis mengenali perangkat dan membangun antarmuka. Dengan kata lain, casing komputer tidak harus dibuka, dan tidak perlu mengatur saklar perangkat lunak atau perangkat keras apa pun. Saat menggunakan perifer yang dirancang dengan konektor USB, satu perifer USB juga dapat dihubungkan ke perifer lainnya. Teknik menghubungkan perangkat ke setiap perangkat berikutnya (bukan kembali ke komputer) dikenal sebagai daisy-chaining. Fitur unik lainnya dari USB adalah kabel USB dapat menyediakan daya listrik yang diperlukan untuk mengoperasikan perangkat. Dengan opsi ini, tidak perlu mencari beberapa outlet listrik (satu untuk setiap perifer). Terakhir, transfer data melalui kabel USB bersifat dua arah, namun hanya satu perangkat—komputer atau perifer—yang dapat melakukan transmisi pada satu waktu. Hal ini menjadikan USB contoh lain dari koneksi setengah dupleks.

Kelemahan awal USB, setidaknya jika dibandingkan dengan antarmuka berkecepatan tinggi lainnya (seperti FireWire, yang akan dibahas segera), adalah kecepatannya yang relatif lambat. USB versi 1.1 memiliki kecepatan transfer maksimum 12 Mbps, jauh lebih lambat dibandingkan FireWire yang 400 Mbps. Untungnya, USB versi 2.0 memiliki kecepatan transfer maksimum 480 Mbps dan kompatibel dengan versi 1.1 sebelumnya, memungkinkan perangkat dengan antarmuka yang lebih baru untuk terhubung dengan antarmuka yang lebih lama (tetapi dengan kecepatan 12-Mbps). Lebih tepatnya, USB 2.0 dapat mendukung perangkat berkecepatan rendah (10 hingga 100 Kbps) seperti keyboard, mouse, dan perifer game; perangkat berkecepatan penuh (500 Kbps hingga 10 Mbps) seperti sirkuit telepon, audio, dan video terkompresi; dan perangkat berkecepatan tinggi (kecepatan lebih besar dari

10 Mbps) seperti video, perangkat pencitraan, dan broadband. Versi terbaru—USB 3.0—memiliki kecepatan 4,8 Gbps (10 kali lebih cepat dibandingkan USB 2.0) dan dirilis pada November 2008.

Seperti yang baru saja kita pelajari, standar antarmuka terdiri dari empat komponen. Dengan standar USB, komponen kelistrikan dan fungsi mendukung transfer daya dan sinyal melalui kabel empat kawat. Dua dari empat kabel ini, VBUS dan GND (ground), membawa sinyal 5 volt yang dapat digunakan untuk memberi daya pada perangkat. Dua kabel lainnya, D+ dan D–, membawa data dan informasi sinyal.

Komponen mekanis USB secara ketat menentukan dimensi pasti dari konektor dan kabel antarmuka. Empat jenis konektor USB ditentukan: konektor A, konektor B, konektor mini A, dan konektor mini B. Seperti yang Anda lihat pada Gambar 4-1, konektor A dan B memiliki empat pin, satu untuk masing-masing dari empat kabel pada komponen kelistrikan, sedangkan konektor mini memiliki lima pin. Pin kelima pada konektor mini disebut pin sinyal dan sering kali hanya dihubungkan ke pin VBUS atau GND. Meskipun terdapat empat jenis konektor yang berbeda, konektor A tampaknya yang paling umum digunakan.



Gambar 4-1 Empat jenis konektor USB

Komponen prosedural USB mungkin yang paling terlibat dari keempat komponen tersebut. Untuk memahami cara kerjanya, pertama-tama Anda harus memahami dua istilah: bus dan polling. Bus hanyalah koneksi berkecepatan tinggi yang dapat dihubungkan dengan beberapa perangkat, dan polling (yang dijelaskan secara lebih rinci di bagian bab ini tentang koneksi komputer terminal-ke-mainframe) adalah proses di mana komputer menanyakan periferal apakah itu memiliki data untuk dikirimkan ke komputer. USB adalah bus yang disurvei di mana pengontrol host (antarmuka USB ke komputer host) memulai semua transfer data. Bus USB dapat mengenali ketika perangkat USB telah dihubungkan ke port USB atau ke hub

USB (perangkat yang seperti kabel ekstensi dan dapat menyediakan beberapa port USB). Itu juga dapat mengenali kapan perangkat yang sama telah dihapus. Selain itu, bus USB dapat mendukung empat tipe dasar transfer data: transfer kontrol, yang digunakan untuk mengkonfigurasi perangkat periferal pada saat pemasangan; transfer data massal, yang digunakan untuk mendukung data dalam jumlah besar dan bursty (yaitu, diproduksi secara burst); mengganggu transfer data, yang digunakan untuk pengiriman data yang tepat waktu namun dapat diandalkan; dan transfer data isochronous, yang, seperti akan kita lihat nanti di bab ini, merupakan koneksi yang memerlukan transfer data secara terus-menerus dan real-time, seperti streaming audio dan video.

Karena kekuatan dan fleksibilitas USB, kemungkinan besar ini akan menjadi antarmuka yang paling umum digunakan di masa depan. Jika hal ini terjadi, kita akan melihat contoh lain dari konvergensi: konvergensi menuju standar antarmuka tunggal yang mampu mendukung beragam perangkat pada berbagai kecepatan transfer, dan secara otomatis mengenali ketika perangkat terpasang dan memperoleh driver yang sesuai.

Standar antarmuka lainnya

Selain USB, standar antarmuka lainnya telah dibuat selama bertahun-tahun untuk menyediakan koneksi berkecepatan tinggi ke berbagai jenis perangkat periferal. Seperti yang akan segera kita pelajari, beberapa standar ini, seperti FireWire, berfungsi seperti USB dan, mengingat kekuatan USB yang besar, suatu hari nanti mungkin akan digantikan oleh USB—sementara standar lainnya akan digunakan bersamaan dengan USB karena dirancang untuk mendukung berbagai bentuk komunikasi. antarmuka. Mari kita lanjutkan pembahasan kita tentang standar antarmuka dengan memeriksa lima protokol lagi yang dirancang untuk berfungsi sebagai antarmuka berkecepatan tinggi antara komputer dan perangkat periferal: FireWire, Thunderbolt, SCSI, iSCSI, InfiniBand, dan Fibre Channel.

Kawat Api

Diciptakan oleh Apple Computer pada pertengahan 1990an, dan kemudian distandarisasi oleh IEEE sebagai standar nomor 1394, FireWire adalah jenis interkoneksi antara perangkat periferal (seperti modem nirkabel dan kamera video digital berkecepatan tinggi) dan komputer mikro. FireWire merupakan antarmuka digital yang mudah digunakan, fleksibel, dan berbiaya rendah yang mampu mendukung kecepatan transfer hingga 400 Mbps. (Versi FireWire terbaru yang mendukung 3,2 Gbps telah disetujui pada tahun 2007.) Karena FireWire, seperti USB, menyediakan antarmuka digital, maka tidak perlu mengubah sinyal digital komputer mikro menjadi sinyal analog untuk ditransfer melalui sambungan. Oleh karena itu, FireWire, seperti halnya USB, menghindari gangguan jenis ini ke dalam sinyal. Selain itu, FireWire juga mirip dengan USB karena dapat dicolokkan secara panas.

FireWire mendukung dua jenis koneksi data: asinkron dan isokron. Kedua koneksi data ini akan dibahas secara rinci nanti dalam bab ini, namun secara singkat, koneksi asynchronous mendukung perangkat periferal yang lebih tradisional seperti modem dan printer, dan koneksi isochronous memberikan jaminan transportasi data pada kecepatan yang telah ditentukan. yang penting untuk aplikasi multimedia. Aplikasi multimedia hampir unik karena memerlukan pengangkutan data penting dan tepat waktu tanpa gangguan. FireWire adalah pilihan yang

baik untuk menghubungkan elektronik konsumen digital dan periferal audio dan visual, seperti kamera video digital dan kamera digital.

Petir

Penambahan terbaru pada daftar standar antarmuka adalah Thunderbolt. Saat ini ditemukan di laptop Apple dan menyediakan koneksi 10 Gbps ke perangkat periferal. Ia menggunakan konektor yang sama dengan Mini DisplayPort yang sudah ada dan menggunakan protokol yang sudah ada yang disebut PCI Express. Dengan menggabungkan dua protokol yang ada (PCI Express didukung oleh hampir semua Intel chipset), relatif mudah untuk membuat antarmuka serial rantai daisy berkecepatan tinggi yang baru. Meskipun desain Thunderbolt pada awalnya dirancang sebagai konektor serat optik, namun kini menjadi populer sebagai konektor kabel tembaga, sehingga menekan biaya. Rumor mengatakan bahwa Thunderbolt pada akhirnya akan mencapai kecepatan data 100 Gbps di masa depan.

SCSI dan iSCSI

SCSI, yang merupakan singkatan dari Small Computer System Interface dan diucapkan “skuzzy,” adalah teknik untuk menghubungkan komputer ke perangkat berkecepatan tinggi seperti hard disk drive, tape drive, CD, dan DVD. Jika USB dan FireWire didesain untuk digunakan dengan perangkat yang dapat ditambahkan dan dilepas, sehingga bersifat hot pluggable, SCSI dirancang untuk mendukung perangkat yang bersifat lebih permanen. Konsekuensinya, SCSI adalah sebuah antarmuka sistem—bukan hanya sebuah teknik antarmuka untuk hard disk drive (seperti yang diyakini sebagian orang)—dan sejalan dengan itu, SCSI mengoptimalkan interaksi antara perangkat input/output dan prosesor pusat komputer.

Untuk memanfaatkan antarmuka SCSI berkecepatan lebih tinggi, Anda perlu menginstal adaptor SCSI di komputer Anda. Setelah adaptor ini dipasang, Anda dapat menghubungkan hingga tujuh perangkat SCSI yang berbeda. Untuk menghubungkan beberapa perangkat SCSI ke satu adaptor SCSI, setiap perangkat tambahan dihubungkan ke perangkat SCSI sebelumnya, atau dirangkai secara daisy-chain. Antarmuka SCSI telah ada selama beberapa waktu (sejak 1986) dan telah mengalami sejumlah modifikasi. Oleh karena itu, terdapat berbagai teknik SCSI, mulai dari Fast SCSI dan UltraSCSI hingga Narrow SCSI dan Wide SCSI. Masing-masing teknik ini berbeda berdasarkan kecepatan transmisi yang didukungnya dan jumlah bit yang ditransfer pada saat tertentu (yang ditetapkan seolah-olah itu adalah “lebar” kabel). Misalnya, Ultra160 SCSI dirancang untuk transfer data hingga 160 MB per detik, yang, Anda akan lihat, hampir tiga kali lebih cepat dibandingkan 480 Mbps pada USB 2.0. Meskipun ada beberapa keunggulan SCSI, banyak yang merasa bahwa SCSI pada akhirnya akan digantikan oleh USB.

Terlepas dari itu, SCSI masih dapat ditemukan pada workstation dan server jaringan berkinerja tinggi. Variasi lain yang lebih baru pada antarmuka SCSI adalah iSCSI. iSCSI, atau Internet SCSI, adalah teknik untuk menghubungkan penyimpanan disk ke komputer melalui Internet. Jadi, jika Anda memiliki penyimpanan disk dalam jumlah besar yang terletak di tempat lain di Internet, Anda dapat menghubungkan komputer Anda ke penyimpanan tersebut menggunakan Internet dan standar antarmuka iSCSI. Pada dasarnya apa yang terjadi

di sini adalah bahwa perintah SCSI dienkapsulasi dalam paket TCP/IP dan dikirim melalui Internet, seperti perintah Internet pada umumnya seperti mengirim email atau meminta halaman Web.

InfiniBand dan Saluran Fibre

InfiniBand dan Fibre Channel adalah dua protokol modern yang digunakan untuk menghubungkan komputer ke perangkat input/output melalui koneksi berkecepatan tinggi. Mereka sering ditemukan pada jaringan yang memerlukan penyimpanan periferal dalam jumlah besar. Misalnya, jika sebuah bisnis perlu menghubungkan penyimpanan hard disk dalam jumlah besar ke jaringan area lokal, InfiniBand atau Fibre Channel dapat memenuhi tagihan tersebut. Lebih tepatnya, InfiniBand adalah koneksi serial atau bus yang dapat membawa banyak saluran data secara bersamaan. Ini dapat mendukung kecepatan transfer data 2,5 miliar bit (2,5 gigabit) per detik (kecepatan data tunggal), 5 gigabit per detik (kecepatan data ganda), dan 10 gigabit per detik (kecepatan data quad); dan dapat mengatasi (interkoneksi) ribuan perangkat menggunakan kabel tembaga dan kabel serat optik. Daripada menjadi satu bus bersama, InfiniBand adalah jaringan link dan switch berkecepatan tinggi. Dengan demikian, lalu lintas yang dilewatkan antara komputer dan perangkat input/outputnya sebenarnya bergerak melalui jaringan berkecepatan tinggi.

Fibre Channel mirip dengan InfiniBand karena merupakan jaringan serial berkecepatan tinggi yang menghubungkan komputer ke beberapa perangkat input/output. Fibre Channel juga mendukung kecepatan transfer data hingga miliaran bit per detik, namun mampu mendukung interkoneksi hingga 126 perangkat saja.

Jelasnya, antarmuka telah berkembang pesat sejak awal EIA-232. Jika tren antarmuka yang sederhana namun canggih seperti USB, Thunderbolt, FireWire, SCSI, dan Fibre Channel terus berlanjut (seperti yang pasti akan terjadi), topik antarmuka menggunakan EIA-232F suatu hari akan menjadi sejarah kuno. Sekarang mari kita mengalihkan perhatian kita dari properti lapisan fisik komputer ke koneksi periferal dan berkonsentrasi pada properti data link dari sebuah koneksi.

4.3 KONEKSI TAUTAN DATA

Seperti yang telah kita lihat, standar antarmuka seperti USB dan Thunderbolt terdiri dari empat komponen: listrik, mekanik, fungsional, dan prosedural. Karena keempat komponen ini menentukan koneksi fisik antara komputer dan periferal, maka keempat komponen ini berada pada lapisan fisik rangkaian protokol TCP/IP. Namun menciptakan koneksi lebih dari sekadar mendefinisikan berbagai komponen fisik. Agar berhasil mengirimkan data antara dua titik di jaringan, misalnya antara stasiun kerja dan server jaringan, kita juga perlu menentukan koneksi tautan data. Jika kita sekali lagi menghubungkan ini dengan rangkaian protokol TCP/IP, Anda akan melihat bahwa definisi koneksi data link dilakukan pada data link, atau lapisan akses jaringan.

Untuk memahami masalah yang terlibat dalam pendefinisian koneksi data link, pertama-tama asumsikan bahwa koneksi lapisan fisik sudah ditentukan oleh beberapa protokol seperti USB. Sekarang, mengingat pengirim dan penerima menggunakan protokol

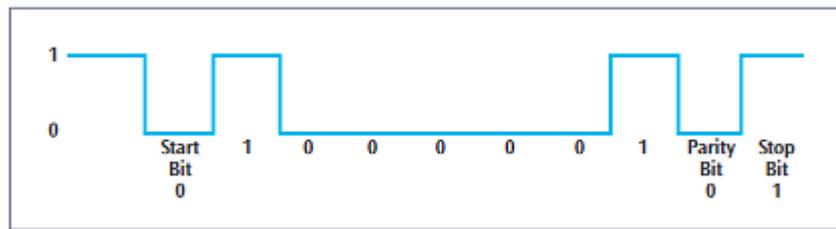
lapisan fisik yang sama, pertanyaan selanjutnya yang harus diselesaikan adalah sebagai berikut: Apa bentuk dasar dari bingkai data yang diteruskan antara pengirim dan penerima? Apakah data dikirimkan dalam blok byte tunggal, atau apakah koneksi membuat blok multi-byte yang lebih besar? Opsi transmisi data sebelumnya adalah contoh koneksi asinkron, sedangkan opsi kedua adalah koneksi sinkron. Apakah data harus dikirimkan dengan kecepatan konstan, seperti yang diperlukan untuk sambungan kamera video? Jika ya, ini adalah contoh koneksi isokron. Bisakah koneksi mengirimkan data dua arah secara bersamaan, atau hanya satu arah dalam satu waktu? Seperti yang telah kita pelajari, inilah perbedaan antara koneksi full-duplex dan koneksi half-duplex. Pertanyaan seperti ini menentukan jenis koneksi yang ditemukan pada lapisan data link.

Saat memeriksa koneksi data link, ingatlah tugas lapisan data link dari rangkaian protokol TCP/IP—dua di antaranya adalah membuat kerangka data untuk transmisi antara pengirim dan penerima, dan menyediakan beberapa cara untuk memeriksa kesalahan selama penulatan. Ingatlah tugas-tugas ini saat kita memeriksa tiga jenis koneksi data link yang berbeda.

Koneksi asinkron

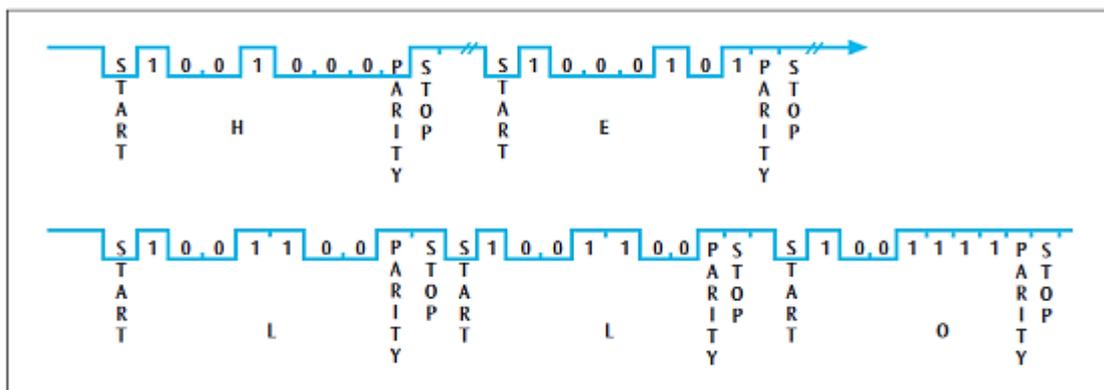
Koneksi asynchronous adalah salah satu contoh paling sederhana dari protokol data link dan ditemukan terutama pada koneksi mikrokomputer-ke-dial-up-modem dan terminal-ke-modem. Dalam koneksi asynchronous, satu karakter, atau byte data, adalah unit transfer antara pengirim dan penerima. Pengirim menyiapkan karakter data untuk transmisi, mengirimkan karakter tersebut, dan kemudian mulai menyiapkan karakter data berikutnya untuk transmisi.

Mungkin ada waktu yang tidak terbatas antara transmisi satu karakter data dan transmisi karakter berikutnya. Untuk mempersiapkan karakter data untuk transmisi, beberapa bit informasi tambahan ditambahkan ke bit data karakter untuk membuat bingkai, atau paket data kecil. Bit awal, yang selalu berlogika 0, ditambahkan ke awal karakter dan menginformasikan kepada penerima bahwa bingkai data masuk telah tiba. Bit awal juga memungkinkan penerima untuk menyinkronkan dirinya dengan karakter. Di akhir karakter data, satu atau dua bit stop, yang selalu berlogika 1, ditambahkan untuk menandakan akhir frame. (Meskipun biasanya hanya ada satu bit stop, beberapa sistem memperbolehkan pilihan satu atau dua.) Bit awal dan bit stop, pada dasarnya, menyediakan bingkai awal dan akhir di sekitar data. Terakhir, satu bit paritas, yang disisipkan di antara bit data dan bit stop, dapat ditambahkan ke data. Bit paritas ini (dibahas secara lebih rinci di Bab Enam) dapat menunjukkan paritas genap atau paritas ganjil, dan melakukan pemeriksaan kesalahan hanya pada bit data. Pemeriksaan kesalahan ini dicapai dengan menambahkan 0 atau 1 sedemikian rupa sehingga jumlah 1 yang genap atau ganjil dipertahankan. Gambar 4-2 menunjukkan contoh karakter A (dalam ASCII) dengan satu bit awal, satu bit akhir, dan bit paritas genap ditambahkan.



Gambar 4-2 Contoh karakter A dengan satu bit awal, satu bit akhir, dan paritas genap

Karena setiap karakter mempunyai bit awal, akhir, dan paritasnya masing-masing, transmisi beberapa karakter, seperti HELLO, dapat dilakukan. Gambar 4-3 menunjukkan transmisi HELLO.



Gambar 4-3 Contoh string karakter HELLO yang menyertakan bit start, stop, dan parity

Koneksi asinkron memiliki kelebihan dan kekurangan. Sisi positifnya, pembuatan bit start, stop, dan parity sederhana dan memerlukan sedikit perangkat keras atau perangkat lunak. Sisi negatifnya, koneksi asinkron memiliki satu kelemahan khusus yang tidak dapat diabaikan. Mengingat bahwa tujuh bit data (kumpulan kode karakter ASCII) sering digabungkan dengan satu bit awal, satu bit akhir, dan satu bit paritas, karakter yang ditransmisikan yang dihasilkan berisi tiga bit pemeriksaan dan tujuh bit data, dengan rasio 3:7. Dalam skenario ini dengan total 10 bit pemeriksaan dan data, 3 dari 10—atau 30 persen—bit digunakan sebagai bit pemeriksaan.

Rasio bit pemeriksaan terhadap bit data ini tidak terlalu efisien untuk transfer data dalam jumlah besar dan, oleh karena itu, mengakibatkan transfer data menjadi lambat. Menariknya, istilah “koneksi asinkron” menyesatkan bagi pemula karena protokol sebenarnya, meskipun ada kata “asinkron”, mempertahankan sinkronisasi dengan aliran data yang masuk. Ingat kembali dari Bab Dua pentingnya penerima tetap tersinkronisasi dengan aliran data yang masuk, terutama jika aliran data berisi rangkaian panjang nilai yang tidak berubah. Kode Manchester dirancang untuk membantu mengatasi masalah ini, namun kode tersebut belum dibuat ketika koneksi asinkron dikembangkan. Dengan demikian, koneksi asinkron menggabungkan metodenya sendiri untuk menjaga agar penerima tetap

tersinkronisasi dengan aliran data yang masuk. Bagaimana mereka melakukannya? Dua fitur utama koneksi asinkron membantu mereka mempertahankan sinkronisasi:

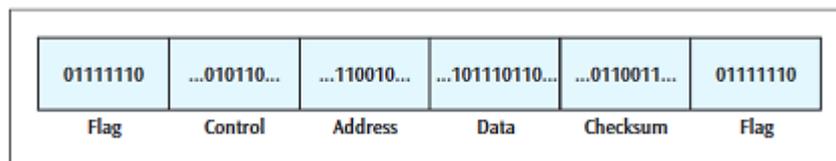
- Ukuran frame—Karena setiap frame dalam koneksi asinkron terdiri dari satu karakter ditambah beberapa bit pengecekan, penerima hanya akan menerima sejumlah kecil informasi pada satu waktu. Oleh karena itu, tidak akan sulit bagi receiver untuk tetap tersinkronisasi dalam waktu singkat.
- Bit awal—Bila penerima mengenali bit awal, sinkronisasi akan dimulai. Karena hanya sekitar 8 atau 9 bit yang mengikuti, tidak akan ada rangkaian panjang nilai yang tidak berubah.

Selama tahun-tahun awal industri mikrokomputer, kesederhanaan (dan biaya rendah) dari koneksi asynchronous cocok untuk segmen pasar penghobi. Namun pasar segmen bisnis membutuhkan koneksi data link yang lebih efisien dan bertenaga. Bisnis memerlukan koneksi yang efisien dan berkecepatan lebih tinggi—koneksi yang sinkron.

Selama tahun-tahun awal industri mikrokomputer, kesederhanaan (dan biaya rendah) dari koneksi asynchronous cocok untuk segmen pasar penghobi. Namun pasar segmen bisnis membutuhkan koneksi data link yang lebih efisien dan bertenaga. Bisnis memerlukan koneksi yang efisien dan berkecepatan lebih tinggi—koneksi yang sinkron.

Koneksi sinkron

Jenis koneksi data link yang kedua (dengan nama yang tidak terlalu menyesatkan) adalah koneksi sinkron. Dengan koneksi sinkron, unit transmisi adalah rangkaian karakter. Urutan karakter ini mungkin berukuran ribuan karakter. Mirip dengan cara bit awal, akhir, dan paritas mbingkai bit data dalam koneksi asinkron, urutan awal (bendera), byte kontrol, alamat, checksum, dan urutan akhir (bendera) mbingkai bit data dalam a koneksi sinkron, seperti yang ditunjukkan pada Gambar 4-4.



Gambar 4-4 Diagram blok bagian-bagian sambungan sinkron generik

Urutan awal dan akhir dari koneksi sinkron disebut flag dan masing-masing biasanya panjangnya 8 bit (satu byte). Mengikuti tanda urutan awal biasanya berisi satu atau lebih byte informasi kontrol. Informasi kontrol ini memberikan informasi tentang data yang disertakan atau memberikan informasi status mengenai pengirim atau penerima atau keduanya. Misalnya, bit unik dalam byte informasi kontrol dapat diatur ke 1, yang menunjukkan bahwa data yang disertakan memiliki prioritas tinggi. Seringkali byte kontrol berisi informasi pengalamatan yang menunjukkan dari mana data tersebut berasal, atau untuk siapa data tersebut ditujukan. Bidang alamat menunjukkan tujuan frame, asal frame, atau keduanya. Mengikuti data hampir selalu merupakan suatu bentuk urutan pengecekan kesalahan, seperti checksum siklik. Checksum siklik (dijelaskan secara rinci di Bab Enam) adalah teknik

pengecekan kesalahan yang lebih canggih daripada pengecekan paritas dan digunakan dalam banyak implementasi jaringan komputer modern. Setelah urutan pengecekan kesalahan adalah tanda urutan akhir.

Bagaimana koneksi sinkron menjaga pengirim dan penerima tetap tersinkronisasi? Pertanyaan ini sangat penting karena dimungkinkan untuk mengirim ribuan karakter dalam satu paket. Tiga metode digunakan untuk menjaga sinkronisasi dalam koneksi sinkron:

- Kirim sinyal jam sinkronisasi melalui jalur terpisah yang berjalan paralel dengan aliran data. Saat data tiba di satu jalur, sinyal jam tiba di jalur kedua. Penerima dapat menggunakan sinyal jam ini untuk tetap tersinkronisasi dengan data yang masuk.
- Jika mengirimkan sinyal digital, gunakan kode Manchester. Karena kode Manchester selalu mempunyai transisi sinyal di tengah setiap bit, penerima dapat mengantisipasi transisi sinyal ini dan membaca aliran data yang masuk tanpa kesalahan. Sinyal digital berkode Manchester adalah contoh sinyal self-clocking.
- Jika mentransmisikan sinyal analog, gunakan properti sinyal analog itu sendiri untuk self-clocking. Misalnya, sinyal analog dengan perubahan fasa periodik dapat memberikan sinkronisasi yang diperlukan.

Karena efisiensinya yang lebih tinggi, sambungan sinkron hampir sepenuhnya menggantikan sambungan asinkron. Namun masih ada satu jenis koneksi lagi yang perlu diperkenalkan: koneksi isochronous.

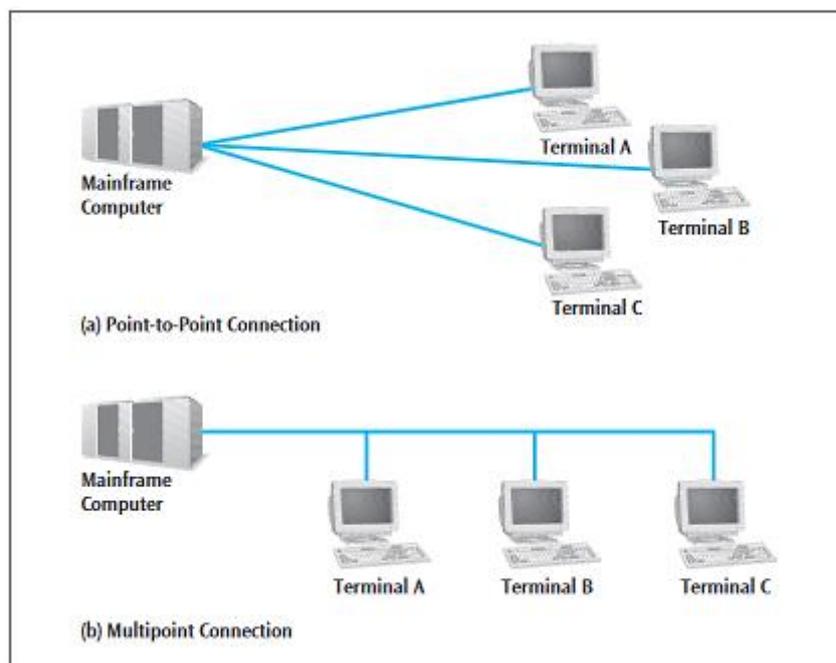
Koneksi isokron

Koneksi isochronous adalah jenis koneksi data link khusus yang digunakan untuk mendukung berbagai jenis aplikasi real-time. Contoh aplikasi real-time biasanya mencakup streaming suara, video, dan musik. Aplikasi real-time memiliki keunikan karena datanya harus dikirimkan ke komputer dengan kecepatan yang tepat. Jika data dikirimkan terlalu lambat, maka musik akan terdistorsi, atau video akan pecah. Jika data dikirim terlalu cepat, komputer penerima mungkin tidak dapat melakukan buffering data, yang mungkin mengakibatkan data hilang.

Seperti yang kita pelajari sebelumnya di bab ini, USB dan FireWire dapat mendukung koneksi isochronous. Namun, sebelum transfer data dapat dimulai, sumber daya isochronous yang tepat harus dialokasikan dalam koneksi. Untuk melakukan alokasi ini, pengirim dan penerima bertukar sejumlah paket awal, yang antara lain menentukan saluran apa yang akan digunakan untuk mentransfer data dan bandwidth yang diperlukan. Masalah lain yang diselesaikan antara pengirim dan penerima adalah pemeriksaan kesalahan harus dinonaktifkan di kedua sisi. Pengecekan error tidak dilakukan pada transfer data secara real-time karena lamanya waktu yang diperlukan untuk meminta pengirim melakukan transmisi ulang seiring dengan lamanya waktu yang diperlukan untuk melakukan transmisi ulang data akan menyebabkan data datang terlambat untuk dikirimkan kepada viewer secara real-time. Karakteristik utama dari transfer data real-time adalah: Data harus dikirimkan secara real-time (sebagaimana atau hampir segera setelah data dihasilkan). Meminta pengirim untuk mengirimkan ulang beberapa byte data yang salah akan mengurangi ketepatan waktu pengiriman secara real-time.

4.4 KONEKSI KOMPUTER TERMINAL KE MAINFRAME

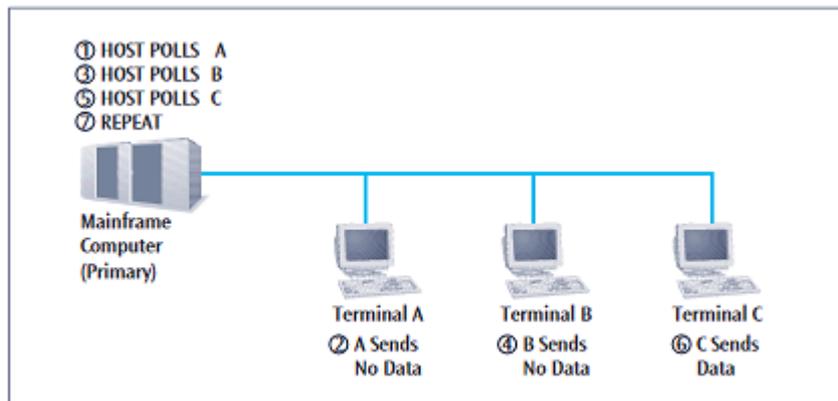
Salah satu jenis koneksi yang didasarkan pada koneksi sinkron dan asinkron adalah koneksi komputer terminal-ke-mainframe. Tata letak terminal-ke-mainframe diperkenalkan pada Bab Satu sebagai salah satu konfigurasi jaringan asli yang masih digunakan. Karena terminal (atau stasiun kerja komputer mikro yang bertindak sebagai terminal) memiliki kekuatan pemrosesan yang kecil dibandingkan dengan stasiun kerja komputer mikro, komputer mainframe harus mengambil kendali dan melakukan semua operasi transfer data. Seperti yang Anda bayangkan, operasi yang dilakukan oleh komputer mainframe bergantung pada jenis koneksi fisik yang ada antara terminal dan mainframe. Koneksi langsung antara terminal dan komputer mainframe, seperti yang ditunjukkan pada Gambar 4-5(a), adalah koneksi point-to-point. Sebuah kabel tunggal berjalan di antara kedua perangkat, dan tidak ada terminal atau komputer lain yang berbagi koneksi ini. Ketika beberapa terminal berbagi satu koneksi langsung ke mainframe, seperti yang ditunjukkan pada Gambar 4-5(b), koneksi tersebut disebut multipoint. Koneksi multipoint adalah kabel tunggal dengan mainframe terhubung di satu ujung dan beberapa terminal terhubung di ujung lainnya.



Gambar 4-5 Koneksi terminal dan komputer mainframe point-to-point dan multipoint

Sekali lagi, jika beberapa perangkat ingin berbagi satu saluran, sesuatu yang khusus harus dilakukan agar lebih dari satu perangkat tidak mencoba melakukan transmisi pada saat yang bersamaan. Sebuah teknik yang disebut polling, yang memungkinkan hanya satu terminal untuk melakukan transmisi pada satu waktu, berhasil mengendalikan beberapa terminal yang berbagi koneksi ke komputer mainframe. (Saat Anda terus membaca, Anda harus menyadari bahwa konsep polling tidak hanya terjadi pada terminal dan mainframe. Kita telah melihat di bab ini bahwa USB melakukan polling, dan kita akan meninjau kembali konsep ini di Bab Lima ketika kita membahas multiplexing.) Polling berasal dari tahun-tahun awal komputasi ketika

terminal merupakan perangkat yang relatif bodoh, tidak mampu melakukan banyak operasi selain entri dan tampilan data. Selama periode ini, komputer mainframe disebut komputer primer, dan setiap terminal disebut komputer sekunder. Dalam teknik polling, terminal, atau terminal sekunder, akan mengirimkan data hanya jika diminta. Roll-call polling adalah metode polling dimana komputer mainframe (primer) melakukan polling pada setiap terminal (sekunder), satu per satu, dengan cara round-robin. Jika terminal A, B, dan C berbagi satu sambungan, seperti pada Gambar 4-6, sambungan primer akan dimulai dengan melakukan polling pada terminal A. Jika A mempunyai data untuk dikirim ke host, maka terminal tersebut akan melakukan hal yang sama. Ketika A selesai melakukan transmisi, terminal utama akan melakukan polling pada terminal B. Jika B tidak punya apa-apa untuk dikirim, B akan menginformasikannya pada terminal primer, dan terminal primer akan melakukan polling pada terminal C. Ketika terminal C selesai, terminal primer akan kembali ke terminal A dan melanjutkan transmisi. proses pemungutan suara.



Gambar 4-6 Terminal A, B, dan C sedang disurvei oleh primer

Perhatikan bahwa hanya satu perangkat yang berbicara pada satu waktu—atau lebih tepatnya, hanya satu sisi sambungan yang berbicara pada satu waktu. Hal ini benar meskipun kabel mampu mentransmisikan data dua arah. Ini adalah contoh lain dari koneksi setengah dupleks.

Alternatif untuk jajak pendapat adalah jajak pendapat hub. Sebuah lembaga primer yang melakukan pemungutan suara hub hanya melakukan pemungutan suara pada terminal pertama, yang kemudian meneruskan pemungutan suara tersebut ke terminal kedua, dan setiap terminal berturut-turut meneruskan pemungutan suara tersebut. Misalnya, setelah disurvei oleh primer, terminal A, ketika selesai merespons, meneruskan polling ke terminal B. Ketika terminal B selesai melakukan transmisi, terminal meneruskan polling ke terminal C. Dalam skenario ini, primer tidak memerlukan untuk melakukan polling pada setiap terminal secara terpisah. Proses pengiriman polling utama ke terminal dan menunggu tanggapan membutuhkan waktu. Ketika sejumlah besar data dikirimkan, waktu ini mungkin menjadi signifikan.

Ketika primer ingin mengirim data ke terminal, ia menggunakan proses yang disebut seleksi. Dalam pemilihan, primer membuat paket data dengan alamat terminal yang dituju

dan mengirimkan paket tersebut. Hanya terminal tertentu yang mengenali alamat tersebut dan menerima data yang masuk. Primer juga dapat menggunakan seleksi untuk menyiarkan data ke semua terminal.

Jika kesederhanaan kontrol adalah tujuan utama Anda, koneksi terminal point-to-point jelas lebih unggul daripada koneksi multipoint. Dengan koneksi point-to-point, polling tidak diperlukan karena hanya ada satu terminal per jalur. Dalam koneksi multipoint, terminal harus memiliki perangkat lunak yang diperlukan untuk mendukung polling. Kerugian lain dari koneksi multipoint di mana beberapa terminal berbagi satu koneksi adalah setiap terminal harus menunggu sementara terminal lain melakukan transmisi. Di sisi lain, meskipun koneksi point-to-point membuat penggunaan waktu transmisi lebih efisien, koneksi tersebut juga memerlukan perangkat keras yang lebih mahal—artinya, lebih banyak kabel diperlukan ketika setiap terminal memiliki koneksi langsung ke terminal primer.

4.5 MELAKUKAN KONEKSI KOMPUTER

Komputer laptop yang dipesan perusahaan Anda baru saja tiba. Meskipun cukup mudah hanya dengan membuka bagian atas komputer dan menyalakannya, Anda akan melihat bahwa terdapat cukup banyak konektor di keempat sisi unit. Faktanya, Anda melihat bahwa ada tidak kurang dari 12 tempat di mana sesuatu dapat dicolokkan ke komputer baru Anda. Mari kita lihat koneksi ini dan lihat kegunaannya.

Sambungan pertama adalah yang paling mudah: Di sinilah kabel listrik dicolokkan. Semua barang elektronik konsumen beroperasi dengan daya DC (arus searah). Untuk menjaga laptop tetap kecil, perangkat keras (“bata”) yang mengubah AC (arus bolak-balik) dari stopkontak di dinding menjadi DC biasanya terdapat di kabel listrik, dan bukan di komputer laptop. Kabel daya jelas membuat baterai tetap terisi dan unit tetap berjalan saat tidak menggunakan daya baterai.

Tiga konektor berikutnya cukup sederhana: Mereka adalah konektor USB. Anda mengenalinya sebagai Tipe A dan mengetahui bahwa Anda mungkin akan menggunakan konektor ini lebih dari apa pun. Dua konektor berikutnya berukuran kecil dan relatif persegi: Ini adalah konektor RJ-11 dan RJ-45. Konektor RJ-11 digunakan untuk menyambungkan laptop ke saluran telepon melalui modem bawaan, dan konektor RJ-45 digunakan untuk menyambungkan laptop ke jaringan area lokal Ethernet melalui antarmuka jaringan Ethernet bawaan kartu. Konektor yang cukup kecil, hampir berbentuk persegi dengan cetakan 1394 di sebelahnya adalah konektor FireWire. Dua konektor bulat kecil digunakan untuk menyambungkan mikrofon dan satu set headphone atau speaker eksternal.

Selanjutnya kita melihat slot persegi panjang yang cukup besar di sisi unit. Konektor ini digunakan untuk mencolokkan PC Card/SmartCard. Kartu PC, yang sebelumnya disebut Kartu PCMCIA, adalah standar antarmuka lama yang memungkinkan perangkat seperti kartu memori, modem, kartu jaringan, dan hard disk ditambahkan ke komputer laptop. Meskipun Kartu PC telah digantikan oleh antarmuka USB, kartu ini memiliki keuntungan karena dapat digeser ke dalam laptop, sehingga sebagian besar tidak terlihat dan tidak mengganggu. Konektor SmartCard memungkinkan pengguna menyambungkan SmartCard dengan konektor

logam (ada juga SmartCard yang tidak menggunakan konektor tetapi menggunakan sinyal nirkabel untuk berkomunikasi dengan perangkat lain). SmartCard berukuran sebesar kartu kredit dan memiliki kemampuan pemrosesan yang tertanam. Mereka sering digunakan untuk memberikan keamanan pada laptop.

Di sebelah slot Kartu PC terdapat konektor persegi panjang kecil seukuran konektor USB, namun dengan huruf D di atasnya. Ini adalah konektor DisplayPort. Konektor ini mirip dengan DVI dan HDMI yang digunakan pada televisi dan perangkat video lainnya, dan memungkinkan Anda menyambungkan laptop ke perangkat audio/video. Konektor lain yang cukup tipis dan berbentuk persegi panjang (sedikit lebih lebar dari konektor DisplayPort) adalah pembaca Kartu Media 7-in-1. Konektor ini memungkinkan Anda menyambungkan kartu media seperti SD, SDHC, xD, xD Tipe H, MMC, MS, dan MS-PRO. Jenis kartu media ini sering ditemukan pada kamera digital dan kamera video digital dan digunakan untuk menyimpan gambar dan video. Jadi, jika Anda ingin menyalin foto digital dari kamera ke komputer, Anda dapat menggunakan slot ini.

Terakhir, ada konektor berbentuk persegi panjang dengan 15 lubang kecil. Ini adalah konektor monitor eksternal, yang dapat digunakan untuk menyambungkan laptop Anda ke perangkat video lain seperti proyektor overhead. Sekarang Anda seharusnya memiliki pemahaman dasar tentang berbagai jenis konektor dan koneksi yang tersedia pada komputer laptop/notebook pada umumnya. Meskipun kami tidak memeriksa setiap jenis koneksi secara rinci, Anda harus memahami bahwa banyak jenis koneksi berbeda yang mungkin dilakukan, dan setiap koneksi memiliki banyak kemungkinan lapisan standar antarmuka. Jelasnya, konektor USB (atau salah satu konektornya) belum menggantikan semua bentuk antarmuka lainnya.

RINGKASAN

- Koneksi antara komputer dan perangkat periferan sering disebut antarmuka, dan proses penyediaan semua interkoneksi yang tepat antara komputer dan perangkat periferan disebut antarmuka.
- Standar antarmuka memiliki dua karakteristik dasar: Standar tersebut dibuat dan disetujui oleh organisasi pembuat standar yang dapat diterima, dan dapat terdiri dari satu hingga empat komponen: kelistrikan, mekanik, fungsional, dan prosedural.
- DTE adalah perangkat pengakhiran data seperti komputer, dan DCE adalah perangkat pemutus sirkuit data seperti modem.
- Selama bertahun-tahun, sejumlah standar antarmuka telah dikembangkan. Dua yang layak untuk dipelajari lebih lanjut adalah EIA-232F dan USB. EIA-232F adalah salah satu standar paling awal, sedangkan USB saat ini merupakan standar antarmuka paling populer. Kedua standar tersebut memberikan spesifikasi mekanik, listrik, fungsional, dan prosedural.
- Sistem transmisi half-duplex dapat mengirimkan data dalam dua arah, namun hanya dalam satu arah pada satu waktu. Sistem full-duplex dapat mengirimkan data dua arah secara bersamaan.

- Standar antarmuka periferal lain yang memberikan daya, fleksibilitas, kecepatan lebih tinggi, dan kemudahan pemasangan mencakup FireWire, Thunderbolt, SCSI, iSCSI, InfiniBand, dan Fibre Channel.
- Menghubungkan perangkat ke komputer dianggap sebagai aktivitas lapisan fisik dan, dengan demikian, terutama berada pada lapisan fisik. Namun koneksi data link juga diperlukan ketika data ditransmisikan antara dua titik di jaringan. Tiga koneksi data link yang umum adalah koneksi asinkron, koneksi sinkron, dan koneksi isokron.
- Koneksi asinkron menggunakan frame karakter tunggal serta bit awal dan akhir untuk menetapkan titik awal dan akhir frame.
- Koneksi sinkron menggunakan bingkai multi-karakter, terkadang terdiri dari ribuan karakter. Sinyal jam sinkronisasi atau semacam pencatatan jam kerja sendiri harus digunakan dengan transmisi sinkron agar penerima tetap tersinkronisasi selama frame besar ini.
- Koneksi isochronous menyediakan koneksi real-time antara komputer dan periferal, dan memerlukan dialog yang cukup rumit untuk mendukung koneksi tersebut.
- Koneksi antara terminal komputer dan komputer mainframe yang didedikasikan untuk satu terminal disebut koneksi point-to-point. Koneksi bersama antara lebih dari satu terminal komputer dan komputer mainframe disebut koneksi multipoint. Komputer mainframe menggunakan teknik polling seperti roll-call polling dan hub polling untuk mendukung koneksi multipoint.

PERTANYAAN

1. Apa itu DTE dan DCE?
2. Apa saja empat komponen antarmuka?
3. Apa kelebihan USB dibandingkan EIA-232F dan jenis standar antarmuka lainnya?
4. FireWire dan USB merupakan standar untuk interkoneksi apa dengan apa?
5. Apa kelebihan Thunderbolt?
6. Kapan seseorang dapat menggunakan SCSI untuk menghubungkan perangkat?
7. Apa perbedaan antara SCSI dan iSCSI?
8. Apakah InfiniBand dan Fibre Channel mungkin digunakan pada komputer di rumah Anda?
9. Apa perbedaan utama antara koneksi asinkron, sinkron, dan isokron?
10. Dalam koneksi asinkron, bit tambahan apa yang ditambahkan ke karakter untuk mempersiapkannya ditransfer?
11. Dalam koneksi asynchronous, berapa banyak karakter yang ditempatkan dalam satu frame?
12. Apa kelebihan dan kekurangan komunikasi asinkron?
13. Apa diagram blok dasar dari bingkai sinkron?
14. Apa kelebihan dan kekurangan komunikasi sinkron?
15. Apa perbedaan antara komunikasi half-duplex dan full-duplex?
16. Apa perbedaan antara koneksi point-to-point dan koneksi multipoint?

17. Bagaimana komputer mainframe meminta terminal untuk mengirimkan data?

LATIHAN TAMBAHAN

1. Jika ada, apa kelebihan antarmuka EIA 232F lama dibandingkan antarmuka USB baru?
2. Apa keunggulan utama antarmuka Thunderbolt dibandingkan antarmuka Universal Serial Bus?
3. Jika saya memiliki perangkat yang memiliki Universal Serial Bus
 1. Antarmuka 3.0, tetapi komputer saya hanya memiliki konektor Universal Serial Bus 2.0, apakah perangkat saya dapat berfungsi? Jelaskan mengapa atau mengapa tidak.
 4. Buatlah tabel yang membandingkan kelebihan dan kekurangan Universal Serial Bus dengan antarmuka EIA-232F.
 5. Tunjukkan urutan bit awal, data, dan penghentian yang dihasilkan selama transmisi asinkron dari string karakter LUNCH.
 6. Sebutkan dua contoh yang tidak disebutkan dalam buku untuk masing-masing koneksi berikut: half-duplex dan full-duplex.
 7. Terminal A, B, dan C dihubungkan ke komputer mainframe. Hanya terminal C yang memiliki data untuk dikirim. Tampilkan urutan pesan yang dikirim antara mainframe dan tiga terminal menggunakan polling roll-call.
 8. Dengan menggunakan skenario yang sama seperti pada soal sebelumnya, tunjukkan urutan pesan yang dipertukarkan menggunakan hub polling.
 9. Misalkan Anda ingin mengirim 1000 karakter data 7-bit. Berapa total bit yang akan Anda transmisikan menggunakan transmisi asinkron? Berapa total bit yang akan Anda transmisikan menggunakan transmisi sinkron? Asumsikan bahwa 1000 karakter akan muat dalam satu frame transmisi sinkron.
 10. Sebutkan dua fitur koneksi asinkron yang memungkinkan penerima tetap sinkron dengan aliran data masuk.
 11. Bagaimana cara penerima dalam koneksi sinkron tetap sinkron dengan aliran data masuk?
 12. Jenis perangkat apa yang paling baik dilayani dengan koneksi isochronous?
 13. Dalam situasi seperti apa jajak pendapat di pusat (hub polling) lebih disukai daripada jajak pendapat yang dilakukan secara absensi?
 14. Sebuah perusahaan memiliki komputer yang sangat kuat, dan perusahaan ingin menghubungkan komputer tersebut ke sejumlah besar perangkat penyimpanan disk berkecepatan tinggi. Protokol manakah yang diperkenalkan pada bab ini yang dapat menyediakan antarmuka yang baik untuk skenario ini?

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Anda sedang merancang aplikasi di tempat kerja yang mengirimkan catatan data ke gedung lain dalam kota yang sama. Catatan data panjangnya 500 byte, dan aplikasi Anda akan mengirimkan satu catatan setiap 0,5 detik. Apakah lebih efisien menggunakan koneksi sinkron atau koneksi asinkron? Berapa kecepatan saluran

transmisi yang diperlukan untuk mendukung kedua jenis sambungan tersebut? Tunjukkan semua pekerjaan Anda.

2. Anda menggunakan sistem komputer yang memiliki 20 terminal yang terhubung ke komputer mainframe menggunakan roll-call polling. Setiap terminal disurvei satu kali dalam satu detik oleh mainframe dan mengirimkan catatan 200-byte setiap 10 detik. Bos mengatakan Anda harus melepas terminal, memasang stasiun kerja komputer, dan mengganti polling dengan koneksi asinkron. Mana yang lebih efisien: menjaga terminal dan polling, atau menggunakan stasiun kerja dan koneksi asinkron?
3. Bagaimana koneksi isokron dibandingkan dengan koneksi asinkron dan sinkron? Bandingkan aplikasi dan efisiensi ketiganya.
4. Sebuah produsen komputer ingin menyederhanakan produknya dengan memproduksi komputer dengan satu konektor Universal Serial Bus dan tidak ada konektor lain. Apakah ini ide yang bagus? Apakah itu mungkin? Menjelaskan.
5. Melanjutkan soal dari bab sebelumnya (lihat pertanyaan nomor 5 di Bab Tiga bagian “Berpikir di Luar Kotak”), Anda memiliki komputer di lantai utama rumah Anda dan komputer lain di kamar tidur di lantai dua. Anda ingin menghubungkan kedua komputer sehingga keduanya berbagi koneksi Internet berkecepatan tinggi dan printer berkualitas tinggi. Jenis media apa yang akan Anda gunakan untuk menghubungkan kedua komputer ini satu sama lain dan ke printer serta perangkat akses Internet, dan jenis antarmuka/konektor apa yang akan digunakan masing-masing komputer?
1. Salah satu standar antarmuka lama disebut X.21. Bagaimana cara membandingkannya dengan USB? Sinyal apa selain T, C, R, dan I yang digunakan dalam standar antarmuka X.21?
2. Protokol asinkron, seperti yang pertama kali muncul, menjelaskan opsi untuk 1, 1,5, atau 2 bit stop. Mengapa ada orang yang membutuhkan atau ingin menggunakan 1,5 atau 2 stop bit?
3. Buat daftar produk berbeda yang menggunakan antarmuka Universal Serial Bus. Produk apa saja yang lebih “kreatif”?
4. Apa status terkini standar FireWire? Apakah itu akan menyerah pada standar USB? Jelaskan tanggapan Anda.
5. Apakah menurut Anda standar Thunderbolt akan bersaing dengan baik dengan standar USB, atau menurut Anda standar USB akan berusaha mengejar Thunderbolt?

BAB 5

MEMBUAT KONEKSI EFISIEN MULTIPLEXING DAN KOMPRESI

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Jelaskan multiplexing pembagian frekuensi dan buat daftar aplikasi, kelebihan, dan kekurangannya
- Jelaskan multiplexing pembagian waktu sinkron dan buat daftar aplikasi, kelebihan, dan kekurangannya
- Menguraikan karakteristik dasar multiplexing sistem telepon T-1 dan SONET/SDH
- Jelaskan statistik multiplexing pembagian waktu dan buat daftar aplikasi, kelebihan, dan kekurangannya
- Sebutkan karakteristik utama multiplexing pembagian panjang gelombang serta kelebihan dan kekurangannya
- Jelaskan karakteristik dasar multinada diskrit
- Sebutkan karakteristik utama multiplexing divisi kode serta kelebihan dan kekurangannya
- Terapkan teknik multiplexing pada situasi bisnis pada umumnya
- Jelaskan perbedaan antara kompresi lossy dan lossless
- Jelaskan operasi dasar kompresi run-length, JPEG, dan MP3

BANYAK ORANG SEKARANG MEMILIKI sistem pemutaran musik portabel seperti iPod Apple Computer. iPod berukuran 20 GB ini mampu menyimpan hingga 5000 lagu. Berapa banyak penyimpanan yang diperlukan tahan musik sebanyak ini? Jika kita menganggap bahwa sebuah lagu yang diambil dari compact disc terdiri dari sekitar 32 juta byte (dengan asumsi rata-rata panjang lagu adalah 3 menit, musik tersebut diambil sampelnya 44.100 kali per detik, dan setiap sampel berukuran 16 bit, di saluran kiri dan kanan), maka menyimpan 5000 lagu masing-masing 32 juta byte akan membutuhkan 160 miliar byte. Bagaimana mungkin memasukkan 5.000 lagu (160 miliar byte) ke dalam ruang penyimpanan yang berukuran lebih dari 20 miliar byte? Jawabannya adalah melalui kompresi. Meskipun ada banyak jenis teknik kompresi, tujuan dasar yang mendasarinya sama: untuk memasukkan data sebanyak mungkin ke dalam ruang penyimpanan yang terbatas.

Musik bukan satu-satunya jenis data yang dapat dikompresi. iPod juga dapat memampatkan ucapan, sehingga memungkinkan pengguna untuk merekam pesan dan memo untuk diri mereka sendiri atau untuk kemudian dikirimkan ke orang lain. Demikian pula, video musik, acara televisi, dan film dapat dikompresi, disimpan, dan kemudian diputar ulang menggunakan berbagai versi iPod serta berbagai pemutar musik portabel, pemutar video, dan ponsel pintar lainnya. Jelas, iPod dan semua perangkat sejenisnya tidak akan menjadi seperti sekarang ini tanpa teknik kompresi.

Apakah ada yang hilang saat kita mengompresi data menjadi bentuk yang lebih kecil?

Apakah ada berbagai bentuk kompresi?

Apakah teknik kompresi tertentu berfungsi lebih baik pada jenis aplikasi tertentu?

5.1 PENDAHULUAN

Dalam kondisi yang paling sederhana, suatu media hanya dapat membawa satu sinyal pada suatu saat. Misalnya, kabel twisted pair yang menghubungkan keyboard ke komputer mikro membawa sinyal digital tunggal. Demikian pula, kabel twisted pair Kategori 6 yang menghubungkan komputer mikro ke jaringan area lokal hanya membawa satu sinyal digital pada satu waktu. Namun, sering kali kita menginginkan suatu media membawa banyak sinyal pada saat yang bersamaan. Saat menonton televisi misalnya, kita ingin menerima beberapa saluran televisi jika kita tidak menyukai acara di saluran yang sedang kita tonton. Kami memiliki harapan yang sama terhadap siaran radio. Selain itu, ketika Anda berjalan atau berkendara keliling kota dan melihat banyak orang berbicara melalui telepon seluler, Anda menyaksikan transmisi beberapa sinyal telepon seluler secara bersamaan melalui media nirkabel. Teknik transmisi banyak sinyal melalui satu media adalah multiplexing.

Agar beberapa sinyal dapat berbagi satu media, media tersebut harus “dibagi” untuk memberikan masing-masing sinyal sebagian dari total bandwidth. Saat ini, suatu media dapat dibagi dalam tiga cara dasar: pembagian frekuensi, pembagian waktu, dan pembagian kode transmisi. Terlepas dari jenis pembagian yang dilakukan, multiplexing dapat membuat tautan komunikasi, atau koneksi, menjadi lebih efisien dengan menggabungkan sinyal dari berbagai sumber. Kita akan mengkaji tiga cara suatu media dapat dibagi dengan menjelaskan secara rinci teknik multiplexing yang sesuai dengan masing-masing divisi dan kemudian dilanjutkan dengan diskusi yang membandingkan kelebihan dan kekurangan dari semua teknik tersebut.

Cara lain untuk membuat koneksi antara dua perangkat lebih efisien adalah dengan mengompresi data yang ditransfer melalui koneksi tersebut. Jika file dikompres menjadi setengah ukuran normalnya, dibutuhkan setengah waktu atau setengah bandwidth untuk mentransfer file tersebut. File terkompresi ini juga akan memakan lebih sedikit ruang penyimpanan, yang jelas merupakan keuntungan lainnya. Seperti yang akan kita lihat, sejumlah teknik kompresi saat ini digunakan dalam sistem komunikasi (dan hiburan). Beberapa dari teknik kompresi ini mampu mengembalikan salinan persis dari data asli (lossless), sementara yang lain tidak (lossy). Tapi mari kita mulai dengan multiplexing.

5.2 MULTIPLEXING DIVISI FREKUENSI

Multiplexing pembagian frekuensi adalah teknik multiplexing tertua dan digunakan di banyak bidang komunikasi, termasuk siaran televisi dan radio, televisi kabel, dan telepon seluler. Ini juga merupakan salah satu teknik multiplexing yang paling sederhana. Pengandaan pembagian frekuensi (FDM) adalah penetapan rentang frekuensi yang tidak tumpang tindih untuk setiap “pengguna” suatu media. Pengguna mungkin adalah stasiun televisi yang mentransmisikan saluran televisinya melalui gelombang udara (media) ke rumah-rumah dan bisnis. Seorang pengguna mungkin juga merupakan ponsel yang mengirimkan

sinyal melalui media yang Anda gunakan untuk berbicara. Untuk memungkinkan banyak pengguna berbagi satu media, FDM menetapkan saluran terpisah untuk setiap pengguna. Saluran adalah sekumpulan frekuensi yang digunakan untuk mengirimkan sinyal pengguna. Dalam multiplexing pembagian frekuensi, sinyal ini sering kali bersifat analog.

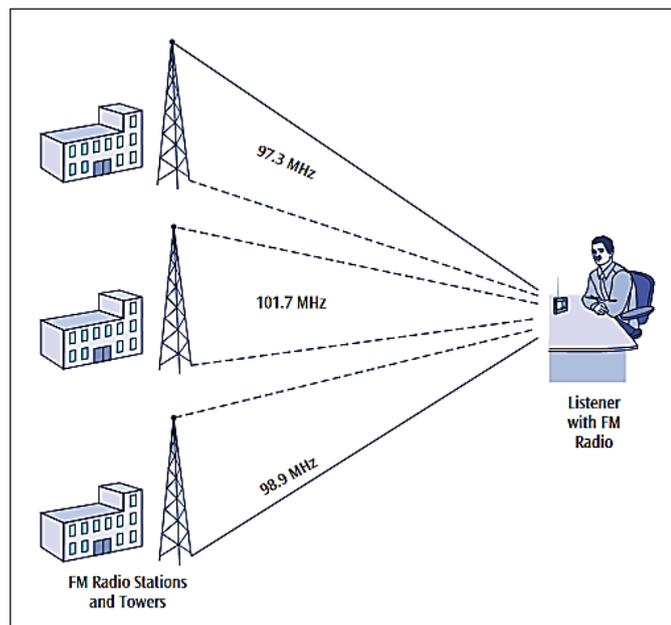
Banyak contoh multiplexing pembagian frekuensi dapat ditemukan dalam bisnis dan kehidupan sehari-hari. Televisi kabel masih merupakan salah satu aplikasi multiplexing pembagian frekuensi yang paling umum ditemukan. Seperti ditunjukkan pada Tabel 5-1, setiap saluran televisi kabel diberi rentang frekuensi unik oleh Federal Communications Commission (FCC), dan penetapan frekuensi ini bersifat tetap, atau statis. Perhatikan dari Tabel 5-1 bahwa frekuensi berbagai saluran tidak tumpang tindih. Pesawat televisi, kotak televisi kabel, atau perekam video digital berisi tuner, atau pemilih saluran. Tuner memisahkan satu saluran dari saluran berikutnya dan menampilkan masing-masing saluran sebagai aliran data individual kepada Anda.

Tabel 5-1 Penetapan frekuensi saluran televisi kabel

	Saluran	Frekuensi dalam MHz
VHF dan Kabel Pita Rendah	2	55–60
	3	61–66
	4	67–72
	5	77–82
	6	83–88
Kabel Pita Menengah	95	91–96
	96	97–102
	97	103–108
	98	109–114
	99	115–120
	14	121–126
	15	127–132
	16	133–138
	17	139–144
	18	145–150
	19	151–156
	20	157–162
	21	163–168
	22	169–174
VHF dan Kabel Pita Tinggi	7	175–180
	8	181–186
	9	187–192
	10	193–198
	11	199–204
	12	205–210
	13	211–216

Contoh umum lainnya dari multiplexing pembagian frekuensi adalah sistem telepon seluler. Sistem ini membagi bandwidth yang tersedia menjadi beberapa saluran. Jadi, sambungan telepon dari satu pengguna diberikan satu set frekuensi untuk transmisi, sedangkan sambungan telepon dari pengguna kedua diberi rangkaian frekuensi kedua. Sebagaimana dijelaskan dalam Bab Tiga, sistem telepon seluler generasi pertama mengalokasikan saluran menggunakan rentang frekuensi dalam spektrum 800 hingga 900 megahertz (MHz). Lebih tepatnya, rentang 824 hingga 849 MHz digunakan untuk menerima sinyal dari telepon seluler (uplink), sedangkan rentang 869 hingga 894 MHz digunakan untuk transmisi ke telepon seluler (downlink). Untuk memungkinkan terjadinya percakapan dua arah, dua saluran ditetapkan untuk setiap sambungan telepon. Sinyal yang masuk ke telepon seluler masuk pada satu pita 30 kHz (pada rentang 869 hingga 894 MHz), sedangkan sinyal yang keluar dari telepon seluler keluar pada pita 30 kHz yang berbeda (pada rentang 824 hingga 849 MHz). rentang -849 MHz). Meskipun ponsel generasi selanjutnya mungkin menggunakan rentang frekuensi yang berbeda, konsep multipleksingnya serupa. Ponsel adalah contoh saluran yang ditetapkan secara dinamis.

Ketika pengguna memasukkan nomor telepon dan menekan tombol Kirim, jaringan seluler menetapkan rentang frekuensi pada koneksi ini berdasarkan ketersediaan jaringan saat ini. Seperti yang mungkin Anda perkirakan, penetapan frekuensi dinamis tidak terlalu boros dibandingkan penetapan frekuensi statis, yang ditemukan pada sistem multipleks komputer terminal-ke-mainframe dan sistem televisi.



Gambar 5-1 Contoh sederhana multiplexing pembagian frekuensi

Secara umum, perangkat yang menerima masukan dari satu atau lebih pengguna disebut multipleksor. Perangkat yang dipasang pada ujung penerima media yang memisahkan setiap sinyal untuk mengirimkannya ke penerima yang sesuai disebut multiplexor kedua, atau demultipleksor. Dalam semua sistem multiplexing pembagian frekuensi, multipleksor

menerima masukan dari pengguna, mengubah aliran data menjadi sinyal analog menggunakan frekuensi tetap atau dinamis, dan mentransmisikan sinyal analog gabungan melalui media yang memiliki bandwidth yang cukup lebar untuk mendukungnya. jangkauan total semua frekuensi yang ditetapkan. Demultiplexor kemudian menerima sinyal analog gabungan, memisahkan satu atau lebih sinyal analog individual, dan mengirimkannya ke pengguna yang sesuai. Gambar 5-1 menunjukkan diagram multiplexing pembagian frekuensi yang disederhanakan. Dalam contoh ini, sejumlah stasiun radio telah menggandakan sinyal radionya ke dalam suatu pita frekuensi. Di sisi penerima, masing-masing radio menggunakan demultiplexor (tuner) untuk memisahkan setiap sinyal radio dari yang lain.

Untuk menjaga agar satu sinyal tidak mengganggu sinyal lainnya, sekumpulan frekuensi yang tidak terpakai yang disebut pita pelindung biasanya disisipkan di antara dua sinyal untuk memberikan suatu bentuk isolasi. Pita penjaga ini mengambil frekuensi yang mungkin digunakan untuk saluran data lain, sehingga menimbulkan tingkat pemborosan tertentu. Dalam upaya memanfaatkan data biner, bentuk lain dari multiplexing— multiplexing pembagian waktu—dikembangkan.

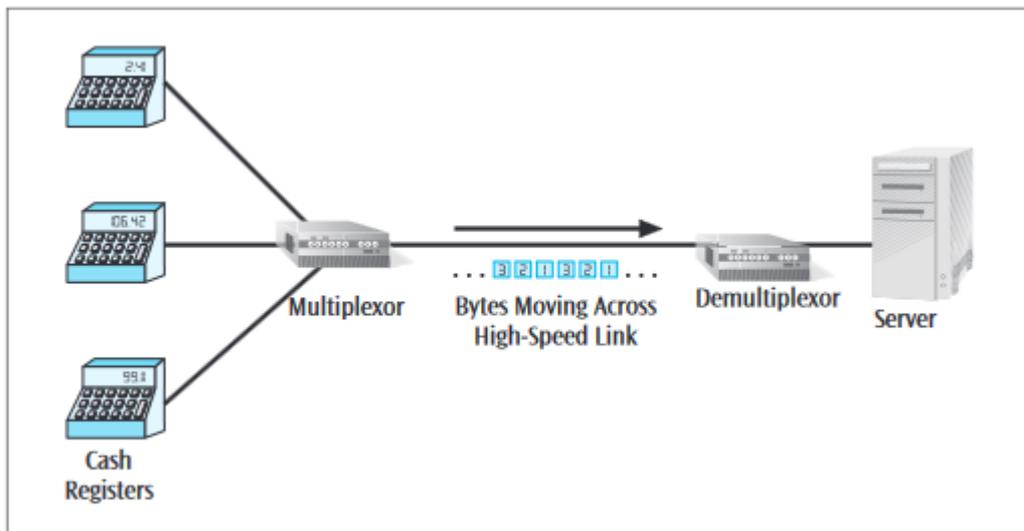
5.3 MULTIPLEXING DIVISI WAKTU

Multiplexing pembagian frekuensi mengambil bandwidth yang tersedia pada suatu media dan membagi frekuensi di antara beberapa saluran, atau pengguna. Pada dasarnya, divisi ini memungkinkan banyak pengguna untuk mengirimkan secara bersamaan. Sebaliknya, time Division multiplexing (TDM) hanya memperbolehkan satu pengguna pada satu waktu untuk melakukan transmisi, dan pembagian media dilakukan dengan membagi waktu transmisi yang tersedia di antara pengguna. Di sini, pengguna menggunakan seluruh bandwidth saluran, namun hanya untuk sesaat.

Bagaimana cara kerja multiplexing pembagian waktu? Misalkan seorang instruktur di kelas mengajukan pertanyaan kontroversial kepada siswa. Sebagai tanggapan, sejumlah tangan terangkat, dan instruktur memanggil setiap siswa, satu per satu. Merupakan tanggung jawab instruktur untuk memastikan bahwa hanya satu siswa yang berbicara pada saat tertentu, sehingga tanggapan setiap individu dapat didengar. Dalam cara yang relatif kasar, instruktur adalah multipleksor pembagian waktu, yang memberikan setiap pengguna (siswa) waktu untuk mengirimkan data (mengungkapkan pendapat kepada seluruh kelas). Dengan cara serupa, multipleksor pembagian waktu memanggil perangkat input satu demi satu, memberikan giliran pada setiap perangkat dalam mentransmisikan datanya melalui saluran berkecepatan tinggi. Misalkan dua pengguna, A dan B, ingin mengirimkan data melalui media bersama ke komputer yang jauh. Kita dapat membuat skema multiplexing pembagian waktu yang cukup sederhana dengan mengizinkan pengguna A untuk melakukan transmisi pada detik pertama, kemudian pengguna B pada detik berikutnya, diikuti lagi oleh pengguna A pada detik ketiga, dan seterusnya. Sejak multiplexing pembagian waktu diperkenalkan (pada tahun 1960an), teknologi ini telah terpecah menjadi dua teknologi yang kira-kira paralel namun terpisah: multiplexing pembagian waktu sinkron dan multiplexing pembagian waktu statistik.

Multiplexing pembagian waktu sinkron

Multiplexing pembagian waktu sinkron (Sync TDM) memberi setiap sinyal sumber yang masuk giliran untuk ditransmisikan, dilanjutkan melalui sumber-sumber dengan cara round-robin. Dengan adanya n masukan, multipleksor pembagian waktu sinkron menerima satu bagian data, misalnya satu byte, dari perangkat pertama, mentransmisikannya melalui tautan berkecepatan tinggi, menerima satu byte dari perangkat kedua, mentransmisikannya melalui tautan berkecepatan tinggi, dan melanjutkan proses ini hingga satu byte diterima dari perangkat ke- n . Setelah byte pertama perangkat ke- n ditransmisikan, multipleksor kembali ke perangkat pertama dan melanjutkan dengan cara round-robin. Sebagai alternatif, daripada menerima byte pada suatu waktu dari setiap sumber, multipleksor dapat menerima bit tunggal sebagai input unit dari setiap perangkat. Gambar 5-2 menunjukkan aliran keluaran yang dihasilkan oleh multipleksor pembagian waktu sinkron.

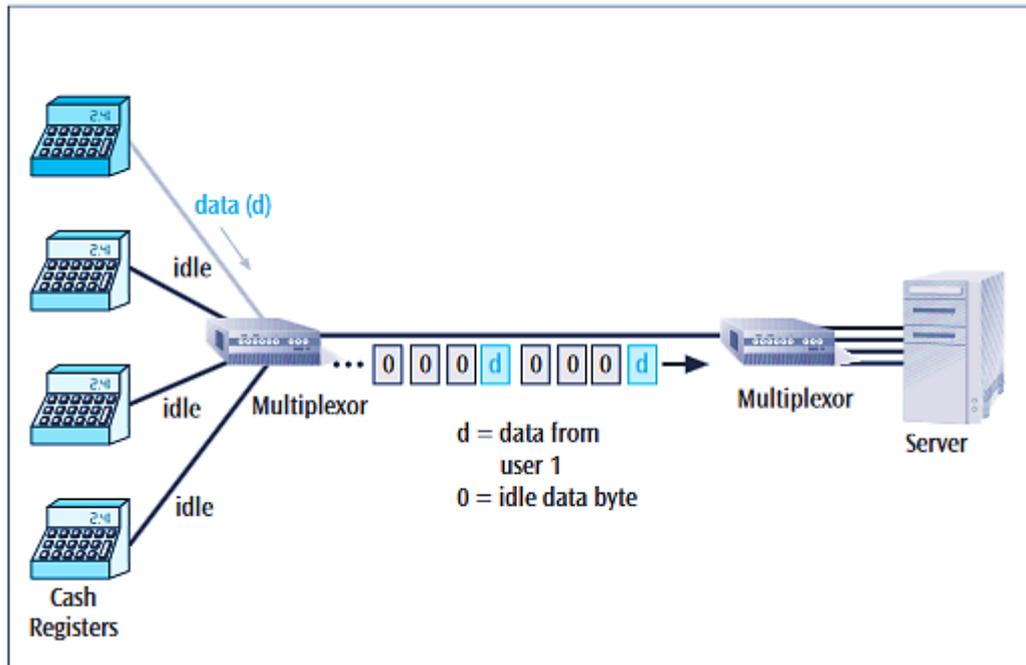


Gambar 5-2 Beberapa mesin kasir dan aliran transaksi multipleksnya

Perhatikan bahwa demultiplexor pada ujung penerima link berkecepatan tinggi harus membongkar aliran byte yang masuk dan mengirimkan setiap byte ke tujuan yang sesuai. Karena aliran data keluaran berkecepatan tinggi yang dihasilkan oleh multipleksor tidak berisi informasi pengalamatan untuk masing-masing byte, urutan yang tepat harus dipertahankan. Hal ini akan memungkinkan demultiplexor untuk membongkar dan mengirimkan byte ke masing-masing pemilik dalam urutan yang sama dengan byte yang dimasukkan.

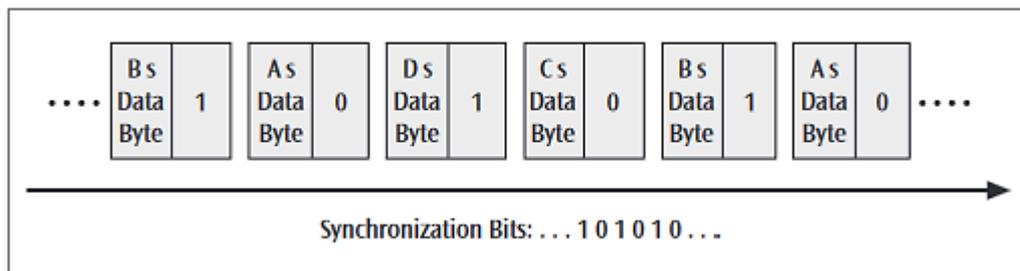
Apa yang terjadi jika perangkat tidak memiliki apa pun untuk dikirimkan? Dalam hal ini, multipleksor masih harus mengalokasikan slot untuk perangkat tersebut dalam aliran output berkecepatan tinggi; namun slot waktu tersebut, pada dasarnya, akan kosong. Karena setiap slot waktu ditetapkan secara statis dalam multiplexing pembagian waktu sinkron, multipleksor tidak dapat memanfaatkan slot yang kosong dan menugaskan kembali perangkat yang sibuk ke dalamnya. Jika, misalnya, hanya satu perangkat yang melakukan transmisi, multipleksor masih harus mengambil sampel dari setiap perangkat input (Gambar 5-3). Selain itu, link berkecepatan tinggi yang menghubungkan kedua multipleksor harus selalu mampu

membawa total semua kemungkinan sinyal masuk, bahkan ketika tidak ada sumber input yang mengirimkan data.



Gambar 5-3 Aliran transmisi multipleksor dengan hanya satu perangkat input yang mentransmisikan data

Seperti halnya koneksi sederhana antara satu perangkat pengirim dan satu perangkat penerima, menjaga sinkronisasi di seluruh tautan multipleks adalah hal yang penting. Untuk menjaga sinkronisasi antara multipleksor pengirim dan demultipleksor penerima, data dari sumber input sering kali dikemas ke dalam bingkai sederhana, dan bit sinkronisasi ditambahkan di suatu tempat di dalam bingkai (Gambar 5-4).



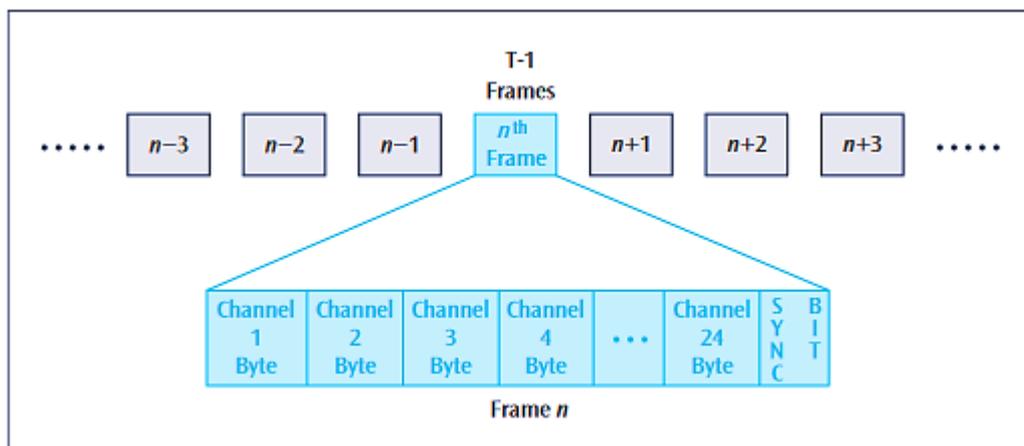
Gambar 5-4 Bingkai yang ditransmisikan dengan bit sinkronisasi tambahan

Tergantung pada teknologi TDM yang digunakan, dari satu bit hingga beberapa bit dapat ditambahkan ke bingkai untuk menyediakan sinkronisasi. Bit sinkronisasi bertindak dengan cara yang mirip dengan sinyal diferensial Manchester yang terus berubah: Bit tersebut menyediakan urutan bit yang muncul kembali secara konstan sehingga dapat diantisipasi oleh penerima dan dapat dikunci.

Dua jenis multiplexing pembagian waktu sinkron yang populer saat ini adalah multiplexing T-1 dan SONET/SDH. Meskipun rincian T-1 dan SONET/SDH bisa sangat teknis, pemeriksaan singkat masing-masing teknologi akan menunjukkan bagaimana teknologi ini menggandakan beberapa saluran informasi menjadi satu aliran data.

T-1 Multiplexing

Pada tahun 1960an, AT&T menciptakan layanan yang dikenal sebagai T-1, yang menggandakan data digital dan mendigitalkan suara ke saluran telepon berkecepatan tinggi dengan kecepatan data 1,544 megabit per detik. Tujuan awal T-1 adalah untuk menyediakan koneksi berkecepatan tinggi antara pusat switching AT&T. Ketika dunia usaha mengetahui layanan berkecepatan tinggi ini, mereka mulai memintanya untuk menghubungkan komputer dan sistem komunikasi suara mereka ke jaringan telepon. Pada tahun 1984, AT&T akhirnya mulai menawarkan layanan ini kepada pelanggan bisnis.



Gambar 5-5 Aliran data multipleks T-1

Dalam multiplexing T-1, frame aliran keluaran multiplexor T-1 dibagi menjadi 24 saluran suara/data digital terpisah yang masing-masing berukuran 64 kbps (Gambar 5-5). Pengguna yang ingin menggunakan seluruh 24 saluran menggunakan T-1 penuh, sementara pengguna lain yang perlu menggunakan hanya sebagian dari 24 saluran dapat meminta T-1 pecahan. Aliran multipleks T-1 adalah pengulangan frame yang terus menerus. Setiap frame terdiri dari 1 byte dari masing-masing 24 saluran (pengguna) ditambah 1 bit sinkronisasi. Dengan demikian, data dari pengguna pertama disusul oleh data dari pengguna kedua, dan seterusnya hingga data dari pengguna ke-24 kembali diikuti oleh data dari pengguna pertama. Jika salah satu dari 24 sumber masukan tidak memiliki data untuk dikirimkan, ruang dalam frame masih dialokasikan untuk sumber masukan tersebut. Data masukan dari maksimal 24 perangkat ditetapkan pada interval tetap. Setiap perangkat hanya dapat melakukan transmisi selama interval tetap tersebut. Jika perangkat tidak memiliki data penting untuk dikirim, slot waktu masih ditetapkan ke perangkat tersebut, dan data seperti kosong atau nol dikirimkan. Sistem T-1 adalah aplikasi klasik multiplexing pembagian waktu sinkron.

Jalur komunikasi T-1 adalah teknologi populer untuk menghubungkan bisnis ke sumber berkecepatan tinggi seperti penyedia layanan Internet dan jaringan area luas lainnya. Karena

multiplexing T-1 adalah contoh klasik multiplexing pembagian waktu sinkron, maka hal ini perlu diperiksa lebih lanjut.

Jalur telekomunikasi T-1 menggunakan teknik multipleksing yang disebut pensinyalan DS-1, yang menyediakan multipleksing hingga 24 saluran terpisah dengan kecepatan total 1,544 Mbps. Bagaimana jalur T-1 mencapai kecepatan transmisi unik 1,544 Mbps? Untuk menjawab pertanyaan ini, mari kita perhatikan contoh di mana saluran T-1 mendukung maksimal 24 saluran suara.

Karena rata-rata suara manusia menempati rentang frekuensi yang relatif sempit (kira-kira 300 hingga 3400 Hz), maka digitalisasi suara cukup mudah. Faktanya, konverter analog-ke-digital hanya memerlukan 128 tingkat kuantisasi berbeda untuk mencapai representasi digital yang adil dari suara manusia. Karena 128 sama dengan 2^7 , setiap sampel suara yang dimodulasi kode pulsa dapat masuk ke dalam nilai 7-bit. Dua ratus lima puluh enam tingkat kuantisasi akan memungkinkan representasi suara manusia yang lebih tepat. Karena $256 \frac{1}{8}$ 28, dan 8 bit sama dengan 1 byte, sistem telepon menggunakan 256 tingkat kuantisasi untuk mendigitalkan suara manusia. (Jika Anda memerlukan penyegaran pada materi ini, lihat kembali modulasi kode pulsa di Bab Dua.)

Ingatlah bahwa untuk membuat representasi digital yang akurat dari sinyal analog, Anda perlu mengambil sampel sinyal analog dengan kecepatan dua kali frekuensi tertinggi. Mengingat perusahaan telepon menetapkan saluran 4000 Hz untuk membawa sinyal suara, Anda perlu mengambil sampel sinyal suara analog 8000 kali per detik saat mendigitalkan suara. Ingat juga, dari Gambar 5-5, urutan frame T-1. Karena setiap frame T-1 berisi 1 byte data suara untuk 24 saluran berbeda, sistem memerlukan 8000 frame per detik untuk mempertahankan 24 saluran suara secara bersamaan.

Karena setiap frame memiliki panjang 193 bit ($24 \text{ saluran} \times 8 \text{ bit per saluran} + 1 \text{ bit kontrol} \frac{1}{8} 193 \text{ bit}$), 8000 frame per detik dikalikan dengan 193 bit per frame, sehingga menghasilkan kecepatan 1,544 Mbps.

T-1 dapat digunakan untuk mentransfer data dan juga suara. Jika data sedang dikirim, byte 8-bit untuk setiap saluran dipecah menjadi 7 bit data dan 1 bit informasi kontrol. Tujuh bit data per frame \times 8000 frame per detik $\frac{1}{8}$ 56.000 bit per detik per saluran. Jadi, bila digunakan untuk data, masing-masing dari 24 saluran T-1 mampu mendukung koneksi 56 kbps.

Multipleksing SONET/SDH

Synchronous Optical Network (SONET) dan Synchronous Digital Hierarchy (SDH) adalah standar yang kuat untuk multiplexing aliran data melalui satu media. SONET (dikembangkan di Amerika Serikat oleh ANSI) dan SDH (dikembangkan di Eropa oleh ITU-T) adalah dua standar yang hampir identik untuk transmisi bandwidth tinggi dari berbagai tipe data melalui kabel serat optik. SONET dan SDH memiliki dua fitur yang menarik dalam konteks multiplexing. Pertama, keduanya merupakan teknik multiplexing sinkron. Sebuah jam tunggal mengontrol waktu semua transmisi dan peralatan di seluruh jaringan SONET (atau SDH). Hanya dengan menggunakan satu jam ke waktu, seluruh transmisi data menghasilkan tingkat sinkronisasi yang lebih tinggi karena sistem tidak harus menangani dua jam atau lebih yang

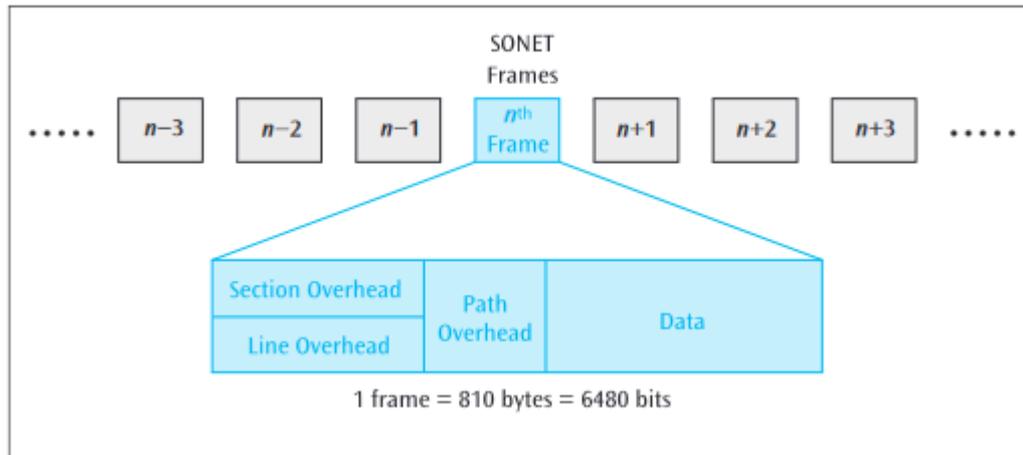
mempunyai waktu yang sedikit berbeda. Sinkronisasi tingkat tinggi ini diperlukan untuk mencapai tingkat presisi tinggi yang diperlukan saat data dikirim dengan kecepatan ratusan dan ribuan megabit per detik.

Kedua, SONET dan SDH mampu melipatgandakan aliran data dengan kecepatan berbeda-beda ke dalam satu koneksi fiber. SONET mendefinisikan hierarki level pensinyalan, atau kecepatan transmisi data, yang disebut sinyal transport sinkron (STS). Setiap level STS mendukung kecepatan data tertentu, seperti ditunjukkan pada Tabel 5-2, dan didukung oleh spesifikasi fisik yang disebut pembawa optik (OC). Perhatikan bahwa kecepatan data OC-3 tepat tiga kali lipat kecepatan OC-1; hubungan ini terbawa ke seluruh tabel nilai. SONET dirancang dengan mempertimbangkan hubungan kecepatan data ini sehingga proses multiplexing sinyal relatif mudah. Misalnya, relatif mudah untuk menggandakan tiga sinyal STS-1 menjadi satu sinyal STS-3. Demikian pula, empat sinyal STS-12 dapat dimultipleks menjadi satu sinyal STS-48. Multiplexor STS dalam jaringan SONET dapat menerima sinyal listrik dari media berbasis tembaga, mengubah sinyal listrik tersebut menjadi pulsa cahaya, dan kemudian menggandakan berbagai sumber menjadi satu aliran berkecepatan tinggi.

Tabel 5-2 Level sinyal STS, level OC yang sesuai, dan kecepatan data

Tingkat STS	Spesifikasi OC	Kecepatan Data (dalam Mbps)
STS-1	OK-1	51.84
STS-3	OK-3	155.52
STS-9	OK-9	466.56
STS-12	OK-12	622.08
STS-18	OK-18	933.12
STS-24	OK-24	1244.16
STS-36	OK-36	1866.24
STS-48	OK-48	2488.32
STS-96	OK-96	4976.64
STS-192	OK-192	9953.28

Setiap frame SONET berisi data yang sedang dikirim ditambah sejumlah bit kontrol, yang tersebar di seluruh frame. Gambar 5-6 menunjukkan tata letak frame untuk level sinyal STS-1. Level pensinyalan STS-1 mendukung 8000 frame per detik, dan setiap frame berisi 810 byte (6480 bit). Mengalikan 8000 frame per detik dengan 6480 bit per frame menghasilkan 51.840.000 bit per detik, yang merupakan kecepatan data OC-1. Level pensinyalan STS lainnya serupa kecuali untuk tata letak data dan penempatan serta kuantitas bit kontrol.

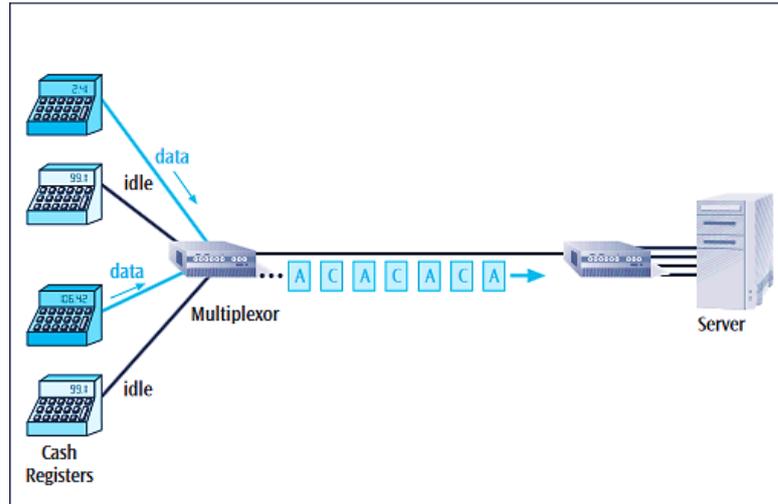


Gambar 5-6 Tata letak bingkai SONET STS-1

SONET dan SDH digunakan dalam berbagai aplikasi yang memerlukan kecepatan transfer data yang sangat tinggi melalui jalur serat optik. Misalnya, dua pengguna umum SONET adalah perusahaan telepon dan perusahaan yang menyediakan layanan tulang punggung Internet. Baik perusahaan telepon maupun penyedia tulang punggung Internet memiliki jalur transmisi berkecepatan sangat tinggi yang menjangkau sebagian wilayah negara dan harus mengirimkan ratusan dan ribuan juta bit per detik dalam jarak jauh. Memasang jalur serat optik yang mendukung teknologi transmisi SONET adalah salah satu cara terbaik untuk memenuhi tuntutan aplikasi yang menantang tersebut.

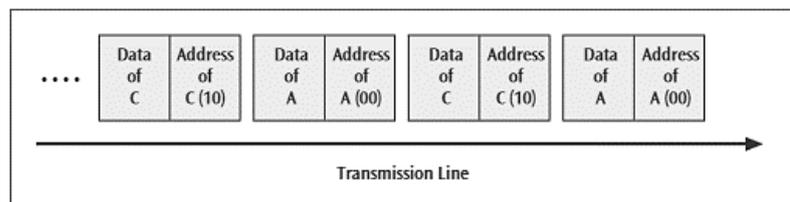
Multiplexing pembagian waktu statistik

Seperti yang telah Anda lihat dalam diskusi sebelumnya, multiplexing pembagian frekuensi dan multiplexing pembagian waktu sinkron dapat membuang-buang ruang transmisi yang tidak terpakai. Salah satu solusi untuk masalah ini adalah multiplexing pembagian waktu statistik. Kadang-kadang disebut multiplexing pembagian waktu asinkron, multiplexing pembagian waktu statistik (Stat TDM) mentransmisikan data hanya dari pengguna aktif dan tidak mengirimkan slot waktu kosong. Untuk mengirimkan data hanya dari pengguna aktif, multipleksor membuat bingkai yang lebih kompleks yang berisi data hanya dari sumber masukan yang memiliki sesuatu untuk dikirim. Misalnya, pertimbangkan skenario sederhana berikut. Jika empat stasiun, A, B, C, dan D, terhubung ke multipleksor statistik, namun hanya stasiun A dan C yang sedang melakukan transmisi, multipleksor statistik hanya mentransmisikan data dari stasiun A dan C, seperti ditunjukkan pada Gambar 5-7. Perhatikan bahwa setiap saat, jumlah stasiun yang melakukan transmisi dapat berubah dari dua menjadi nol, satu, tiga, atau empat. Jika hal ini terjadi, multipleksor statistik harus membuat frame baru yang berisi data dari stasiun transmisi saat ini.



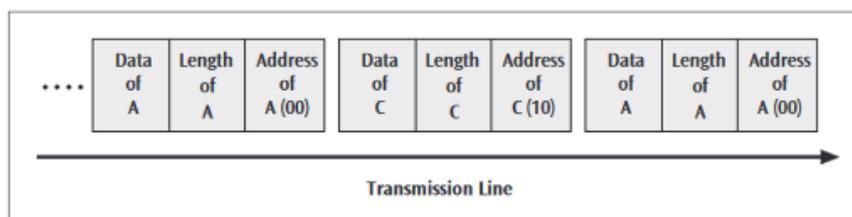
Gambar 5-7 Dua dari empat stasiun memancarkan melalui multipleksor statistik

Karena hanya dua dari empat stasiun yang melakukan transmisi, bagaimana demultiplexor di sisi penerima mengenali penerima data yang benar? Beberapa jenis alamat harus disertakan dengan setiap byte data untuk mengidentifikasi siapa yang mengirim data dan untuk siapa data tersebut dituju (Gambar 5-8). Alamatnya bisa sesederhana angka biner yang secara unik mengidentifikasi stasiun yang melakukan transmisi. Misalnya, jika multipleksor dihubungkan ke empat stasiun, maka alamatnya bisa berupa 0, 1, 2, dan 3 untuk stasiun A, B, C, dan D. Dalam biner, nilainya masing-masing adalah 00, 01, 10, dan 11.



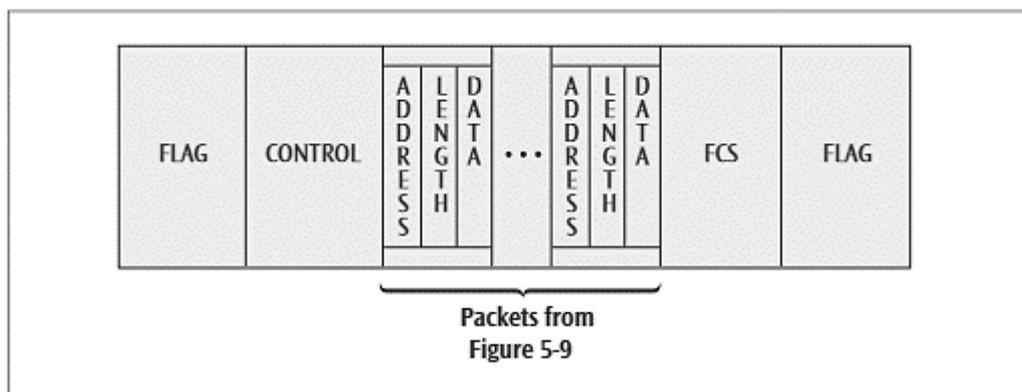
Gambar 5-8 Contoh alamat dan data dalam aliran keluaran multipleksor statistik

Jika multipleksor mengirimkan lebih dari satu byte data pada satu waktu dari masing-masing sumber, maka diperlukan bentuk alamat dan data alternatif. Untuk mengirimkan potongan data dengan ukuran variabel, bidang panjang yang menentukan panjang blok data disertakan bersama dengan alamat dan data. Paket alamat/panjang/data/alamat/panjang/data ini ditunjukkan pada Gambar 5-9.



Gambar 5-9 Paket alamat, panjang, dan bidang data dalam aliran keluaran multipleksor statistik

Terakhir, urutan alamat/panjang/data/alamat/panjang/data... dikemas ke dalam unit yang lebih besar oleh multiplexor statistik. Unit yang lebih besar ini, ditunjukkan pada Gambar 5-10, merupakan contoh yang lebih realistis dibandingkan Gambar 5-9 dan tampak seperti frame yang ditransmisikan menggunakan sambungan sinkron. Bendera di awal dan akhir membatasi awal dan akhir bingkai. Bidang kontrol menyediakan informasi yang digunakan oleh multiplexor pengirim dan penerima untuk mengontrol aliran data di antara keduanya. Terakhir, frame check sequence (FCS) memberikan informasi yang dapat digunakan oleh multiplexor penerima untuk mendeteksi kesalahan transmisi dalam frame.



Gambar 5-10 Tata letak bingkai untuk paket informasi yang ditransfer antar multiplexor statistik

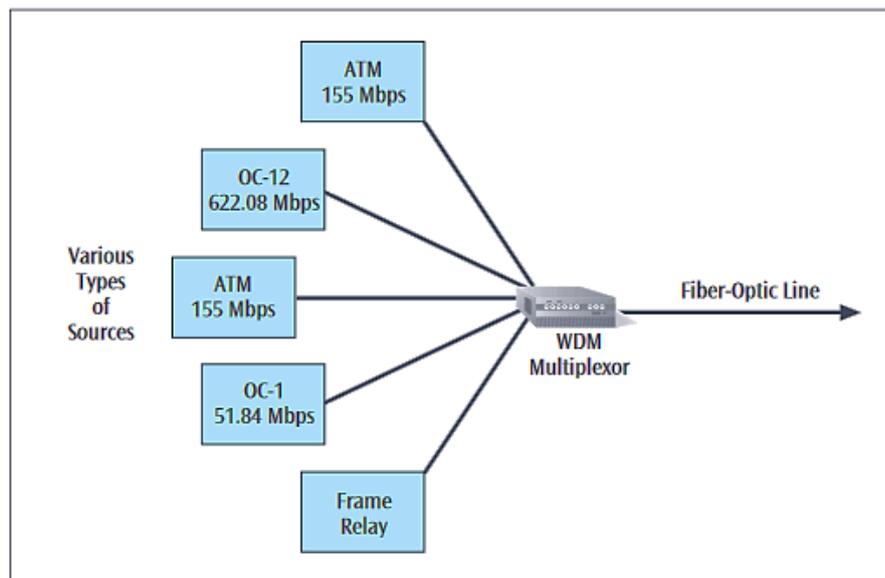
5.4 MULTIPLEXING DIVISI PANJANG GELOMBANG

Meskipun pembagian frekuensi dan pembagian waktu adalah dua teknik multiplexing yang sangat umum, teknik multiplexing lainnya—multiplexing pembagian panjang gelombang—muncul beberapa tahun yang lalu dan sejak itu menjadi alternatif yang ampuh. Ketika sistem transmisi yang menggunakan kabel serat optik pertama kali dipasang (pada tahun 1980an), ledakan pertumbuhan Internet dan jaringan transmisi data lainnya bahkan tidak terbayangkan. Kini, setelah abad kedua puluh satu dimulai, sangat jelas terlihat bahwa perkiraan awal pertumbuhan terlalu jauh di bawah perkiraan. Dengan pertumbuhan akses Internet lebih dari 100 persen per tahun dan individu meminta beberapa saluran telepon untuk digunakan dengan faks dan modem, transmisi video, dan telekonferensi, satu saluran serat optik (sepasang untuk operasi dupleks penuh) mentransmisikan miliaran informasi. bit per detik tidak lagi mencukupi. Ketidakmampuan satu jalur serat optik untuk memenuhi kebutuhan pengguna disebut fiber exhaust. Selama bertahun-tahun, pakar teknologi hanya melihat sedikit cara untuk mengatasi knalpot fiber selain dengan memasang jalur fiber tambahan, yang terkadang membutuhkan biaya besar. Sekarang tampaknya ada solusi menarik yang memanfaatkan jalur serat optik yang saat ini terpasang: multiplexing pembagian panjang gelombang.

Wavelength Division Multiplexing (WDM) menggandakan beberapa aliran data ke dalam satu jalur serat optik. Pada dasarnya, ini adalah teknik multiplexing pembagian frekuensi yang menetapkan sumber input ke kumpulan frekuensi terpisah. Multiplexing

pembagian gelombang menggunakan laser dengan panjang gelombang (frekuensi) berbeda untuk mentransmisikan banyak sinyal secara bersamaan melalui satu media. Panjang gelombang setiap laser dengan warna berbeda disebut lambda. Jadi, WDM mendukung banyak lambda.

Teknik ini memberikan laser berwarna unik ke setiap sumber masukan dan menggabungkan beberapa sinyal optik dari sumber masukan sehingga sinyal tersebut dapat diperkuat sebagai satu kelompok dan diangkut melalui satu serat. Menarik untuk dicatat bahwa, karena sifat sinyal dan serat kaca, ditambah sifat cahaya itu sendiri, setiap sinyal yang dibawa pada serat dapat ditransmisikan dengan kecepatan berbeda dari sinyal lainnya. Artinya, satu jalur serat optik dapat mendukung kecepatan transmisi simultan seperti 51,84 Mbps, 155,52 Mbps, 622,08 Mbps, dan 2,488 Gbps (yang kebetulan merupakan kelipatan kecepatan T-1 dan didefinisikan sebagai OC-1, OC-3, OC-12, dan OC-48, spesifikasi pembawa optik untuk jalur serat optik berkecepatan tinggi). Selain itu, satu jalur serat optik dapat mendukung sejumlah format transmisi berbeda seperti SONET, Asynchronous Transfer Mode (ATM), dan lainnya, dalam berbagai kombinasi (lihat Gambar 5-11).



Gambar 5-11 Jalur serat optik menggunakan multiplexing pembagian panjang gelombang dan mendukung transmisi multi-kecepatan

Multiplexing pembagian panjang gelombang juga dapat diskalakan. Seiring dengan meningkatnya permintaan terhadap sistem dan penerapannya, panjang gelombang tambahan, atau lambda, dapat ditambahkan pada serat, sehingga semakin melipatgandakan kapasitas keseluruhan sistem serat optik asli. Meskipun sebagian besar sistem mendukung kurang dari 100 lambda, beberapa sistem dengan harga sangat tinggi dapat menangani lebih dari 100 lambda. Ketika WDM dapat mendukung lambda dalam jumlah besar, hal ini sering disebut dengan multiplexing pembagian panjang gelombang padat (DWDM). Namun, kekuatan tambahan ini bukannya tanpa label harga. Multiplexing pembagian panjang gelombang padat adalah cara yang mahal untuk mengirimkan sinyal dari beberapa perangkat

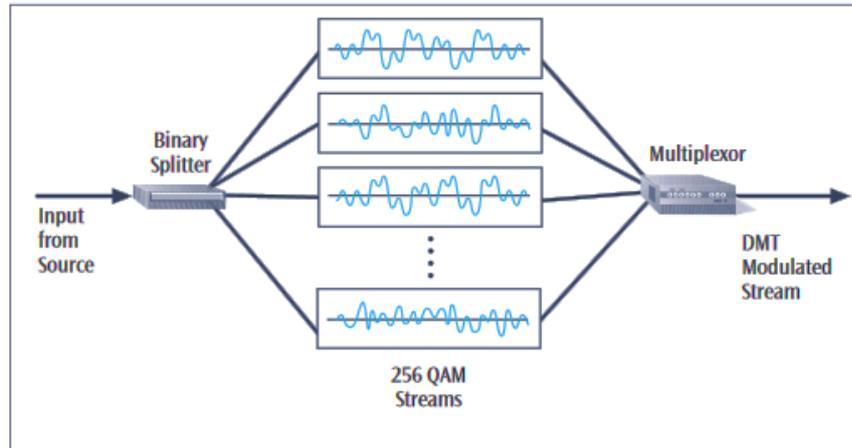
karena tingginya jumlah laser dengan warna berbeda yang diperlukan dalam satu unit. Salah satu variasi yang lebih murah pada multiplexing pembagian panjang gelombang padat adalah multiplexing pembagian panjang gelombang kasar. Multiplexing pembagian panjang gelombang kasar (CWDM) adalah teknologi yang lebih murah karena dirancang untuk koneksi jarak pendek dan hanya memiliki beberapa lambda, dengan jarak antar lambda yang lebih besar. Karena jarak panjang gelombangnya lebih jauh dan tidak berdekatan seperti pada DWDM, laser yang digunakan untuk multiplexing pembagian panjang gelombang kasar bisa lebih murah dan tidak memerlukan pendinginan yang ekstensif. Terlepas dari biaya dan kompleksitasnya, banyak pakar teknologi memperkirakan bahwa multiplexing divisi panjang gelombang akan tetap menjadi teknologi yang kuat.

Meskipun multiplexing pembagian panjang gelombang adalah teknologi canggih yang relatif mahal dan tidak umum, jenis multiplexing berikutnya yang akan kita periksa—multinada diskrit—tidak kalah mengesankannya. Selain cukup umum dan murah, multitone diskrit adalah teknologi di balik sistem saluran pelanggan digital (DSL) yang populer.

5.5 MULTITON DISKRIT

Discrete multitone (DMT) adalah teknik multiplexing yang umum ditemukan dalam sistem DSL. DSL, seperti yang telah kita lihat, adalah teknologi yang memungkinkan sinyal data berkecepatan tinggi melintasi saluran telepon standar berbasis tembaga. Kita juga telah melihat bahwa kecepatan transmisi tertinggi yang dapat kita capai dengan saluran telepon dial-up standar adalah 56 kbps. DSL, bagaimanapun, mampu mencapai kecepatan hingga jutaan bit per detik. Bagaimana ini mungkin? Jawabannya adalah teknik multiplexing DMT. DMT pada dasarnya menggabungkan ratusan sinyal atau subsaluran berbeda ke dalam satu aliran; tidak seperti teknik multiplexing yang telah dibahas sebelumnya, DMT dirancang sedemikian rupa sehingga semua subsaluran ini diperuntukkan bagi satu pengguna.

Kekuatan sebenarnya dari DMT adalah kenyataan bahwa masing-masing subsaluran dapat melakukan modulasi amplitudo kuadratur (QAM) sendiri. (Ingat dari Bab Dua bahwa contoh umum QAM adalah yang melibatkan kode 4-bit di mana delapan sudut fasa memiliki amplitudo tunggal, dan empat sudut fasa memiliki amplitudo ganda.) Misalnya, salah satu bentuk DMT mendukung 256 subsaluran, masing-masing mampu melakukan aliran termodulasi QAM 60-kbps (Gambar 5-12). Jadi, 256 60 kbps menghasilkan sistem 15,36 juta bps. Sayangnya, karena adanya noise, tidak semua 256 sub-saluran dapat mentransmisikan dengan kecepatan penuh 60 kbps. Sub-saluran yang mengalami noise akan mengubah teknik modulasinya dan turun kembali ke kecepatan yang lebih lambat. Oleh karena itu, sistem DSL yang mengirimkan data dalam ratusan ribu bit per detik lebih merupakan hal yang biasa.



Gambar 5-12 256 aliran termodulasi amplitudo kuadratur digabungkan menjadi satu sinyal DMT untuk layanan DSL

DMT adalah teknologi menarik yang dikembangkan dalam upaya meningkatkan kecepatan transmisi data bagi konsumen rata-rata. Bayangkan sebuah teknologi yang dapat mendukung 256 aliran yang dimodulasi secara independen, banyak di antaranya yang mentransmisikan dengan kecepatan berbeda! Mari kita alihkan perhatian kita ke teknik multiplexing lain yang juga meningkatkan kemampuan teknologi yang sudah ada: multiplexing pembagian kode.

5.6 MULTIPLEXING DIVISI KODE

Juga dikenal sebagai akses ganda pembagian kode, multiplexing pembagian kode (CDM) adalah teknologi yang relatif baru yang telah digunakan secara luas oleh militer dan perusahaan telepon seluler. Sedangkan teknik multiplexing lainnya membedakan satu pengguna dari yang lain dengan menetapkan rentang frekuensi atau menyisipkan urutan bit dalam waktu, multiplexing pembagian kode memungkinkan banyak pengguna untuk berbagi kumpulan frekuensi yang sama dengan menetapkan kode digital unik untuk setiap pengguna.

Lebih tepatnya, multiplexing pembagian kode didasarkan pada kelas teknik modulasi yang dikenal sebagai teknologi spektrum tersebar. Teknologi spektrum tersebar akan dibahas lebih rinci di Bab Sebelas, namun secara singkat, ini adalah teknik yang digunakan dalam industri komunikasi untuk memodulasi sinyal menjadi sinyal baru yang lebih aman sehingga lebih tahan terhadap penyadapan. Teknologi ini terbagi dalam dua kategori: frekuensi hopping dan direct sequence. Multiplexing pembagian kode menggunakan teknologi spektrum penyebaran urutan langsung, suatu teknik yang menyebarkan transmisi sinyal pada rentang frekuensi yang luas, menggunakan nilai matematika. Saat data asli dimasukkan ke dalam modulator urutan langsung, setiap biner 1 dan 0 diganti dengan urutan bit yang lebih besar dan unik. Misalnya, setiap perangkat di pasar telepon seluler yang menggunakan multiplexing pembagian kode untuk mengirimkan sinyalnya diberi urutan bitnya sendiri. Ketika urutan bit tiba di stasiun tujuan, multiplexor divisi kode mampu memberitahu urutan bit satu perangkat seluler dari perangkat seluler lainnya. Dalam sistem telepon seluler yang sebenarnya, multiplexing pembagian kode hanya digunakan selama transmisi dari kantor telepon seluler

ke telepon seluler, bukan selama transmisi dari telepon seluler ke kantor telepon seluler. Hal ini disebabkan oleh masalah sinkronisasi yang melekat pada multiplexing pembagian kode. Meskipun demikian, untuk menyederhanakan contoh ini, kita akan berpura-pura bahwa telepon seluler melakukan transmisi ke kantor telepon seluler menggunakan multiplexing pembagian kode.

Terlepas dari kenyataan bahwa ini adalah prosedur yang cukup rumit, multiplexing pembagian kode adalah salah satu teknologi yang lebih menarik dalam komunikasi data, dan ini memerlukan pemeriksaan lebih dekat. Mari kita buat contoh menggunakan tiga pengguna ponsel: A, B, dan C. (Untuk membantu pemahaman teknologi ini, contoh ini menyederhanakan konsep yang lebih teknis.) Misalkan pengguna ponsel A telah diberi kode biner 11110000; pengguna ponsel B, kode 10101010; dan pengguna ponsel C, kode 00110011. Kode biner ini disebut kode penyebaran chip. Di dunia nyata, kode-kode ini panjangnya 64 bit. Untuk menyederhanakan contoh kita, kita akan menggunakan kode 8-bit. Jika pengguna seluler A ingin mengirimkan biner 1, ia mengirimkan kodenya: 11110000. Jika pengguna seluler A ingin mengirimkan biner 0, ia mengirimkan kebalikan dari kodenya: 00001111. Sebenarnya, pengguna seluler mengirimkan serangkaian bilangan positif dan tegangan negatif: tegangan positif untuk 1 dan tegangan negatif untuk 0. Sekarang, misalnya, katakanlah pengguna seluler A mentransmisikan biner 1, pengguna seluler B mentransmisikan biner 0, dan pengguna seluler C mentransmisikan biner 1 Berikut ini yang sebenarnya ditularkan:

Pengguna seluler A mengirimkan biner 1 (11110000), atau p p p p - - - -
 Pengguna seluler B mengirimkan biner 0 (01010101), atau - p - p - p - p
 Pengguna seluler C mengirimkan biner 1 (00110011), atau - - p p - - p p

Penerima menerima ketiga sinyal secara bersamaan dan menambahkan tegangan seperti yang ditunjukkan di bawah ini:

	+	+	+	+	-	-	-	-
	-	+	-	+	-	+	-	+
	-	-	+	+	-	-	+	+
Sums:	-1	+1	+1	+3	-3	-1	-1	+1

Kemudian, untuk menentukan apa yang ditransmisikan oleh setiap pengguna ponsel, penerima mengalikan jumlah tersebut dengan kode asli dari setiap pengguna ponsel, dinyatakan sebagai dan - nilai, dan kemudian mengambil jumlah dari produk tersebut:

Sums:		-1	+1	+1	+3	-3	-1	-1	+1
Mobile user A's code:		+1	+1	+1	+1	-1	-1	-1	-1
Products:		-1	+1	+1	+3	+3	+1	+1	-1
Sum of Products:					+8				

Karena Jumlah Produk lebih besar atau sama dengan 8 (≥ 8) dalam contoh 8-bit ini, nilai yang dikirimkan harus berupa biner 1. Di dunia nyata, dengan sistem 64-bit, Jumlah Produk akan

harus lebih besar atau sama dengan 64 (≥ 64). Jika Jumlah Produk adalah ≤ -8 (atau ≤ -64 menggunakan kode nyata), nilai yang dikirimkan akan menjadi biner 0.

Prosedur yang sama akan dilakukan untuk menentukan nilai yang dikirimkan pengguna seluler B:

Sums:	-1	+1	+1	+3	-3	-1	-1	+1
Mobile user B's code:	+1	-1	+1	-1	+1	-1	+1	-1
Products:	-1	-1	+1	-3	-3	+1	-1	-1
Sum of Products:	-8							

Karena Jumlah Produknya adalah ≤ -8 , nilai yang dikirimkan harus berupa biner 0.

Sekarang kita telah memeriksa cara kerja berbagai teknik multiplexing, mari kita bandingkan kelebihan dan kekurangannya.

5.7 PERBANDINGAN TEKNIK MULTIPLEXING

Multiplexing pembagian frekuensi mempunyai dua kelemahan utama. Kerugian pertama ditemukan pada sistem yang menggandakan banyak saluran melalui satu media. Karena frekuensi biasanya ditetapkan secara statis, perangkat yang tidak memiliki apa pun untuk ditransmisikan masih diberi frekuensi, sehingga bandwidth terbuang sia-sia.

Kerugian kedua dari multiplexing pembagian frekuensi adalah karena teknik ini menggunakan sinyal analog, dan sinyal analog lebih rentan terhadap gangguan noise dibandingkan sinyal digital. Meskipun demikian, banyak jenis aplikasi yang berbeda (seperti televisi dan radio) menggunakan multiplexing pembagian frekuensi karena kesederhanaannya, dan teknik ini mungkin akan bertahan lama.

Multiplexing pembagian waktu sinkron juga relatif mudah; tetapi seperti pada multiplexing pembagian frekuensi, perangkat input yang tidak memiliki apa pun untuk ditransmisikan dapat membuang-buang ruang transmisi. Keuntungan besar TDM sinkron dibandingkan multiplexing pembagian frekuensi adalah kebisingan yang lebih rendah karena penggunaan sinyal digital selama transmisi. Meskipun T-1 menggunakan TDM sinkron, dan T-1 tidak akan hilang dalam semalam, TDM sinkron digantikan dengan sistem seperti Ethernet, seperti yang akan kita lihat di bab selanjutnya. TDM Statistik adalah salah satu variasi TDM yang mengirimkan data hanya dari perangkat input yang memiliki data untuk dikirim. Dengan demikian, TDM statistik membuang lebih sedikit bandwidth pada link transmisi.

Multiplexor statistik mempunyai keunggulan lain yang sangat baik dibandingkan multiplexor pembagian waktu sinkron. Meskipun kedua jenis multiplexing pembagian waktu dapat mengirimkan data melalui link berkecepatan tinggi, multiplexing pembagian waktu statistik tidak memerlukan saluran berkecepatan tinggi seperti multiplexing pembagian waktu sinkron. Multiplexing pembagian waktu statistik mengasumsikan bahwa semua perangkat tidak melakukan transmisi pada waktu yang sama; oleh karena itu, tidak memerlukan link berkecepatan tinggi yang merupakan total semua aliran data yang masuk. Konsekuensi lain dari asumsi ini adalah bahwa kapasitas jalur keluaran yang berasal dari multiplexor statistik

bisa lebih kecil daripada kapasitas jalur keluaran dari multipleksor sinkron, yang juga memungkinkan adanya hubungan berkecepatan lebih lambat antar multipleksor. Tautan berkecepatan lebih lambat ini biasanya berarti biaya yang lebih rendah.

Salah satu kelemahan multipleksor statistik adalah peningkatan tingkat kompleksitasnya. TDM Sinkron hanya menerima data dari setiap perangkat yang terpasang dan mengirimkan data tersebut dalam siklus tanpa akhir. Multipleksor statistik harus mengumpulkan dan menyangga data dari perangkat terpasang aktif dan, setelah membuat bingkai dengan informasi kontrol yang diperlukan, mengirimkan bingkai tersebut ke multipleksor penerima. Meskipun tingkat kerumitan yang sedikit lebih tinggi ini berarti biaya awal yang lebih tinggi, biaya tersebut biasanya diimbangi oleh kemampuan statistik TDM untuk menggunakan jalur interkoneksi berkapasitas lebih kecil.

Multiplexing pembagian waktu statistik adalah pilihan yang baik untuk menghubungkan sejumlah perangkat berkecepatan rendah yang tidak mengirimkan data secara terus menerus ke sistem komputer jarak jauh. Contoh sistem ini mencakup sistem entri data, sistem tempat penjualan, dan banyak aplikasi komersial lainnya di mana pengguna memasukkan data di terminal komputer.

Multiplexing pembagian panjang gelombang adalah teknik yang baik untuk mentransmisikan beberapa sinyal secara bersamaan melalui jalur serat optik. Multiplexing pembagian panjang gelombang juga dapat diskalakan. Seiring dengan meningkatnya permintaan terhadap sistem dan penerapannya, lebih banyak panjang gelombang, atau lambda, dapat ditambahkan ke serat, sehingga semakin melipatgandakan kapasitas keseluruhan sistem serat optik asli. Sistem multiplexing pembagian panjang gelombang yang menggunakan lambda dalam jumlah besar disebut multiplexing pembagian panjang gelombang padat, sedangkan sistem yang hanya menggunakan sedikit lambda disebut multiplexing pembagian panjang gelombang kasar. Meskipun multiplexing pembagian panjang gelombang bisa menjadi alternatif yang mahal, hal ini mungkin lebih murah dibandingkan mencoba memasang jalur serat optik tambahan.

Teknologi multinada diskrit adalah bentuk multiplexing unik di mana semua subsaluran yang dimultiplekskan ditujukan untuk satu pengguna. Dengan demikian, multinada diskrit tidak secara langsung dibandingkan dengan teknik multipleksing lainnya, di mana setiap subsaluran atau saluran diperuntukkan bagi pengguna yang berbeda. Namun, multinada diskrit adalah teknologi yang kompleks dan dapat mengalami gangguan akibat terlalu banyak noise.

Yang terakhir, multiplexing pembagian kode, meskipun menggunakan bandwidth frekuensi yang cukup lebar dan teknologi yang kompleks, dapat diskalakan seperti WDM dan dapat menghasilkan kapasitas sistem 8 hingga 10 kali lipat dari sistem multiplexing pembagian frekuensi. Keuntungan dan kerugian masing-masing teknik multiplexing dirangkum dalam Tabel 5-3.

Tabel 5-3 Keuntungan dan kerugian teknik multiplexing

Teknik Multipleksing	Keuntungan	Kekurangan
Multipleksing Pembagian Frekuensi	Sederhana. Populer dengan radio, TV, TV kabel. Semua receiver, seperti telepon seluler, tidak perlu berada di lokasi yang sama.	Masalah kebisingan karena sinyal analog Membuang bandwidth. Dibatasi oleh rentang frekuensi
Multipleksing Pembagian Waktu Sinkron	Sinyal digital. Relatif sederhana. Biasa digunakan dengan T-1, SONET.	Membuang bandwidth
Multipleksing Pembagian Waktu Statistik	Penggunaan bandwidth yang lebih efisien. Bingkai dapat berisi informasi kontrol dan kesalahan. Paket dapat memiliki ukuran yang bervariasi	Lebih kompleks daripada multiplexing pembagian waktu sinkron
Multipleksing Pembagian Panjang Gelombang	Kapasitas yang sangat tinggi melalui fiber, Sinyal dapat memiliki kecepatan yang bervariasi dan Dapat Diskalakan	Biaya, Kompleksitas
Multinada Diskrit	Mampu mencapai kecepatan transmisi tinggi	Kompleksitas, masalah kebisingan
Multiplexing Divisi Kode	Kapasitas besar Dapat diskalakan	Kompleksitas

Sejauh ini, dengan multiplexing, kita telah meneliti bagaimana beberapa aliran data dapat digabungkan secara beragam untuk memaksimalkan jumlah aliran data yang dapat ditransmisikan melalui berbagai jenis media, sehingga menghasilkan koneksi yang lebih efisien. Sekarang mari kita periksa teknik lain yang dapat memaksimalkan jumlah data yang dapat dikirim pada suatu waktu atau disimpan dalam ruang tertentu—yaitu, prosesnya dikenal sebagai kompresi.

5.8 KOMPRESI

Seperti yang telah kita lihat, kompresi adalah proses mengambil data dan mengemas lebih banyak data ke dalam ruang yang sama, baik dalam bentuk perangkat penyimpanan seperti hard drive atau iPod, atau media seperti jalur serat optik. Ketika data dikompresi untuk transmisi, data ditransfer lebih cepat karena jumlahnya lebih sedikit, dan ini dapat menghasilkan koneksi yang lebih efisien. Sejalan dengan itu, dalam hal kapasitas penyimpanan, kompresi juga memungkinkan lebih banyak data disimpan dalam jumlah memori atau ruang disk yang sama. Cara dasar untuk melakukan kompresi adalah dengan mencari beberapa pola umum pada data dan mengganti setiap pola data dengan simbol atau simbol yang akan memakan lebih sedikit ruang selama transmisi atau penyimpanan. Misalnya, jika dokumen berisi banyak kemunculan kata “salju”, pengirim mungkin ingin mengganti kata “salju” dengan simbol seperti tanda persen, %. Setelah data dikirimkan, penerima kemudian mengganti simbol % dengan kata aslinya, “salju”. Penggantian ini segera menimbulkan dua pertanyaan: Bagaimana penerima mengetahui cara mengganti simbol % dengan kata “salju”? Apa yang terjadi jika tanda persen (%) sebenarnya muncul di dokumen sebagai tanda persen?

Kita tentu tidak ingin penerima mengganti tanda persen yang valid dengan kata “salju”. Saat kita melihat contoh nyata kompresi, Anda akan melihat bagaimana pertanyaan-pertanyaan ini, dan pertanyaan-pertanyaan serupa lainnya, dijawab.

Namun, sebelum kita membahas beberapa teknik kompresi sebenarnya, kita harus membagi proses kompresi menjadi dua kategori. Jika suatu teknik kompresi memampatkan data kemudian mendekompresinya kembali menjadi data asli, maka disebut sebagai teknik lossless. Dengan teknik kompresi lossless, tidak ada data yang hilang akibat kompresi. Jika suatu teknik kompresi kehilangan sebagian data akibat proses kompresi, maka disebut sebagai teknik kompresi lossy. Ambil contoh sebuah bank yang ingin mengompresi semua rekening nasabahnya untuk menambah ruang penyimpanan data sistem komputernya. Mengingat bencana yang akan terjadi jika rekening nasabah kehilangan data karena kompresi, bank jelas ingin menggunakan teknik kompresi lossless untuk melakukan tugas ini. Di sisi lain, misalkan Anda ingin menyalin lagu dari compact disc ke iPod. Untuk melakukan ini, Anda perlu mengompres lagunya terlebih dahulu. Selama proses kompresi, jika beberapa data hilang, Anda mungkin tidak menyadarinya, terutama jika algoritme kompresi dirancang untuk dengan sengaja “menghilangkan” hanya suara-suara yang kemungkinan besar tidak dapat dideteksi oleh sebagian besar telinga manusia. Karena rentang data audio dan video tertentu tidak dapat dideteksi dengan mudah, algoritma kompresi lossy sering digunakan untuk mengompresi file musik dan video, dan dengan demikian biasanya dimasukkan ke dalam perangkat teknologi seperti pemutar musik digital portabel. Untuk menyelidiki proses kompresi secara lebih rinci, mari kita mulai dengan mempelajari teknik lossless.

Kompresi tanpa rugi

Mengganti setiap pola data dengan simbol atau simbol yang akan memakan lebih sedikit ruang selama transmisi atau penyimpanan. Misalnya, jika dokumen berisi banyak kemunculan kata “salju”, pengirim mungkin ingin mengganti kata “salju” dengan simbol seperti tanda persen, %. Setelah data dikirimkan, penerima kemudian mengganti simbol % dengan kata aslinya, “salju”. Penggantian ini segera menimbulkan dua pertanyaan: Bagaimana penerima mengetahui cara mengganti simbol % dengan kata “salju”? Apa yang terjadi jika tanda persen (%) sebenarnya muncul di dokumen sebagai tanda persen?

Kita tentu tidak ingin penerima mengganti tanda persen yang valid dengan kata “salju”. Saat kita melihat contoh nyata kompresi, Anda akan melihat bagaimana pertanyaan-pertanyaan ini, dan pertanyaan-pertanyaan serupa lainnya, dijawab.

Namun, sebelum kita membahas beberapa teknik kompresi sebenarnya, kita harus membagi proses kompresi menjadi dua kategori. Jika suatu teknik kompresi memampatkan data kemudian mendekompresinya kembali menjadi data asli, maka disebut sebagai teknik lossless. Dengan teknik kompresi lossless, tidak ada data yang hilang akibat kompresi. Jika suatu teknik kompresi kehilangan sebagian data akibat proses kompresi, maka disebut sebagai teknik kompresi lossy. Ambil contoh sebuah bank yang ingin mengompresi semua rekening nasabahnya untuk menambah ruang penyimpanan data sistem komputernya. Mengingat bencana yang akan terjadi jika rekening nasabah kehilangan data karena kompresi, bank jelas ingin menggunakan teknik kompresi lossless untuk melakukan tugas ini. Di sisi lain, misalkan

Anda ingin menyalin lagu dari compact disc ke iPod. Untuk melakukan ini, Anda perlu mengompres lagunya terlebih dahulu. Selama proses kompresi, jika beberapa data hilang, Anda mungkin tidak menyadarinya, terutama jika algoritme kompresi dirancang untuk dengan sengaja “menghilangkan” hanya suara-suara yang kemungkinan besar tidak dapat dideteksi oleh sebagian besar telinga manusia. Karena rentang data audio dan video tertentu tidak dapat dideteksi dengan mudah, algoritma kompresi lossy sering digunakan untuk mengompresi file musik dan video, dan dengan demikian biasanya dimasukkan ke dalam perangkat teknologi seperti pemutar musik digital portabel. Untuk menyelidiki proses kompresi secara lebih rinci, mari kita mulai dengan mempelajari teknik lossless.

Salah satu contoh kompresi lossless yang lebih umum dan sederhana adalah pengkodean run-length. Teknik ini menggantikan pengulangan bit atau byte yang sama yang terjadi dalam urutan data dengan satu kemunculan bit/byte dan jumlah proses, atau hanya dengan jumlah proses. Misalnya, teknik ini bekerja pada tingkat biner dengan menghitung string panjang (atau proses) dari biner 0 atau string panjang biner 1. Mari kita perhatikan string data berikut, yang sebagian besar terdiri dari biner 0:

00000100000000011000000000000000100001100000000000000000000000001000000

Teknik kompresi berdasarkan pengkodean run-length akan memampatkan angka 0 dengan terlebih dahulu menghitung “proses” dari 0—artinya, teknik ini akan dimulai dengan menghitung angka 0 hingga ditemukan biner 1. Jika tidak ada angka 0 di antara pasangan angka 1, maka pasangan tersebut akan dianggap sebagai proses yang berisi nol angka 0. Melakukan ini pada string data kami, kami menemukan proses berikut:

5	9	0	15	4	0	20	6
---	---	---	----	---	---	----	---

Jadi, pada putaran pertama, kami menemukan lima angka 0, sedangkan putaran kedua menghasilkan sembilan angka 0. Putaran ketiga tidak mempunyai angka 0 karena angka 1 segera diikuti dengan angka 1. Pada putaran berikutnya, kita menemukan lima belas angka 0, diikuti dengan putaran empat angka 0, nol angka 0, dua puluh angka 0, dan terakhir enam angka 0.

Langkah selanjutnya dalam teknik kompresi ini adalah mengubah setiap nilai desimal (5, 9, 0, 15, dan seterusnya) menjadi nilai biner 4-bit, atau camilan. Satu-satunya aturan unik yang harus diikuti selama konversi ini berlaku ketika Anda menemukan nilai desimal 15 atau lebih besar. Karena bilangan desimal terbesar yang dapat diwakili oleh nibble biner 4-bit adalah 15 (yang setara dengan empat biner 1—1111), Anda harus mengonversi proses yang memiliki nilai desimal lebih besar dari 15 menjadi beberapa camilan 4-bit. Misalnya, jumlah 20 akan dikonversi menjadi 1111 0101, dengan nibble pertama bernilai 15, dan nibble kedua

bernilai 5. Peringatan pada aturan ini adalah jika Anda mengonversi nilai 15 itu sendiri, maka Anda juga akan membuat dua nibble: 1111 diikuti oleh 0000. Alasannya adalah agar tetap konsisten—sehingga setiap kali nibble biner 1111 (atau 15) ditemukan, nibble berikutnya (0000, yang sesuai dengan a nilai desimal 0) ditambahkan ke camilan itu.

Jadi, mengkonversi proses 5, 9, 0, 15, 4, 0, 20, dan 6 di atas akan menghasilkan camilan berikut:

0101	1001	0000	1111	0000	0100	0000	1111	0101	0110
------	------	------	------	------	------	------	------	------	------

Dalam contoh ini, perhatikan bahwa string bit asli, yang terdiri dari 68 bit, dikompresi menjadi 40 bit—pengurangan sebesar 42 persen—dan tidak ada data yang hilang (oleh karena itu, dinamakan *lossless*). Salah satu kelemahan dari teknik ini adalah teknik ini hanya berguna jika data asli sebagian besar terdiri dari biner 0. Seperti yang akan kita lihat nanti di bab ini, pengkodean run-length digunakan dalam mengompresi gambar video (karena adanya banyak nilai nol), serta mengompresi dokumen lain yang memiliki karakter berulang.

Teknik kedua yang dapat digunakan untuk mengompres data ketika kompresi *lossless* diperlukan adalah teknik Lempel-Ziv. Teknik ini cukup populer dan digunakan oleh program seperti PKZIP WinZip, gzip, UNIX Compress, dan Microsoft Compressed Folders. Meskipun algoritme sebenarnya cukup rumit, pemahaman dasar tentang cara kerja algoritme dapat diperoleh. Saat string yang akan dikirim diproses, pengirim data membuat “kamus” string karakter dan kode terkait. Kumpulan kode ini ditransmisikan dan penerima kemudian membuat kembali kamus dan string data asli saat kode data diterima.

Algoritma Lempel-Ziv cukup efektif dalam mengompresi data. Penelitian telah menunjukkan bahwa file program komputer dapat diperkecil hingga 44 persen dari ukuran aslinya, file teks dapat diperkecil hingga 64 persen dari ukuran aslinya, dan file gambar dapat diperkecil hingga 88 persen dari ukuran aslinya.

Dimungkinkan juga untuk mengompresi file musik dan audio dan tidak kehilangan konten audio apa pun. Meskipun sebagian besar pemutar musik portabel menggunakan skema kompresi *lossy* (seperti MP3), semakin banyak pengguna yang beralih ke kompresi *lossless* untuk mempertahankan salinan rekaman analog yang lebih tepat. Demikian pula, sebagian besar pengguna komersial yang mendigitalkan dan mengompresi rekaman analog tidak ingin kehilangan musik aslinya. Untuk tujuan ini, tersedia sejumlah skema kompresi audio *lossless*. Ini termasuk FLAC (Codec Audio Lossless Gratis), MPEG-4 ALS (Audio Lossless Coding), TTA (The True Audio), WavPak, Apple Lossless Encoder (ALE), dan Monkey's Audio. Meskipun beberapa skema ini bersifat eksklusif, FLAC, TTA, dan WavPak gratis dan/atau open source. Dan sebagian besar, jika tidak semua, dapat mengompresi sumber audio setidaknya 50 persen.

Kompresi yang merugikan

Semua teknik kompresi yang dijelaskan sejauh ini merupakan contoh kompresi *lossless*. Kompresi *lossless* diperlukan jika sifat data sedemikian rupa sehingga penting agar

tidak ada data yang hilang selama tahap kompresi dan dekompresi. Seperti file program, teks, dan gambar, gambar video dan file audio berkualitas lebih tinggi (seperti yang baru saja kita lihat) juga dapat dikompresi menggunakan kompresi lossless, namun persentase pengurangannya biasanya tidak terlalu signifikan. Hal ini disebabkan oleh sifat data dalam file video dan audio: Tidak ada satu simbol atau kumpulan simbol yang muncul cukup sering untuk menghasilkan tingkat kompresi yang wajar. Misalnya, jika Anda mengambil beberapa video dan mendigitalkannya, Anda akan menghasilkan aliran biner 1 dan 0 yang panjang. Untuk mengompresi aliran ini, Anda dapat memilih untuk melakukan pengkodean run-length lossless pada angka 1 atau 0. Namun sayangnya, karena jenis data ini bersifat dinamis, mungkin tidak akan ada pengulangan bit yang cukup untuk menghasilkan kompresi yang wajar. Oleh karena itu, Anda mungkin ingin mempertimbangkan beberapa teknik kompresi lainnya.

Namun, musik dan video memiliki properti lain yang dapat dimanfaatkan untuk melakukan kompresi yang efektif. Mari kita pertimbangkan musik terlebih dahulu. Ketika seseorang sedang mendengarkan musik, jika dua suara dimainkan secara bersamaan, telinga akan mendengar suara yang lebih keras dan biasanya mengabaikan suara yang lebih lembut. Selain itu, telinga manusia hanya dapat mendengar suara dalam rentang tertentu, yang rata-rata orang adalah 20 Hz hingga 20 kHz (20.000 Hz). Akibatnya, terdapat suara-suara, yang biasanya terjadi pada batas jangkauan pendengaran normal yang ekstrem, yang tidak dapat didengar oleh telinga manusia dengan baik atau bahkan tidak dapat didengar sama sekali. Insinyur audio memanfaatkan fakta ini (dan fakta lainnya) untuk mengompresi musik melalui teknik yang disebut pembentukan derau perseptual, atau pengkodean perseptual. Jika pengkodean perseptual dilakukan dengan baik, versi aliran audio yang dikompresi terdengar cukup mirip dengan versi yang tidak dikompresi (yaitu, hampir berkualitas CD) meskipun beberapa data asli telah dihapus.

MP3, yang merupakan singkatan dari MPEG (Moving Picture Experts Group) Audio Layer-3, adalah bentuk kompresi audio yang umum. (Kelompok Pakar Gambar Bergerak juga telah mengembangkan standar kompresi untuk siaran HDTV, sistem satelit digital [DSS], dan film DVD.) Setelah menggunakan trik pengkodean perseptual ini, encoder MP3 menghasilkan aliran data yang memiliki kecepatan data jauh lebih lambat. dibandingkan musik konvensional berkualitas CD. Sementara pemutar CD dirancang untuk mereproduksi musik yang telah dikodekan dengan 44.100 sampel per detik, yang menghasilkan aliran data 705.600 bit per detik (44.100 sampel per detik dikalikan 16 bit per sampel) atau sekitar 706 kbps, encoder MP3 biasanya mereproduksi aliran data 128 kbps hingga 192 kbps. Pengurangan data semacam ini menghasilkan rasio kompresi 10 banding 1 untuk lagu pada umumnya. Dengan demikian, proses kompresi mengurangi jumlah data serta kecepatan transfer data musik dalam perangkat penghasil musik.

File video juga dapat dikompresi dengan menghilangkan detail kecil dari gambar yang, dalam hal ini, rata-rata mata manusia tidak akan menyadarinya. JPEG yang merupakan singkatan dari Joint Photographic Experts Group merupakan teknik yang sangat umum digunakan untuk mengompres gambar video. Proses konversi gambar ke format JPEG melibatkan tiga fase: transformasi kosinus diskrit, kuantisasi, dan pengkodean run-length.

Untuk melakukan transformasi kosinus diskrit, gambar dipecah menjadi beberapa blok piksel berukuran 8 kali 8, di mana setiap piksel mewakili satu titik warna dalam gambar berwarna atau satu bayangan hitam putih dalam gambar hitam putih. . Setiap blok berukuran 8 kali 8 (sesuai dengan 64 piksel) kemudian dikenakan rutinitas matematika yang cukup umum yang disebut transformasi kosinus diskrit. Pada dasarnya, apa yang dilakukan transformasi ini adalah menghasilkan blok nilai berukuran 8 kali 8 yang baru. Nilai-nilai ini, sekarang disebut frekuensi spasial, yang merupakan perhitungan kosinus dari seberapa besar perubahan setiap nilai piksel sebagai fungsi dari posisinya dalam blok. Daripada membahas proses ini secara matematis, mari kita periksa dua contoh yang cukup sederhana.

Jika kita mempunyai gambar dengan perubahan warna yang cukup seragam di seluruh area gambar—dengan kata lain, tidak banyak detail halus—maka salah satu dari blok piksel berukuran 8 x 8 mungkin terlihat seperti blok berikut, yang setiap nilai desimalnya mewakili tingkat warna tertentu:

15	18	21	24	28	32	36	40
19	22	25	28	32	36	40	44
22	25	28	32	36	40	44	48
26	29	32	35	39	43	47	51
30	34	38	42	46	51	56	61
34	38	42	46	51	56	61	66
38	42	46	51	56	61	66	72
43	48	53	58	63	68	74	80

Setelah menerapkan transformasi kosinus diskrit pada piksel-piksel ini, kita kemudian akan mendapatkan sekumpulan frekuensi spasial seperti berikut:

628	-123	12	-8	0	-2	-1
-185	23	-5	0	0	0	0
10	0	0	0	0	0	0
0	0	0	0	0	0	0
3	0	0	0	0	0	0
-1	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

Perhatikan banyaknya entri nol, dan entri bukan nol dikelompokkan di sudut kiri atas blok. Hal ini disebabkan oleh perhitungan kosinus diskrit, yang pada dasarnya menggambarkan perbedaan antara warna suatu piksel relatif terhadap warna piksel tetangganya, bukan nilai absolut warna piksel tertentu. Alasan lain dilakukannya pengelompokan adalah karena gambar ini, seperti disebutkan sebelumnya, merupakan gambar dengan warna yang cukup seragam—artinya, tidak banyak variasi warna—sehingga hanya ada sedikit perubahan saat Anda menjauh dari sudut kiri atas.

Namun, misalkan kita mempunyai gambar yang memiliki banyak detail halus. Ini akan memiliki blok piksel berukuran 8 kali 8 yang memiliki nilai sangat berbeda dan mungkin terlihat seperti berikut:

120	80	110	65	90	142	56	100
40	136	93	188	90	210	220	56
95	89	134	74	170	180	45	100
9	110	145	93	221	194	83	110
65	202	90	18	164	90	155	43
93	111	39	221	33	37	40	129
55	122	52	166	93	54	13	100
29	92	153	197	84	197	84	83

Setelah menerapkan transformasi kosinus diskrit ke piksel gambar ini, kita kemudian akan mendapatkan sekumpulan frekuensi spasial seperti berikut:

652	32	-40	54	-18	129	-33	84
111	-33	53	9	122	-43	65	100
-22	101	94	-32	23	104	76	101
88	33	211	2	-32	143	43	14
132	-32	43	0	122	-48	54	110
54	11	133	27	56	154	13	-94
-54	-69	10	109	65	0	27	-33
199	-18	99	98	22	43	8	32

Perhatikan bahwa hanya sedikit entri nol di blok frekuensi spasial ini. Mari kita lanjutkan proses konversi dengan memfokuskan pada blok ini yang sesuai dengan gambar dengan banyak detail halus.

Fase kedua dalam konversi gambar ke file JPEG adalah fase kuantisasi. Tujuan dari fase ini adalah mencoba menghasilkan lebih banyak entri nol di blok 8 kali 8. Untuk melakukan ini, kita perlu membagi setiap nilai dalam blok dengan angka tertentu dan mengabaikan sisanya. Misalnya, jika blok piksel berisi frekuensi spasial dengan nilai 9, kita akan membaginya dengan 10 untuk mendapatkan hasil 0. Namun kita tidak ingin membagi 64 frekuensi spasial dengan nilai yang sama karena nilai di atas -sudut kiri blok lebih penting (karena operasi transformasi kosinus diskrit). Jadi mari kita bagi blok frekuensi spasial dengan blok nilai yang mana nilai di sudut kiri atas mendekati 1—dan dengan demikian akan berfungsi untuk mereproduksi bilangan asli dalam suatu pembagian. Contoh blok tersebut adalah sebagai berikut:

1	4	7	10	13	16	19	22
4	7	10	13	16	19	22	25
7	10	13	16	19	22	25	28
10	13	16	19	22	25	28	31
13	16	19	22	25	28	31	33

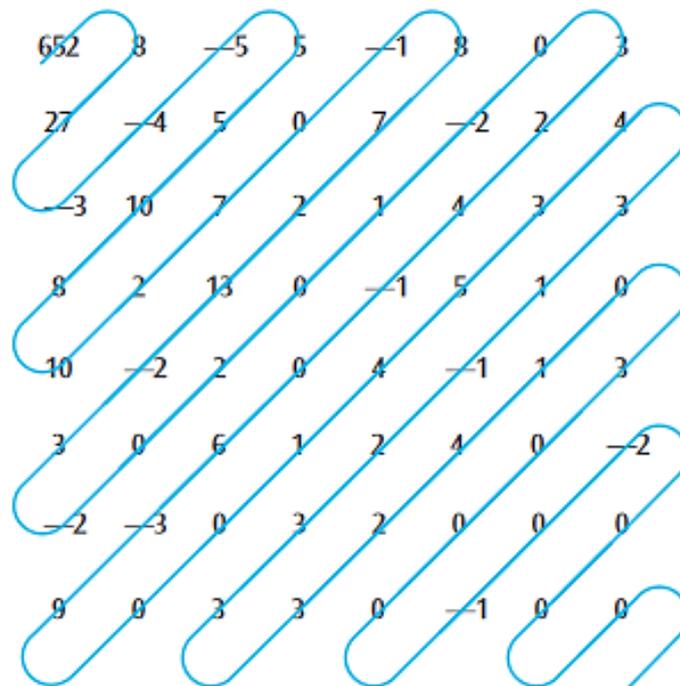
16	19	22	25	28	31	33	36
19	22	25	28	31	34	37	40
22	25	28	31	34	37	40	43

Sekarang ketika kita membagi blok frekuensi spasial dengan blok nilai tertimbang ini, kita harus menghasilkan blok nilai baru dengan lebih banyak entri nol, seperti yang ditunjukkan di sini:

652	8	-5	5	-1	8	0	3
27	-4	5	0	7	-2	2	4
-3	10	7	2	1	4	3	3
8	2	13	0	-1	5	1	0
10	-2	2	0	4	-1	1	3
3	0	6	1	2	4	0	-2
-2	-3	0	3	2	0	0	0
9	0	3	3	0	-1	0	0

Pertanyaan yang harus Anda ajukan saat ini adalah: Jika kita melakukan 64 pembagian dan membuang sisanya, bukankah kita akan kehilangan sesuatu dari gambar aslinya? Jawabannya adalah ya, kami akan melakukannya. Namun kami berharap dapat memilih serangkaian nilai optimal sehingga kami tidak kehilangan terlalu banyak gambar aslinya. Dengan kata lain, dalam upaya untuk memaksimalkan jumlah nol di setiap blok (sehingga kita dapat berhasil melakukan pengkodean run-length pada fase akhir), kita mengizinkan data (yaitu gambar) untuk berubah sedikit—tetapi mudah-mudahan tidak terlalu banyak sehingga mata manusia dapat mendeteksi perbedaan besar antara file asli dan file yang telah dikompresi dan didekompresi.

Terakhir, fase ketiga dari teknik kompresi JPEG adalah mengambil matriks nilai terkuantisasi dan melakukan pengkodean run-length pada angka nol. Namun triknya di sini adalah Anda tidak mengkodekan angka nol dengan run-length hanya dengan naik dan turun baris pada blok 8 kali 8. Sebaliknya, kita memanfaatkan fakta bahwa kita akan mencapai angka nol yang lebih panjang jika kita mengkodekan secara diagonal, seperti yang ditunjukkan pada Gambar 5-13.



Gambar 5-13 Pengkodean run-length pada gambar JPEG

Bagaimana dengan gambar video bergerak, seperti yang Anda temui saat menonton televisi digital atau DVD? Apakah jenis data ini mempunyai karakteristik unik yang dapat kita manfaatkan untuk mengompresi file? Ternyata memang demikian. Video sebenarnya adalah serangkaian gambar. Bila gambar atau bingkai ini ditampilkan secara berurutan, objek dalam gambar tampak seolah-olah bergerak. Untuk membuat gerakan (karakter, objek, pemandangan) dalam sebuah film tampak mengalir, perangkat proyeksi film atau televisi menampilkan gambar atau bingkai tersebut dengan kecepatan kira-kira 30 bingkai per detik. Namun ada aspek menarik dari bingkai ini, yang mungkin Anda perhatikan jika Anda pernah mencoba membuat kartun dengan menggambar di beberapa lembar kertas dan kemudian membolak-balik halamannya. Kecuali jika ada perubahan adegan secara menyeluruh, satu gambar terlihat sangat mirip dengan gambar berikutnya. Dalam konteks kompresi, pertanyaan yang perlu dipertimbangkan adalah: Jika gambar yang berurutan sangat mirip, mengapa harus mentransfer gambar penuh dari setiap frame? Mengapa tidak mentransfer perbedaan antara kedua frame saja? Transfer semacam ini adalah contoh pengkodean diferensial. MPEG-1 dan MPEG-2—atau sekadar MPEG—adalah contoh umum dari bentuk kompresi ini.

Ingatlah bahwa perangkat video menampilkan beberapa (biasanya 30) frame per detik. Untuk menghemat ruang, tidak semua dari 30 frame tersebut merupakan gambar lengkap. MPEG sebenarnya menciptakan kerangka informasi yang lengkap, diikuti oleh beberapa bingkai parsial, atau perbedaan, diikuti oleh bingkai lengkap. Lebih tepatnya, frame berikut dibuat:

I B B P B B B I B B P ...

dimana I-frame merupakan frame lengkap, P-frame adalah perbedaan dari I-frame sebelumnya (dan dibuat menggunakan prediksi kompensasi gerak), dan B-frame adalah frame perbedaan, yang berisi perbedaan lebih kecil antara bingkai I dan bingkai P dan disisipkan di antara bingkai I dan P untuk menghaluskan gerakan.

Karena MPEG rumit secara komputasi, chip prosesor telah dirancang, seperti Teknologi MMX Intel, khusus untuk kompresi dan dekompresi gambar MPEG.

5.9 MULTIPLEXING BISNIS

Bill's Market adalah toko berukuran sedang di kota yang menjual bahan makanan. Di konter check-out, seseorang dapat menemukan 10 mesin kasir tempat penjualan. Toko ingin menghubungkan semua mesin kasir ke server di ruang belakang. Ruang belakang kira-kira berjarak 100 meter dari mesin kasir. Mengingat teknologi yang telah diperkenalkan dalam teks sejauh ini, ada tiga skenario yang mungkin untuk menghubungkan mesin kasir ke server:

- Hubungkan setiap mesin kasir ke server menggunakan jalur point-to-point yang terpisah. Setiap baris akan menjadi suatu bentuk media yang dilakukan.
- Mengirimkan keluaran setiap mesin kasir ke server melalui suatu bentuk sinyal nirkabel.
- Gabungkan semua keluaran mesin kasir menggunakan multiplexing, dan kirimkan aliran multipleks ke server melalui jalur media terkonduksi.

Mari kita periksa pro dan kontra dari setiap solusi. Solusi pertama yaitu menghubungkan masing-masing mesin kasir ke server dengan menggunakan media yang dilakukan secara point-to-point mempunyai beberapa kelebihan namun juga terdapat beberapa kekurangan. Jarak 100 meter berpotensi menimbulkan masalah. Saat mentransmisikan data dalam jutaan bit per detik, twisted pair biasanya memiliki jarak maksimum 100 meter. Gangguan elektromagnetik selalu merupakan masalah potensial, dan setelah pemasangan kabel, kita mungkin menemukan bahwa, mengingat jaraknya, terdapat terlalu banyak kebisingan. Media yang lebih tahan kebisingan, seperti kabel twisted pair berpelindung atau kabel serat optik, mungkin merupakan pilihan yang masuk akal. Namun pilihan ini akan lebih mahal. Keuntungan utama dari solusi pertama mencakup biaya yang lebih rendah dalam menggunakan media terkonduksi yang relatif murah dan fakta bahwa banyak jalur point-to-point menghilangkan kebutuhan akan layanan tambahan seperti polling atau multiplexing.

Solusi kedua dengan menggunakan sinyal nirkabel untuk mengirimkan antara mesin kasir dan server cukup menarik, namun bentuk sinyal nirkabel apa yang akan digunakan? Sinyal nirkabel harus menembus dinding (menghilangkan inframerah), mampu melintasi jarak sekitar 100 meter (menghilangkan Bluetooth dan ZigBee), dan mampu membawa sinyal berkecepatan tinggi (sekali lagi menghilangkan ZigBee). Untuk alasan yang jelas, microwave, satelit, WiMax, dan optik ruang bebas adalah solusi yang tidak masuk akal. Satu-satunya pilihan nirkabel yang memerlukan pemeriksaan lebih lanjut adalah LAN nirkabel. Namun kita harus menunggu hingga Bab Tujuh untuk membahas topik tersebut lebih lanjut.

Solusi ketiga—untuk memasang multipleksor dengan mesin kasir dan demultipleksor pada server di ruang belakang—juga memerlukan pemikiran dan penyelidikan terlebih dahulu. Masalah-masalah berikut patut dipertimbangkan:

- Dapatkah sepasang multipleksor menangani 10 mesin kasir? Jika tidak, kita mungkin harus memasang dua atau lebih pasang multipleksor.
- Berapa harga sepasang multipleksor? Akankah biayanya begitu tinggi sehingga kita terpaksa mempertimbangkan alternatif lain?
- Media apa yang bisa kita gunakan untuk menghubungkan multipleksor? Berapa banyak kabel yang perlu kita jalankan? Kabel serat optik atau bahkan kabel koaksial mungkin merupakan pilihan yang baik.
- Apakah solusi multipleksor dapat diskalakan? Dapatkah sistem ini diperluas dengan menyertakan mesin kasir tambahan di masa mendatang? Dalam skenario terburuk, kita harus menambahkan pasangan multipleksor tambahan dan lebih banyak kabel.

Terakhir, seperti telah disebutkan, mungkin ada solusi tambahan yang belum kita temukan dalam teks. Apakah ada cara agar kita dapat menghubungkan semua mesin kasir ke jaringan area lokal? Kita mungkin bisa menggunakan pendekatan kabel atau nirkabel. Sayangnya, kami belum mencakup jaringan area lokal, sehingga pengujian solusi ini harus menunggu.

Kesimpulannya, saat ini tampak bahwa skema multiplexing mungkin memberikan efisiensi penggunaan sejumlah kecil kabel yang melewati penyimpanan. Jika kabel berkualitas tinggi seperti kabel serat optik digunakan, maka akan meminimalkan gangguan kebisingan dan memungkinkan pertumbuhan terbesar di masa depan.

RINGKASAN

- Agar beberapa sinyal dapat berbagi satu media, media tersebut harus dibagi menjadi beberapa saluran. Tiga teknik dasar untuk membagi suatu media menjadi beberapa saluran adalah: pembagian frekuensi, pembagian waktu, dan pembagian kode transmisi.
- Multiplexing pembagian frekuensi melibatkan penetapan rentang frekuensi yang tidak tumpang tindih pada sinyal yang berbeda. Multiplexing pembagian frekuensi menggunakan sinyal analog, sedangkan multiplexing pembagian waktu menggunakan sinyal digital.
- Time Division Multiplexing suatu media melibatkan pembagian waktu transmisi yang tersedia pada suatu media kepada para pengguna. Multiplexing pembagian waktu memiliki dua bentuk dasar: multiplexing pembagian waktu sinkron dan multiplexing pembagian waktu statistik.
- Multiplexing pembagian waktu sinkron menerima masukan dari sejumlah perangkat tetap dan mengirimkan datanya dalam pola berulang yang tidak ada habisnya. Sistem telepon T-1 dan SONET/SDH adalah contoh umum sistem yang menggunakan multiplexing pembagian waktu sinkron. Penugasan statis perangkat input ke frekuensi atau slot waktu tertentu dapat menjadi sia-sia jika perangkat input tidak terus-menerus mengirimkan data.

- Multiplexing pembagian waktu statistik menerima masukan dari sekumpulan perangkat yang memiliki data untuk dikirim, membuat bingkai berisi data dan informasi kontrol, dan mentransmisikan bingkai tersebut. Perangkat input yang tidak memiliki data untuk dikirim tidak termasuk dalam frame.
- Multiplexing pembagian panjang gelombang melibatkan sistem serat optik dan transfer beberapa aliran data melalui satu serat menggunakan beberapa pemancar laser berwarna. Sistem multiplexing pembagian panjang gelombang bisa padat atau kasar.
- Multinada diskrit adalah teknologi yang digunakan dalam sistem DSL. Beberapa subsaluran, masing-masing mendukung bentuk modulasi amplitudo kuadratur, dimultipleks bersama untuk menyediakan satu aliran data bagi pengguna.
- Multiplexing pembagian kode memungkinkan banyak pengguna untuk berbagi rangkaian frekuensi yang sama dengan memberikan kode digital unik kepada setiap pengguna.
- Kompresi adalah proses yang memadatkan data menjadi paket yang lebih kecil. Saat disimpan, data terkompresi menghemat ruang; ketika ditransmisikan, menghasilkan waktu transmisi yang lebih singkat.
- Terdapat dua bentuk dasar kompresi: lossless, yaitu tidak ada data yang hilang selama tahap kompresi dan dekompresi; dan lossy, dimana sebagian data asli hilang.
- Dua bentuk kompresi lossless yang populer mencakup pengkodean run-length dan teknik kompresi Lempel-Ziv. Sejumlah skema kompresi audio lossless juga ada.
- Kompresi lossy merupakan dasar dari sejumlah teknik kompresi, termasuk MP3 untuk audio, JPEG untuk gambar diam, dan MPEG untuk video bergerak.

PERTANYAAN

1. Sebutkan tiga contoh umum multiplexing pembagian frekuensi.
2. Multiplexing pembagian frekuensi sering dikaitkan dengan jenis sinyal apa?
3. Dalam urutan apa multiplexing pembagian waktu sinkron mengambil sampel setiap sinyal yang masuk?
4. Apa yang akan terjadi jika multipleksor pembagian waktu sinkron mengambil sampel sinyal masuk yang tidak berurutan?
5. Bagaimana multipleksor pembagian waktu sinkron tetap tersinkronisasi dengan demultiplexor di sisi penerima?
6. Berapa banyak saluran terpisah yang digabungkan oleh multipleksor T-1 menjadi satu aliran?
7. Apa persamaan T-1 dan SONET?
8. Apa perbedaan utama antara multiplexing pembagian waktu statistik dan multiplexing pembagian waktu sinkron?
9. Jika multipleksor statistik dihubungkan ke 20 perangkat, apakah memerlukan saluran keluaran berkecepatan tinggi yang setara dengan jumlah 20 aliran transmisi? Pertahankan tanggapan Anda.
10. Mengapa pengalamanan aliran data individual diperlukan untuk multiplexing statistik?

11. Jenis media apa yang diperlukan untuk mendukung multiplexing pembagian panjang gelombang?
12. Berapa banyak panjang gelombang berbeda yang dapat ditempatkan pada multiplexing pembagian panjang gelombang padat pada satu sambungan?
13. Apa perbedaan antara multiplexing pembagian panjang gelombang padat dan multiplexing pembagian panjang gelombang kasar?
14. Apa perbedaan multinada diskrit dengan teknik multipleksing lainnya? Bagaimana kemiripannya?
15. Bagaimana cara multiplexing pembagian kode membedakan satu sinyal dengan sinyal lainnya?
16. Apa dua bentuk dasar kompresi?
17. Pengkodean run-length dapat digunakan untuk mengompresi jenis data apa?
18. Apa tiga fase kompresi JPEG?

LATIHAN SOAL

1. Dibandingkan dengan teknik multiplexing lainnya, nyatakan dua kelebihan dan dua kelemahan dari masing-masing teknik berikut:
 - A. multiplexing pembagian frekuensi
 - B. multiplexing pembagian waktu sinkron
 - C. multiplexing pembagian waktu statistik
 - D. multiplexing pembagian panjang gelombang
2. Keuntungan dari multiplexing pembagian frekuensi dan multiplexing pembagian kode adalah semua penerima tidak harus berada di lokasi yang sama. Jelaskan akibat dari manfaat tersebut dan berikan contohnya.
3. Dua puluh empat sinyal suara akan dimultipleks dan ditransmisikan melalui pasangan terpelintir. Berapa total bandwidth yang diperlukan jika multiplexing pembagian frekuensi digunakan?
4. Dua puluh sinyal suara harus dimultipleks dan dikirim melalui pasangan terpilin. Berapa lebar pita yang diperlukan (dalam bps) jika multiplexing pembagian waktu sinkron digunakan, bersama dengan laju pengambilan sampel analog-ke-digital standar, dan setiap sampel diubah menjadi nilai 8-bit?
5. Jika hanya empat komputer yang mentransmisikan data digital melalui jalur T-1, berapakah kecepatan data maksimum yang mungkin untuk setiap komputer?
6. Apa tujuan bit sinkronisasi dalam frame T-1? Mengapa ini perlu?
7. Sepuluh perangkat terhubung ke multipleksor pembagian waktu sinkron. Setiap workstation mentransmisikan pada 128 kbps. Pada suatu saat, 40 persen stasiun kerja tidak melakukan transmisi. Berapa kecepatan minimum yang diperlukan agar saluran meninggalkan multipleksor? Akankah jawabannya berbeda jika kita menggunakan multipleksor statistik? Jelaskan alasan Anda.
8. Ketika data ditransmisikan menggunakan multiplexor statistik, masing-masing unit data harus memiliki suatu bentuk alamat yang memberitahukan kepada penerima

- identitas penerima yang dituju dari setiap bagian data. Alih-alih menetapkan alamat absolut pada setiap bagian data, apakah mungkin untuk memasukkan pengalamatan relatif? Jika ya, jelaskan manfaatnya.
9. Perusahaan telepon memiliki saluran serat optik dengan multiplexing pembagian waktu yang membentang dari Amerika Serikat ke Inggris dan terletak di dasar laut. Jalur serat optik ini telah mencapai kapasitasnya. Alternatif apa yang dapat dipertimbangkan oleh perusahaan telepon untuk meningkatkan kapasitas?
 10. Sistem multinada diskrit menggunakan teknik modulasi pada subsalurannya, yang masing-masing menghasilkan aliran 64-kbps. Dengan asumsi kondisi ideal (tidak ada noise), berapa kecepatan data maksimum sistem multinada diskrit?
 11. Perusahaan telepon seluler di kota menggunakan multiplexing pembagian kode untuk mengirimkan sinyal antara menara selulernya dan telepon seluler. Anda menggunakan ponsel Anda sambil berdiri di samping seseorang yang menggunakan ponselnya. Bagaimana sistem membedakan kedua sinyal tersebut?
 12. Pengguna seluler A menggunakan multiplexing pembagian kode dan telah diberi kode biner 000011111. Pengguna seluler B, yang juga menggunakan multiplexing pembagian kode, telah diberi kode biner 01010101. Menara seluler mentransmisikan 1 ke pengguna seluler A, sedangkan menara seluler mengirimkan 0 ke ponsel pengguna B. Tunjukkan jumlah produk yang dihasilkan dan perhitungan Anda.
 13. Berapa banyak frame per detik yang ditransmisikan oleh T-1 dan SONET? Mengapa nomor ini?
 14. Mengapa multiplexing pembagian panjang gelombang lebih mirip multiplexing pembagian frekuensi dan kurang seperti multiplexing pembagian waktu?
 15. Teknik multiplexing manakah yang dapat digunakan pada media konduksi dan media nirkabel, mana pada media konduksi saja, dan mana pada media nirkabel saja?
 16. Secara teori, multiplexing pembagian kode dapat memiliki 264 sinyal berbeda di area yang sama. Pada kenyataannya, hal ini tidak mungkin dilakukan. Mengapa tidak? Tunjukkan sebuah contoh.
 17. Apakah bentuk DSL yang digunakan perusahaan berbeda dengan bentuk DSL yang digunakan oleh pengguna rumahan? Menjelaskan.
 18. Jika data memiliki satu jenis simbol dalam jumlah besar, jenis kompresi manakah yang paling efektif?
 19. Dengan adanya string bit berikut, tampilkan pengkodean run-length yang akan menghasilkan: 00000001000001100000000000 000000010000 001110000000000
 20. Bisakah Anda mengompresi kumpulan laporan bank menggunakan kompresi JPEG? Menjelaskan.
 21. MP3, JPEG, dan MPEG semuanya bergantung pada karakteristik data apa untuk melakukan kompresi?

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Sebuah perusahaan mempunyai dua gedung yang jaraknya 50 meter (kira-kira 50 yard). Di antara bangunan tersebut terdapat tanah pribadi milik perusahaan. Sebuah terowongan besar menghubungkan kedua bangunan tersebut. Dalam satu gedung terdapat kumpulan 30 stasiun kerja komputer; di gedung lain ada komputer mainframe. Apa cara terbaik untuk menghubungkan workstation ke komputer mainframe? Jelaskan alasan Anda dan semua kemungkinan solusi yang Anda pertimbangkan.
2. Sebuah perusahaan mempunyai dua gedung yang jaraknya 100 meter (kira-kira 100 yard). Di antara bangunan terdapat lahan umum tanpa terowongan akses. Dalam satu gedung terdapat kumpulan 30 stasiun kerja komputer; di gedung lain ada komputer mainframe. Apa cara terbaik untuk menghubungkan workstation ke komputer mainframe? Jelaskan alasan Anda dan semua kemungkinan solusi yang Anda pertimbangkan.
3. Apa hubungan, jika ada, antara multiplexing pembagian waktu sinkron dan koneksi sinkron dan asinkron yang dijelaskan dalam Bab Empat?
4. Bandingkan dan kontraskan teknik multiplexing lama seperti pembagian frekuensi dan multiplexing pembagian waktu dengan teknik yang lebih baru seperti multiplexing pembagian frekuensi diskrit dan ortogonal. Apa yang menjadi tren dalam protokol-protokol baru ini?
5. Anda menerima akses Internet berkecepatan tinggi dari penyedia DSL. Anda juga tinggal tidak jauh dari antena siaran AM stasiun radio. Apakah DSL Anda terpengaruh oleh antena ini? Menjelaskan.
6. Pertimbangkan layar VGA yang memiliki 640.800 piksel per layar. Selanjutnya asumsikan bahwa setiap piksel berukuran 24 bit (8 untuk merah, 8 untuk biru, dan 8 untuk hijau). Jika sebuah video film menampilkan 30 bingkai (gambar) per detik, berapa byte yang diperlukan film berdurasi dua jam untuk penyimpanan? Berapa byte yang dapat ditampung oleh DVD standar? Lalu berapa rasio kompresinya?
7. Temukan materi iklan yang mencantumkan jumlah maksimum perangkat yang dapat ditangani oleh multipleksor pembagian frekuensi atau waktu. Apakah angka ini konsisten dengan apa yang disajikan pada bab tersebut?
8. Televisi siaran digital telah menggantikan televisi analog konvensional. Bentuk multiplexing apa yang digunakan untuk menyiarkan sinyal televisi digital?
9. Radio siaran adalah salah satu bentuk hiburan terakhir yang beralih ke digital. Temukan materi terbaru yang menjelaskan keadaan radio siaran digital saat ini, dan tulis laporan dua atau tiga halaman yang mencakup jenis multipleksing yang diharapkan dan dampak radio digital terhadap pasar radio saat ini.
10. FCC menciptakan serangkaian frekuensi untuk radio walkie-talkie. Perangkat ini disebut layanan radio keluarga dan memungkinkan dua radio memancarkan hingga jarak beberapa mil. Jenis multiplexing apa yang digunakan pada radio ini? Berapa

banyak saluran bersamaan yang diperbolehkan? Apakah ada teknologi yang lebih baru dari layanan radio keluarga? Jika iya, jelaskan ciri-cirinya.

11. Loop lokal dari rangkaian telepon yang masuk ke rumah Anda menggunakan multiplexing sehingga orang-orang di kedua ujung sambungan dapat berbicara pada saat yang sama (jika mereka mau). Jenis multipleksing apa yang digunakan? Sebutkan rincian teknik multiplexing.
12. Ada berbagai bentuk kompresi MPEG (seperti MPEG-1, MPEG-2, dll.). Cantumkan masing-masing formulir dengan kalimat penyerta yang menjelaskan jenis data apa yang dirancang untuk formulir kompresi tersebut.
13. Skema kompresi apa lagi yang ada selain yang tercantum dalam bab ini? Apa kegunaan masing-masing skema kompresi?

BAB 6

KESALAHAN, DETEKSI KESALAHAN, DAN PENGENDALIAN KESALAHAN

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Identifikasi berbagai jenis kebisingan yang umum ditemukan di jaringan komputer
- Tentukan berbagai teknik pencegahan kesalahan, dan mampu menerapkan salah satunya pada jenis kebisingan
- Bandingkan berbagai teknik deteksi kesalahan dalam hal efisiensi dan kemanjuran
- Lakukan perhitungan paritas sederhana dan paritas longitudinal, serta sebutkan kekuatan dan kelemahannya
- Sebutkan keuntungan dari checksum redundansi siklik, dan tentukan jenis kesalahan apa yang akan dideteksinya
- Sebutkan keuntungan checksum aritmatika, dan tentukan jenis aplikasi apa yang menggunakannya
- Bedakan antara bentuk-bentuk dasar pengendalian kesalahan, dan jelaskan keadaan di mana masing-masing bentuk tersebut dapat digunakan
- Ikuti contoh kode koreksi diri Hamming

SELAMA MUSIM PANAS 2003, planet Mars berada dalam jarak 34.646.418 mil dari Bumi. Ini adalah jarak terdekat Mars ke Bumi dalam 59.619 tahun. Bahkan pada jarak ini, sinyal radio memerlukan waktu 3 menit 6 detik untuk menempuh perjalanan antar planet. Sekarang bayangkan sebuah wahana di Mars yang dapat melintasi lanskap Mars dan melakukan manuver seperti maju, berbelok ke kanan, mengambil gambar, dan menggali sampel. Wahana ini dapat mengambil keputusan sendiri tentang apa yang harus dilakukan selanjutnya, atau—lebih mungkin, demi alasan keamanan—mengirim gambar kembali ke Bumi dan kemudian menunggu instruksi dari para ilmuwan. Jika diperlukan waktu 3 menit 6 detik agar sinyal merambat ke Bumi, beberapa menit bagi para ilmuwan untuk memutuskan apa yang harus dilakukan oleh wahana tersebut, dan kemudian 3 menit 6 detik agar sinyal merambat kembali ke Mars, maka wahana Mars tidak mungkin menyelesaikan tugas dengan sangat cepat. Sekarang mari kita tambahkan satu kerutan lagi. Misalkan selama transfer data sejauh 34,6 juta mil tersebut, sinyal menjadi rusak dan pihak penerima harus meminta pihak pengirim untuk mengirim ulang karena tidak dapat membaca data. Dalam hal ini, membuat wahana tersebut melakukan operasi sederhana dapat memakan waktu berjam-jam bagi para ilmuwan. Mengingat hal ini, versi masa depan dari penyelidikan Mars mungkin harus dirancang untuk membuat keputusan sendiri daripada membuang banyak waktu untuk mengirimkan informasi bolak-balik antara Bumi dan Mars. Namun, sementara itu, cara terbaik untuk mengatasi

penundaan waktu tersebut adalah dengan memperbaiki cara pengiriman sinyal yang ditransmisikan.

Apakah kebisingan menjadi masalah besar saat mengirimkan sinyal?

Apakah tidak ada cara untuk mengirimkan sinyal sehingga seluruh sinyal tidak perlu dikirim ulang jika terjadi kesalahan?

Mungkinkah terjadi kesalahan saat transmisi dan tidak terdeteksi?

6.1 PENDAHULUAN

Proses transmisi data melalui suatu media sering kali berjalan sesuai dengan Hukum Murphy: Jika terjadi kesalahan, kemungkinan besar akan terjadi kesalahan. Bahkan jika semua upaya pengurangan kesalahan diterapkan sebelum dan selama transmisi data, sesuatu akan selalu mengubah bentuk data asli. Jika perubahan ini cukup serius, data asli menjadi rusak, dan penerima tidak menerima data yang dikirimkan semula. Bahkan dengan kabel serat optik kualitas tertinggi, kebisingan pada akhirnya tetap masuk dan mulai mengganggu transmisi data. Oleh karena itu, meskipun upaya terbaik telah dilakukan untuk mengendalikan kebisingan, kebisingan tetap tidak bisa dihindari. Ketika rasio kekuatan derau terhadap kekuatan sinyal sedemikian rupa sehingga derau melebihi sinyal, kesalahan akan terjadi. Pada titik inilah teknik deteksi kesalahan menjadi alat yang berharga.

Mengingat kebisingan tidak dapat dihindari dan kesalahan terjadi, sesuatu perlu dilakukan untuk mendeteksi kondisi kesalahan. Bab ini membahas beberapa metode deteksi kesalahan yang lebih umum dan membandingkannya dalam hal efisiensi dan kemanjuran.

Sebelum Anda mulai mempelajari teknik deteksi kesalahan, penting bagi Anda untuk memahami berbagai bentuk gangguan yang umum terjadi selama transmisi data. Memiliki pemahaman yang lebih baik tentang berbagai jenis kebisingan dan penyebabnya akan memungkinkan Anda menerapkan teknik pengurangan kebisingan pada sistem komunikasi dan, dengan demikian, membatasi jumlah kebisingan sebelum mencapai ambang batas terjadinya kesalahan.

Setelah kesalahan terdeteksi, tindakan apa yang harus diambil oleh penerima? Ada tiga pilihan pengendalian kesalahan: membuang frame/paket (mengabaikan kesalahan), mengembalikan pesan kesalahan ke pemancar, atau memperbaiki kesalahan tanpa bantuan pemancar. Meskipun membuang bingkai/paket tampak seperti posisi yang tidak bertanggung jawab, hal ini ada manfaatnya dan layak untuk dikaji. Opsi kedua—mengembalikan pesan kesalahan ke pemancar sehingga pemancar dapat mengirim ulang data asli—adalah tindakan pengendalian kesalahan yang paling umum. Opsi ketiga—mengoreksi kesalahan tanpa meminta bantuan tambahan dari pemancar—mungkin terdengar seperti situasi yang ideal, namun sulit untuk didukung dan memerlukan biaya overhead yang besar.

Bagaimana deteksi kesalahan dan pengendalian kesalahan cocok dengan rangkaian TCP/IP yang diperkenalkan pada Bab Satu? Kebanyakan orang mengasosiasikan deteksi kesalahan dengan lapisan data link/akses jaringan. Saat lapisan data link membuat bingkai, biasanya lapisan ini menyisipkan kode pengecekan kesalahan setelah kolom data. Ketika

frame tiba di stasiun berikutnya, kode pengecekan kesalahan ini diekstraksi dan frame diperiksa keakuratannya. Namun lapisan data link bukanlah satu-satunya lapisan yang melakukan beberapa jenis deteksi kesalahan. Lapisan transport juga mencakup skema deteksi kesalahan. Ketika paket transport tiba di tujuan akhir (dan hanya tujuan akhir), penerima dapat mengekstrak kode pengecekan kesalahan dari header transport dan melakukan deteksi kesalahan. Selain itu, beberapa protokol lapisan jaringan, seperti Internet Protocol (IP), menyertakan kode pendeteksi kesalahan di header lapisan jaringan. Namun dalam kasus IP, deteksi kesalahan dilakukan hanya pada header IP, dan bukan pada kolom data. Banyak aplikasi juga melakukan beberapa jenis pemeriksaan kesalahan seperti mendeteksi paket yang hilang dari rangkaian paket yang dikirimkan. Untuk saat ini, kita akan berkonsentrasi pada detail deteksi kesalahan dan pengendalian kesalahan yang tercakup dalam lapisan data link dan transport. Namun perlu diperhatikan bahwa semua topik yang dibahas sejauh ini dalam buku ini, dengan kemungkinan pengecualian koneksi asinkron, sinkron, dan isokron, merupakan aktivitas lapisan fisik.

Untuk memahami bagaimana deteksi dan pengendalian kesalahan masuk ke dalam banyak lapisan jaringan komputer, penting untuk mengingat konsep dasar di balik rangkaian protokol TCP/IP dan model OSI: Aktivitas satu lapisan tidak boleh terpengaruh oleh aktivitas dari satu lapisan. lapisan lain. Dengan demikian, pemilihan skema deteksi kesalahan atau teknik pengendalian kesalahan merupakan masalah yang terpisah dari jenis media yang dipilih atau pilihan teknik multipleksing. Skema deteksi dan pengendalian kesalahan apa pun yang disajikan dalam bab ini dapat diterapkan pada semua jenis sistem komunikasi.

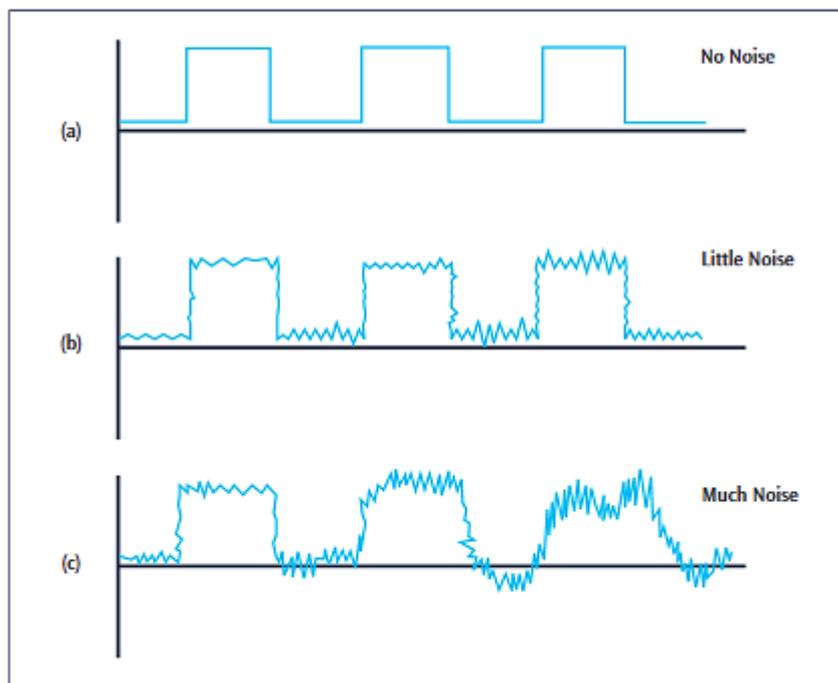
6.2 KEBISINGAN DAN KESALAHAN

Seperti yang Anda duga, sejumlah kesalahan dapat terjadi selama transmisi data. Dari gangguan sederhana hingga gangguan besar-besaran, data yang dikirimkan—baik analog maupun digital—rentan terhadap berbagai jenis gangguan dan kesalahan. Media berbasis tembaga secara tradisional telah diganggu oleh berbagai jenis gangguan dan kebisingan.

Jaringan satelit, gelombang mikro, dan radio juga rentan terhadap interferensi dan crosstalk. Bahkan kabel serat optik dapat menimbulkan kesalahan pada sistem transmisi, meskipun kemungkinan terjadinya kesalahan ini lebih kecil dibandingkan dengan jenis media lainnya. Mari kita periksa beberapa jenis kebisingan utama yang terjadi pada sistem transmisi.

Kebisingan putih

Derau putih, yang juga disebut derau termal atau derau Gaussian, adalah jenis derau yang relatif terus menerus dan mirip dengan derau statis yang Anda dengar saat radio disetel di antara dua stasiun. Sampai tingkat tertentu, ia selalu ada di media transmisi dan perangkat elektronik, dan bergantung pada suhu media. Ketika suhu meningkat, tingkat kebisingan meningkat karena peningkatan aktivitas elektron dalam medium. Karena white noise relatif terus menerus, maka white noise dapat dikurangi secara signifikan namun tidak pernah dapat dihilangkan sepenuhnya. White noise adalah jenis interferensi yang membuat sinyal analog atau digital menjadi kabur (Gambar 6-1).



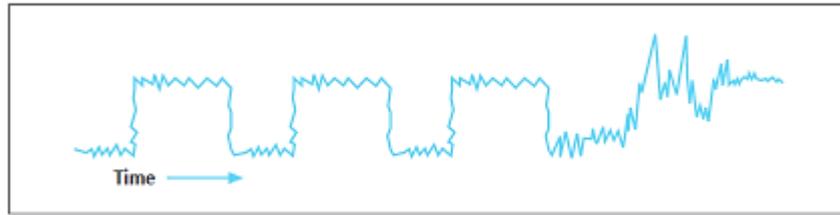
Gambar 6-1 White noise karena mengganggu sinyal digital

Proses pengurangan white noise dari sinyal digital relatif mudah jika sinyal dilewatkan melalui regenerator sinyal sebelum noise tersebut benar-benar menguasai sinyal aslinya. Mengurangi white noise dari sinyal analog juga dimungkinkan sampai tingkat tertentu dan melibatkan melewatkan sinyal analog yang berisik melalui serangkaian filter yang sesuai, yang (diharapkan) hanya menyisakan sinyal asli.

Kebisingan impuls

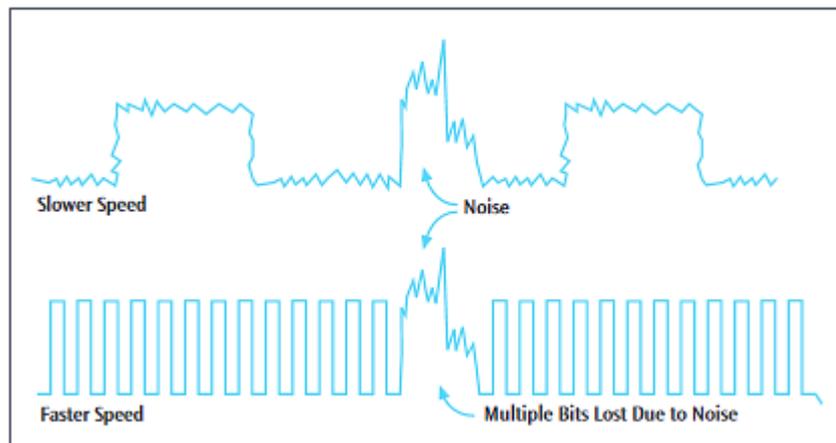
Kebisingan impuls, atau lonjakan kebisingan, adalah kebisingan yang tidak terus-menerus dan salah satu kesalahan yang paling sulit dideteksi karena dapat terjadi secara acak. Kesulitannya muncul dalam memisahkan noise dari sinyal. Biasanya, kebisingan adalah ledakan energi analog. Jika lonjakan impuls mengganggu sinyal analog, menghilangkannya tanpa mempengaruhi sinyal asli bisa jadi sulit. Ingat contoh dari Bab Dua sehubungan dengan album rekaman yang tergores. Pada album, lonjakan impuls berhubungan dengan bunyi letupan dan klik keras yang dihasilkan saat album diputar dan dapat mengganggu kenikmatan musik bagi sebagian orang. Untuk contoh kedua dari kebisingan impuls, pertimbangkan apa yang terjadi ketika Anda mendengarkan radio AM saat terjadi badai petir. Sambaran petir di area tersebut menyebabkan gangguan listrik statis yang parah pada radio—sangat parah sehingga Anda tidak dapat mendengar transmisi radio secara normal.

Jika gangguan impuls mengganggu sinyal digital, seringkali sinyal digital asli dapat dikenali dan dipulihkan. Ketika noise benar-benar menghilangkan sinyal digital, sinyal asli tidak dapat diperoleh kembali (lihat Gambar 6-2).



Gambar 6-2 Pengaruh derau impuls pada sinyal digital

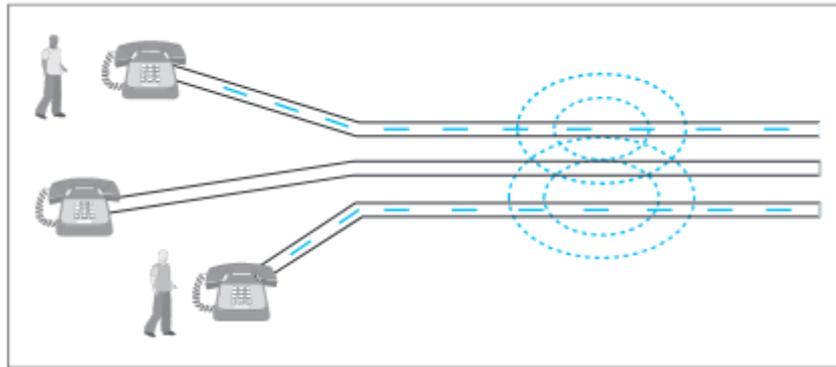
Kebisingan merupakan masalah bagi sinyal analog dan digital, dan kecepatan transmisi data dapat mempengaruhi signifikansi kebisingan. Faktanya, terkadang pengaruh kecepatan transmisi cukup dramatis dan dapat ditunjukkan dengan mudah. Gambar 6-3 menunjukkan transmisi sinyal digital pada kecepatan yang relatif lambat dan kecepatan yang relatif tinggi. Perhatikan pada gambar bahwa ketika kecepatan transmisi lebih lambat, Anda masih dapat menentukan nilai suatu sinyal, namun ketika kecepatan transmisi meningkat, Anda tidak dapat lagi menentukan apakah sinyalnya 0 atau 1.



Gambar 6-3 Kecepatan transmisi dan hubungannya dengan noise dalam sinyal digital

Crosstalk

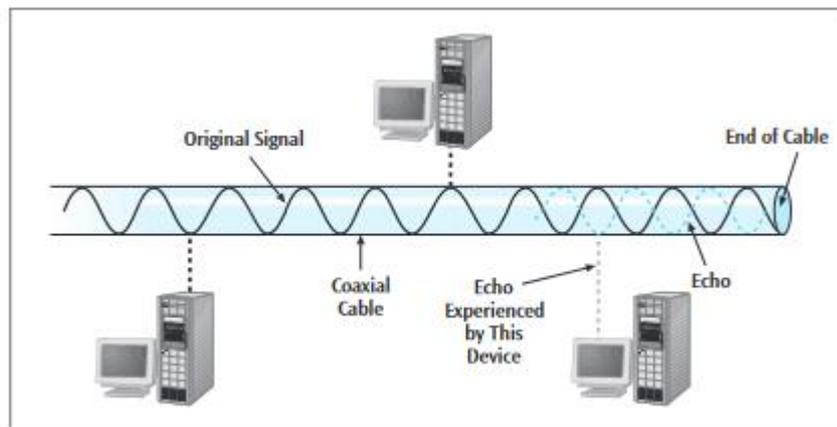
Crosstalk adalah penggabungan yang tidak diinginkan antara dua jalur sinyal yang berbeda. Kopling yang tidak diinginkan ini bisa bersifat elektrik, seperti yang mungkin terjadi antara dua set kabel berpasangan (seperti pada saluran telepon), atau bisa juga bersifat elektromagnetik (seperti ketika sinyal yang tidak diinginkan ditangkap oleh antena gelombang mikro). Crosstalk sinyal telepon merupakan masalah yang lebih umum terjadi 20 hingga 30 tahun yang lalu, sebelum perusahaan telepon menggunakan kabel serat optik dan kabel berpelindung baik lainnya. Ketika crosstalk terjadi selama percakapan telepon, Anda dapat mendengar percakapan telepon lain di latar belakang (Gambar 6-4). Kelembapan tinggi dan cuaca basah dapat menyebabkan peningkatan crosstalk listrik melalui sistem telepon. Meskipun crosstalk relatif terus menerus, hal ini dapat dikurangi dengan tindakan pencegahan dan perangkat keras yang tepat, seperti yang akan Anda lihat segera.



Gambar 6-4 Tiga rangkaian telepon mengalami crosstalk

Gema

Gema adalah umpan balik reflektif dari sinyal yang ditransmisikan saat sinyal bergerak melalui suatu media. Sama seperti suara yang bergema di ruangan kosong, sinyal dapat mengenai ujung kabel, memantul kembali melalui kabel, dan mengganggu sinyal aslinya. Kesalahan ini paling sering terjadi pada sambungan kabel atau pada ujung terbuka kabel koaksial. Gambar 6-5 menunjukkan sinyal memantul kembali dari ujung kabel dan menciptakan gema. Untuk meminimalkan efek gema, perangkat yang disebut penekan gema dapat dipasang pada saluran. Penekan gema pada dasarnya adalah filter yang memungkinkan sinyal lewat dalam satu arah saja. Untuk jaringan yang menggunakan kabel koaksial, filter kecil biasanya ditempatkan di ujung terbuka setiap kabel untuk menyerap sinyal yang masuk.

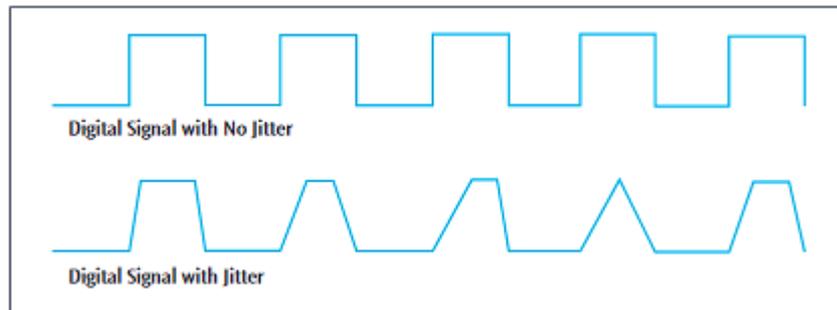


Gambar 6-5 Sinyal memantul kembali pada ujung kabel koaksial dan menyebabkan gema

Jitter

Jitter adalah hasil dari ketidakteraturan waktu kecil yang menjadi lebih besar selama transmisi sinyal digital saat sinyal diteruskan dari satu perangkat ke perangkat lainnya. Dengan kata lain, ketika sinyal digital sedang ditransmisikan, naik turunnya sinyal dapat mulai bergeser, atau menjadi kabur dan, dengan demikian, menghasilkan jitter. Jika tidak dicentang, jitter dapat menyebabkan perangkat video berkedip, transmisi audio berbunyi klik dan putus, dan data komputer yang dikirimkan datang dengan kesalahan. Jika jitter menjadi terlalu besar,

perbaikannya memerlukan perangkat transmisi untuk memperlambat laju transmisinya, yang pada gilirannya membatasi kinerja sistem secara keseluruhan. Gambar 6-6 menunjukkan contoh sederhana sinyal digital yang mengalami jitter.



Gambar 6-6 Sinyal digital asli dan sinyal digital dengan jitter

Penyebab jitter dapat mencakup interferensi elektromagnetik, crosstalk, melewati sinyal melalui terlalu banyak repeater, dan penggunaan peralatan berkualitas rendah. Solusi yang mungkin untuk masalah jitter melibatkan pemasangan pelindung yang tepat, yang dapat mengurangi atau menghilangkan interferensi elektromagnetik dan crosstalk, dan membatasi berapa kali sinyal diulang.

Atenuasi

Penyebab jitter dapat mencakup interferensi elektromagnetik, crosstalk, melewati sinyal melalui terlalu banyak repeater, dan penggunaan peralatan berkualitas rendah. Solusi yang mungkin untuk masalah jitter melibatkan pemasangan pelindung yang tepat, yang dapat mengurangi atau menghilangkan interferensi elektromagnetik dan crosstalk, dan membatasi berapa kali sinyal diulang.

Atenuasi adalah hilangnya kekuatan sinyal secara terus-menerus saat melewati suatu media. Ini belum tentu merupakan bentuk kesalahan tetapi secara tidak langsung dapat menyebabkan peningkatan kesalahan yang mempengaruhi sinyal yang dikirimkan. Seperti yang Anda pelajari di Bab Dua, redaman dapat dihilangkan dengan penggunaan amplifier untuk sistem analog atau repeater untuk sistem digital.

6.3 PENCEGAHAN KESALAHAN

Karena ada begitu banyak bentuk kebisingan dan kesalahan, dan karena kehadiran satu bentuk kebisingan atau lainnya dalam suatu sistem adalah suatu hal yang wajar, setiap sistem transmisi data harus mengambil tindakan pencegahan untuk mengurangi kebisingan dan kemungkinan kesalahan. Efek samping yang tidak menguntungkan dari kebisingan selama transmisi adalah stasiun pemancar harus memperlambat laju transmisinya. Oleh karena itu, ketika modem pertama kali membuat koneksi dengan modem lain, kedua modem tersebut ikut serta dalam negosiasi fallback. Artinya jika modem pengirim mengirim data dan data tiba dalam keadaan kacau, modem penerima mungkin meminta modem pengirim untuk kembali ke kecepatan transmisi yang lebih lambat. Perlambatan ini menciptakan sinyal dengan durasi bit masing-masing 0 dan 1 lebih lama—atau dalam kasus modulasi amplitudo kuadratur,

diagram konstelasi yang memiliki lebih sedikit level atau target diskrit—sehingga memberikan peluang lebih besar bagi penerima untuk membedakannya. nilai dari yang berikutnya, bahkan di hadapan kebisingan. Namun, jika Anda dapat mengurangi kemungkinan kebisingan sebelum terjadi, stasiun pemancar mungkin tidak perlu memperlambat aliran transmisinya.

Anda dapat mencegah terjadinya berbagai jenis kesalahan transmisi dengan menerapkan teknik pencegahan kesalahan yang tepat, termasuk yang tercantum di sini:

- Pasang kabel dengan pelindung yang tepat untuk mengurangi interferensi elektromagnetik dan crosstalk.
- Sadarilah bahwa banyak jenis aplikasi nirkabel yang menggunakan frekuensi nirkabel yang sama. Bahkan beberapa perangkat non-nirkabel menghasilkan sinyal yang dapat mengganggu aplikasi nirkabel. Misalnya, oven microwave dapat mengganggu beberapa sinyal LAN nirkabel.
- Mengganti peralatan lama dengan peralatan digital yang lebih modern; walaupun awalnya mahal, teknik ini seringkali merupakan cara yang paling hemat biaya untuk meminimalkan kesalahan transmisi dalam jangka panjang.
- Gunakan repeater digital dan amplifier analog dalam jumlah yang tepat untuk meningkatkan kekuatan sinyal, sehingga mengurangi kemungkinan kesalahan.
- Perhatikan kapasitas media yang dinyatakan, dan, untuk mengurangi kemungkinan kesalahan, hindari mendorong kecepatan transmisi melampaui batas yang disarankan. Misalnya, ingat dari Bab Dua bahwa kabel twisted pair Kategori 5e/6 tidak boleh lebih panjang dari jarak 100 meter (300 kaki) yang disarankan saat transmisi pada 100 Mbps.

Mengurangi jumlah perangkat, mengurangi panjang kabel, dan mengurangi kecepatan transmisi data juga dapat menjadi cara efektif untuk mengurangi kemungkinan kesalahan. Meskipun pilihan seperti ini tidak selalu diinginkan, terkadang pilihan tersebut merupakan alternatif paling masuk akal yang tersedia. Tabel 6-1 mencantumkan berbagai jenis kesalahan yang dapat timbul dan mencakup satu atau lebih kemungkinan teknik pencegahan kesalahan untuk setiap kesalahan tersebut.

Tabel 6-1 Ringkasan kesalahan dan teknik pencegahan kesalahan

Jenis Kesalahan	Teknik Pencegahan Kesalahan
Kebisingan putih	Pasang filter khusus untuk sinyal analog; menerapkan regenerasi sinyal digital untuk sinyal digital
Kebisingan impuls	Pasang filter khusus untuk sinyal analog; menerapkan pemrosesan sinyal digital untuk sinyal digital
Crosstalk	Pasang pelindung yang tepat pada kabel
Gema	Pasang terminasi kabel yang benar
Jitter	Gunakan sirkuit elektronik berkualitas lebih baik, gunakan lebih sedikit repeater, perlambat kecepatan transmisi
Attenuasi	Pasang perangkat yang memperkuat sinyal analog; menerapkan regenerasi sinyal digital sinyal digital

**Bukan jenis kesalahan, namun secara tidak langsung mempengaruhi kesalahan*

Jangan terpancing untuk berpikir bahwa hanya karena berbagai teknik pencegahan kesalahan telah diterapkan, maka kesalahan tidak akan terjadi. Metode deteksi kesalahan yang tepat masih perlu diterapkan. Mari kita periksa teknik deteksi kesalahan utama selanjutnya.

6.4 DETEKSI KESALAHAN

Meskipun upaya pencegahan terbaik telah dilakukan, kesalahan masih saja terjadi. Karena sebagian besar data yang ditransfer melalui jalur komunikasi penting, biasanya diperlukan penerapan teknik deteksi kesalahan pada data yang diterima untuk memastikan bahwa tidak ada kesalahan yang terjadi pada data selama transmisi. Jika kesalahan terdeteksi, respons umumnya adalah melakukan beberapa jenis permintaan transmisi.

Deteksi kesalahan dapat dilakukan di beberapa tempat dalam model komunikasi. Salah satu tempat paling umum adalah lapisan data link. Saat perangkat membuat bingkai data pada lapisan data link, perangkat tersebut menyisipkan beberapa jenis kode pendeteksi kesalahan. Ketika frame tiba di perangkat berikutnya dalam urutan transmisi, penerima mengekstrak kode deteksi kesalahan dan menerapkannya ke frame data. Kemudian, bingkai data direkonstruksi dan dikirim ke perangkat berikutnya dalam urutan transmisi. Beberapa protokol melakukan rutin deteksi kesalahan di tujuan akhir. Seperti yang kita lihat di Bab Satu, TCP melakukan deteksi kesalahan pada titik akhir koneksi.

Terlepas dari dimana deteksi kesalahan diterapkan, semua sistem masih menyadari pentingnya memeriksa kesalahan transmisi. Teknik pendeteksian kesalahan itu sendiri bisa relatif sederhana atau rumit. Seperti yang Anda duga, teknik sederhana tidak memberikan tingkat pengecekan kesalahan yang sama seperti skema yang lebih rumit. Misalnya, teknik deteksi kesalahan yang paling sederhana adalah paritas sederhana, yang menambahkan satu bit ke karakter data, namun menangkap jumlah kesalahan paling sedikit. Di ujung lain spektrum adalah teknik yang paling rumit dan efektif yang ada saat ini: cyclic redundancy checksum. Checksum redundansi siklik tidak hanya lebih kompleks daripada paritas sederhana, biasanya menambahkan 8 hingga 32 bit pemeriksaan kode pendeteksi kesalahan ke dalam blok data, ini adalah teknik pendeteksi kesalahan paling efektif yang pernah dirancang. Mari kita periksa empat teknik deteksi kesalahan dan evaluasi kekuatan dan kelemahan masing-masing teknik.

Pemeriksaan paritas

Seperti yang kita lihat di Bab Satu, TCP melakukan deteksi kesalahan pada titik akhir koneksi. Terlepas dari dimana deteksi kesalahan diterapkan, semua sistem masih menyadari pentingnya memeriksa kesalahan transmisi. Teknik pendeteksian kesalahan itu sendiri bisa relatif sederhana atau rumit. Seperti yang Anda duga, teknik sederhana tidak memberikan tingkat pengecekan kesalahan yang sama seperti skema yang lebih rumit. Misalnya, teknik deteksi kesalahan yang paling sederhana adalah paritas sederhana, yang menambahkan satu bit ke karakter data, namun menangkap jumlah kesalahan paling sedikit. Di ujung lain spektrum adalah teknik yang paling rumit dan paling efektif yang ada saat ini: cyclic redundancy checksum. Checksum redundansi siklik tidak hanya lebih kompleks daripada paritas

sederhana, biasanya menambahkan 8 hingga 32 bit pemeriksaan kode pendeteksi kesalahan ke dalam blok data, ini adalah teknik pendeteksi kesalahan paling efektif yang pernah dirancang. Mari kita periksa empat teknik deteksi kesalahan dan evaluasi kekuatan dan kelemahan masing-masing teknik.

Teknik pendeteksian kesalahan yang paling dasar adalah pemeriksaan paritas, yang biasanya digunakan dengan koneksi asynchronous. Meskipun ada berbagai bentuk pemeriksaan paritas karakter tunggal, satu fakta tetap ada: Pemeriksaan paritas membiarkan terlalu banyak kesalahan lolos tanpa terdeteksi. Karena alasan ini saja, pemeriksaan paritas jarang, atau bahkan pernah, digunakan pada transmisi data serius apa pun. Meskipun demikian, dua bentuk pemeriksaan paritas—paritas sederhana dan paritas longitudinal—masih ada dan layak untuk dikaji.

Paritas Sederhana

Paritas sederhana (kadang-kadang dikenal sebagai pemeriksaan redundansi vertikal) adalah metode deteksi kesalahan yang paling mudah untuk dimasukkan ke dalam sistem transmisi. Muncul dalam dua bentuk dasar: paritas genap dan paritas ganjil. Konsep dasar pengecekan paritas adalah bahwa sebuah bit ditambahkan ke dalam rangkaian bit untuk menghasilkan paritas genap atau paritas ganjil. Dengan paritas genap, 0 atau 1 yang ditambahkan ke string menghasilkan bilangan biner 1 yang genap. Dengan paritas ganjil, 0 atau 1 yang ditambahkan ke string menghasilkan bilangan biner 1 yang ganjil. Jika rangkaian karakter ASCII 7-bit digunakan, bit paritas ditambahkan sebagai bit kedelapan. Misalkan, misalnya, karakter “k”—yaitu 1101011 dalam biner—ditransmisikan dan paritas genap diterapkan. Dalam hal ini, bit paritas 1 akan ditambahkan ke akhir aliran bit, sebagai berikut: 11010111. Sekarang ada bilangan genap (enam) dari 1s. (Jika paritas ganjil digunakan, angka 0 akan ditambahkan di akhir, menghasilkan 11010110.)

Sekarang, jika kesalahan transmisi menyebabkan salah satu bit terbalik (nilainya secara keliru ditafsirkan sebagai 0 bukannya 1, atau sebaliknya), kesalahan tersebut dapat dideteksi jika penerima memahami bahwa ia perlu memeriksa paritas genap. . Kembali ke contoh karakter “k” yang dikirim dengan paritas genap, jika mengirim 11010111 tetapi 01010111 diterima, penerima akan menghitung angka 1, melihat ada angka ganjil, dan mengetahui ada kesalahan.

Apa yang terjadi jika 11010111 dengan paritas genap dikirim dan dua bit rusak? Misalnya, 00010111 diterima. Apakah kesalahan akan terdeteksi? Jawabannya tidak, error tidak akan terdeteksi karena angka 1 masih genap. Paritas sederhana hanya dapat mendeteksi jumlah bit yang salah per karakternya ganjil. Mungkinkah lebih dari satu bit dalam satu karakter diubah akibat kesalahan transmisi? Ya. Kesalahan bit tunggal yang terisolasi terjadi 50 hingga 60 persen. Semburan kesalahan, di mana dua bit yang salah dipisahkan oleh kurang dari 10 bit yang tidak rusak, terjadi 10 hingga 20 persen.

Perhatikan bahwa ketika rangkaian karakter ASCII 7-bit digunakan, bit paritas ditambahkan untuk setiap 7 bit data, menghasilkan rasio bit paritas terhadap bit data 1:7. Dengan demikian, paritas sederhana menghasilkan rasio bit pemeriksaan terhadap bit data

yang relatif tinggi, namun hanya mencapai hasil deteksi kesalahan yang biasa-biasa saja (50 persen).

Paritas Longitudinal

Paritas longitudinal, terkadang disebut pemeriksaan redundansi longitudinal atau paritas horizontal, mencoba memecahkan kelemahan utama paritas sederhana—bahwa semua kesalahan dalam jumlah genap tidak terdeteksi. Untuk memberikan tingkat perlindungan ekstra ini, paritas longitudinal perlu menggunakan bit pemeriksa paritas tambahan, seperti yang akan Anda lihat segera. Langkah pertama skema paritas ini melibatkan pengelompokan karakter individu dalam satu blok, seperti yang ditunjukkan pada Tabel 6-2. Setiap karakter (disebut juga baris) dalam blok mempunyai bit paritasnya sendiri. Selain itu, setelah sejumlah karakter tertentu dikirim, deretan bit paritas, atau pemeriksaan karakter blok, juga dikirimkan. Setiap bit paritas pada baris terakhir ini merupakan pemeriksaan paritas untuk semua bit pada kolom di atasnya. Jika satu bit diubah pada Baris 1, bit paritas pada akhir Baris 1 menandakan adanya kesalahan. Selain itu, bit paritas untuk kolom terkait juga menandakan adanya kesalahan. Jika dua bit pada Baris 1 dibalik, pemeriksaan paritas Baris 1 tidak akan menandakan kesalahan, namun pemeriksaan paritas dua kolom akan menandakan kesalahan. Ini adalah bagaimana paritas longitudinal mampu mendeteksi lebih banyak kesalahan dibandingkan paritas sederhana. Namun perlu diperhatikan bahwa jika 2 bit dibalik pada Baris 1 dan 2 bit dibalik pada Baris 2, dan kesalahan terjadi pada kolom yang sama, tidak ada kesalahan yang terdeteksi. Skenario ini, yang ditunjukkan pada Tabel 6-3, merupakan batasan paritas longitudinal.

Tabel 6-2 Contoh sederhana paritas memanjang

	Data							Parity
Baris 1	1	1	0	1	0	1	1	1
Baris 2	1	1	1	1	1	1	1	1
Baris 3	0	1	0	1	0	1	0	1
Baris 4	0	0	1	1	0	0	1	1
Baris Parity	0	1	0	0	1	1	1	0

Tabel 6-3 Bit kedua dan ketiga pada Baris 1 dan 2 mempunyai kesalahan, namun paritas longitudinal tidak mendeteksi kesalahan tersebut

	Data							Parity
Baris 1	1	±0	±1	1	0	1	1	1
Baris 2	1	±0	±0	1	1	1	1	1
Baris 3	0	1	0	1	0	1	0	1
Baris 4	0	0	1	1	0	0	1	1
Baris Parity	0	1	0	0	1	1	1	0

Meskipun paritas longitudinal memberikan tingkat perlindungan ekstra dengan menggunakan pemeriksaan paritas ganda, metode ini, seperti paritas sederhana, juga

memperkenalkan jumlah bit pemeriksaan yang tinggi dibandingkan dengan bit data, dengan hanya sedikit lebih baik daripada hasil deteksi kesalahan yang biasa-biasa saja. Jika n karakter dalam satu blok dikirimkan, rasio bit pemeriksaan terhadap bit data adalah $n+8:7n$. Dengan kata lain, untuk mengirimkan blok data 20 karakter, misalnya, bit paritas sederhana perlu ditambahkan ke masing-masing 20 karakter, ditambah pemeriksaan karakter blok 8-bit penuh ditambahkan di akhir, menghasilkan rasio dari bit pemeriksaan ke bit data yaitu 28:140, atau 1:5.

Checksum aritmatika

Banyak protokol tingkat tinggi yang digunakan di Internet (seperti TCP dan IP) menggunakan bentuk deteksi kesalahan di mana karakter yang akan dikirim “dijumlahkan” bersama-sama. Jumlah ini kemudian ditambahkan ke akhir pesan dan pesan dikirimkan ke pihak penerima. Penerima menerima pesan yang dikirimkan dan melakukan operasi penjumlahan yang sama, dan pada dasarnya membandingkan jumlahnya dengan jumlah yang dihasilkan oleh pemancar. Jika kedua jumlah tersebut cocok, maka tidak terjadi kesalahan selama transmisi. Jika kedua jumlah tersebut tidak sesuai, penerima memberitahukan pemancar bahwa telah terjadi kesalahan. Karena penjumlahan dihasilkan dengan melakukan aritmatika yang relatif sederhana, teknik ini sering disebut checksum aritmatika. Lebih tepatnya, mari kita perhatikan contoh berikut. Misalkan kita ingin menyampaikan pesan “Ini keren.” Dalam ASCII (dari Bab Dua), pesan tersebut akan muncul dalam biner sebagai: 1010100 1101000 1101001 1110011 0100000 1101001 1110011 0100000 1100011 1101111 1101111 1101100 010111 0. (Jangan lupa spasi antara kata dan titik di akhir kalimat.)

TCP dan IP sebenarnya menambahkan nilai-nilai ini dalam biner untuk membuat jumlah biner. Namun penambahan biner pada begitu banyak operan cukup berantakan. Agar kita tidak perlu menjumlahkan semua nilai biner ini, mari kita ubah nilai biner tersebut ke bentuk desimalnya. Jika Anda tidak mengetahui biner, kami akan melakukannya untuk Anda. Nilai biner pertama—1010100—adalah nilai 84 dalam desimal. 1101000 sama dengan 104. Nilai biner berikutnya 1101001 sama dengan 105; 1110011 sama dengan 115; 0100000 sama dengan 32; 1101001 sama dengan 105; 1110011 sama dengan 115; 0100000 sama dengan 32; 1100011 sama dengan 99; 1101111 sama dengan 111; 1101111, sekali lagi, adalah 111; 1101100 sama dengan 108; dan 0101110 sama dengan 46. Jika kita menjumlahkan kolom nilai ini, kita akan mendapatkan yang berikut:

84
104
105
115
32
105
115
32
99
111
111

$$\begin{array}{r} 108 \\ + 46 \\ \hline 1167 \end{array}$$

Jumlah 1167 kemudian ditambahkan ke pesan keluar dan dikirim ke penerima. Penerima akan mengambil karakter yang sama, menambahkan nilai ASCII-nya, dan jika tidak ada kesalahan selama transmisi, akan mendapatkan jumlah yang sama yaitu 1167. Sekali lagi, penghitungan dalam TCP dan IP dilakukan dalam biner dengan sedikit lebih rumit, namun semoga anda mendapatkan idenya.

Checksum aritmatika relatif mudah untuk dihitung dan melakukan pekerjaan yang cukup baik dalam mendeteksi kesalahan. Jelasnya, jika kebisingan sedikit mengganggu selama transmisi, kemungkinan besar penerima tidak akan mendapatkan jumlah yang sama. Bisa dibayangkan jika planet dan bintang berada dalam posisi yang tepat, kita bisa “menurunkan” nilai satu karakter sambil “menaikkan” nilai karakter kedua dengan sempurna sehingga hasilnya sama persis. Namun kemungkinan hal itu terjadi kecil. Meskipun demikian, hal ini membuat kita bertanya-tanya apakah ada metode pendeteksi kesalahan lain yang peluangnya sangat kecil sehingga hampir tidak ada kesalahan yang bisa lolos dari deteksi. Memang ada: checksum redundansi siklik.

Checksum redundansi siklik

Berbeda dengan teknik deteksi kesalahan paritas sederhana dan paritas longitudinal, yang menghasilkan rasio bit pemeriksaan terhadap bit data yang tinggi dengan hasil deteksi kesalahan yang biasa-biasa saja, metode cyclic redundancy checksum (CRC), atau cyclic checksum, biasanya menambahkan 8 hingga 32 bit pemeriksaan. terhadap paket data yang berpotensi besar dan menghasilkan kemampuan deteksi kesalahan mendekati 100 persen.

Metode deteksi kesalahan CRC memperlakukan paket data yang akan dikirim (pesan) sebagai polinomial besar. Bit data paling kanan menjadi suku x^0 , bit data berikutnya di sebelah kiri menjadi suku x^1 , dan seterusnya. Jika bit dalam pesan adalah 1, suku polinomial yang sesuai akan disertakan. Jadi, data 101001101 akan setara dengan polinomial:

x^8		$+ x^6$			$+ x^3$	$+ x^2$		$+ x^0$
1	0	1	0	0	1	1	0	1

(Karena nilai apa pun yang dipangkatkan 0 adalah 1, suku x^0 selalu ditulis sebagai 1.) Pemancar mengambil polinomial pesan ini dan, dengan menggunakan aritmatika polinomial, membaginya dengan polinomial penghasil tertentu, dan menghasilkan hasil bagi dan sisa. Hasil bagi dibuang, namun sisanya (dalam bentuk bit) ditambahkan ke akhir polinomial pesan asli, dan unit gabungan ini ditransmisikan melalui media. Ketika data ditambah sisanya tiba di tujuan, polinomial pembangkit yang sama digunakan untuk mendeteksi kesalahan. Polinomial pembangkit adalah string bit yang disetujui industri yang digunakan untuk membuat sisa checksum siklik. Beberapa polinomial pembangkit yang umum digunakan secara luas meliputi:

CRC – 12	$x^{12} + x^{11} + x^3 + x^2 + x + 1$
CRC – 16	$x^{16} + x^{15} + x^2 + 1$
CRC – CCITT	$x^{16} + x^{15} + x^5 + 1$
CRC – 32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$
Transfer Asinkronus model CRC	$x^8 + x^2 + x + 1$

Penerima membagi data yang masuk (polinomial pesan asli ditambah sisanya) dengan polinomial pembangkit yang sama persis dengan yang digunakan oleh pemancar. Jika tidak ada kesalahan yang terjadi selama transmisi data, pembagian akan menghasilkan sisa nol. Jika terjadi kesalahan selama transmisi, polinomial pesan asli yang diterima ditambah sisanya tidak akan terbagi rata dengan polinomial pembangkit dan akan menghasilkan sisa bukan nol, menandakan kondisi kesalahan.

Dalam kehidupan nyata, pemancar dan penerima tidak melakukan pembagian polinomial dengan perangkat lunak. Sebaliknya, perangkat keras yang dirancang ke dalam sirkuit terintegrasi dapat melakukan penghitungan lebih cepat.

Metode CRC hampir sangat mudah dilakukan. Tabel 6-4 merangkum kinerja teknik CRC. Dalam kasus dimana ukuran ledakan kesalahan kurang dari $r + 1$, dimana r adalah derajat polinomial pembangkit, deteksi kesalahan adalah 100 persen. Misalnya, CRC-CCITT digunakan, sehingga derajat, atau pangkat tertinggi, polinomialnya adalah 16. Dalam kasus ini, jika ledakan kesalahan kurang dari $r + 1$ atau panjangnya 17 bit, CRC akan mendeteksinya. . Hanya pada kasus dimana error burst lebih besar atau sama dengan $r + 1$ bit panjangnya maka ada kemungkinan CRC tidak dapat mendeteksi error tersebut. Peluang atau peluang terjadinya error burst berukuran $r + 1$ terdeteksi adalah $1 - (\frac{1}{2})^{(r-1)}$. Dengan asumsi lagi bahwa $r = 16$, $1 - (\frac{1}{2})^{(16-1)}$ sama dengan $1 - 0,0000305$, yang sama dengan 0,999969. Dengan demikian, probabilitas terdeteksinya kesalahan besar sangat mendekati 1,0 (100 persen).

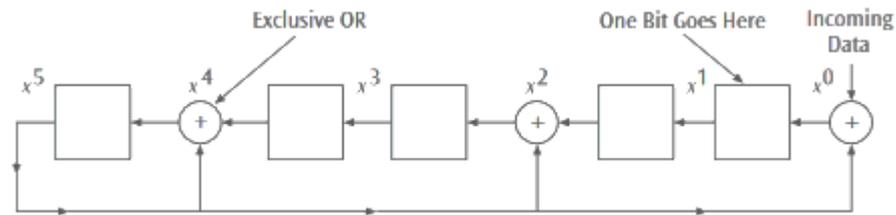
Tabel 6-4 Kinerja deteksi kesalahan checksum redundansi siklik

Jenis Kesalahan	Kinerja Deteksi Kesalahan
Kesalahan Bit Tunggal	100 %
Kesalahan Bit Ganda	100 %, selama polinomial yang menghasilkan setidaknya memiliki tiga angka 1 (semuanya memiliki angka 1)
Jumlah Bit Ganjil dalam Error	100 %, selama polinomial pembangkit mengandung faktor $x + 1$
Panjang Error Burst < $r + 1$	100 %
Panjang Error Burst = $r + 1$	Probabilitas $1 - (\frac{1}{2})^{r-1}$ (sangat mendekati 100%)
Panjang Error Burst > $r + 1$	Probabilitas $1 - (\frac{1}{2})^r$ (sangat mendekati 100%)

Perhitungan Checksum Redundansi Siklik

Perangkat keras melakukan proses pembagian polinomial dengan sangat cepat. Perangkat keras dasar yang digunakan untuk melakukan perhitungan CRC adalah register sederhana yang menggeser semua bit data ke kiri setiap kali bit baru dimasukkan. Fitur unik dari register geser ini adalah bit paling kiri dalam register diumpungkan kembali ke titik-titik

tertentu. Pada titik ini, nilai bit umpan balik ini adalah OR eksklusif dengan bit bergeser ke kiri dalam register (untuk rincian lebih lanjut tentang operasi OR eksklusif, silakan lihat pendamping daring siswa yang menyertai buku ini). Gambar 6-7 menunjukkan skema register geser yang digunakan untuk CRC. Anda dapat melihat dari gambar bahwa jika terdapat suku dalam polinomial pembangkit, terdapat OR eksklusif (ditunjukkan dengan tanda tambah dalam lingkaran) di antara dua kotak shift yang berurutan. Saat bit data memasuki register geser (digeser dari kanan), semua bit bergeser satu posisi ke kiri. Sebelum sedikit bergeser ke kiri, jika ada OR eksklusif yang akan digeser, bit paling kiri yang saat ini disimpan dalam register geser membungkus dan di-OR eksklusif dengan bit yang bergeser. Tabel 6-5 menunjukkan contoh pembuatan CRC menggunakan pesan 1010011010 dan polinomial penghasil $x^5 + x^4 + x^2 + 1$, yang bukan merupakan polinomial penghasil standar namun dibuat untuk contoh yang disederhanakan ini.



Tabel 6-5 Contoh pembangkitan CRC dengan metode shift register

	0	⊕	0		0	⊕	0		0	⊕	Data Masuk
	0		0		0		0		1		1
	0		0		0		1		0		0
	0		0		1		0		1		1
	0		1		0		1		0		0
	1		0		1		0		0		0
	1		1		1		0		0		1
	0		1		1		0		0		1
	1		1		0		0		0		0
	0		0		1		0		0		1
	0		1		0		0		0		0
	1		0		0		0		0		0
	1		0		1		0		1		0
	1		1		1		1		1		0
	0		1		0		1		1		0
Pengingat	1		0		1		1		0		0

} r 0s

Ingatlah bahwa pemeriksaan paritas, tergantung pada apakah paritas sederhana atau paritas longitudinal, hanya dapat mendeteksi antara 50 persen dan sekitar 80 persen kesalahan. Anda dapat melakukan perhitungan paritas manual dengan cukup cepat, namun metode perangkat keras checksum redundansi siklik juga cukup cepat. Seperti yang Anda lihat sebelumnya, skema paritas memerlukan sejumlah besar bit pemeriksaan per bit data.

Sebaliknya, checksum redundansi siklik memerlukan sejumlah bit pemeriksaan berukuran sisa (8, 16, atau 32—seperti yang Anda lihat dari daftar penghasil polinomial) ditambahkan ke pesan. Panjang pesannya sendiri bisa ratusan hingga ribuan bit. Oleh karena itu, jumlah bit pemeriksaan per bit data dalam redundansi siklik bisa jadi relatif rendah.

Checksum redundansi siklik adalah teknik pendeteksi kesalahan yang sangat ampuh dan harus dipertimbangkan secara serius untuk semua sistem transmisi data. Memang benar, semua jaringan area lokal menggunakan teknik CRC (CRC-32 ditemukan di LAN Ethernet) dan banyak protokol jaringan area luas yang menggunakan checksum siklik. Sekarang setelah kita memahami teknik dasar pendeteksian kesalahan, mari kita lihat apa yang terjadi setelah kesalahan terdeteksi.

6.5 KONTROL KESALAHAN

Setelah kesalahan dalam aliran transmisi data yang diterima terdeteksi, apa yang akan dilakukan penerima? Tindakan yang dilakukan penerima disebut pengendalian kesalahan, yang pada dasarnya melibatkan pengambilan salah satu dari tiga tindakan:

- Lemparkan bingkai/paketnya.
- Mengembalikan pesan ke pemancar yang memintanya mengirim ulang paket data yang mengalami kesalahan.
- Perbaiki kesalahan tanpa transmisi ulang.

Mari kita periksa masing-masing opsi ini secara lebih rinci.

Lemparkan bingkai/paketnya

Opsi pengendalian kesalahan yang pertama—melempar bingkai/paket—hampir tidak tampak seperti sebuah opsi sama sekali. Namun membuang frame/paket untuk pengendalian kesalahan menjadi mode operasi untuk beberapa teknik transmisi jaringan area luas yang lebih baru. Misalnya, frame relay, yang baru ada sejak tahun 1994 dan ditawarkan oleh perusahaan telepon untuk mentransfer data melalui area yang luas, mendukung pendekatan “toss the frame” untuk pengendalian kesalahan. Jika frame data tiba di saklar frame relay dan kesalahan terdeteksi setelah checksum siklik dilakukan, frame tersebut akan dibuang begitu saja. Alasan di balik tindakan ini ada dua. Jaringan frame relay dibuat terutama dari kabel serat optik. Karena kabel serat optik adalah media yang paling tidak rentan terhadap kesalahan, diasumsikan bahwa tingkat kesalahannya rendah dan pengendalian kesalahan tidak diperlukan. Jika suatu frame mengalami kesalahan dan dibuang, frame relay mengasumsikan bahwa lapisan transport atau aplikasi lapisan yang lebih tinggi menggunakan frame relay untuk mengirimkan data akan melacak frame tersebut dan akan mengetahui bahwa frame telah dibuang. Lapisan yang lebih tinggi kemudian bertanggung jawab untuk meminta agar frame yang dijatuhkan dikirimkan kembali.

Perhatikan contoh di mana sebuah perusahaan memiliki aplikasi database yang mengirimkan catatan database ke seluruh negara antara dua lokasi perusahaan. Aplikasi database (pada lapisan aplikasi) menggunakan frame relay pada lapisan data link untuk mentransfer catatan sebenarnya. Jika rekaman atau bagian dari rekaman dijatuhkan oleh frame relay karena kesalahan transmisi, frame relay tidak menginformasikan aplikasi.

Sebaliknya, aplikasi database harus melacak semua record yang dikirim dan diterima, dan jika satu record tidak sampai di tujuan, aplikasi database harus meminta transmisi ulang.

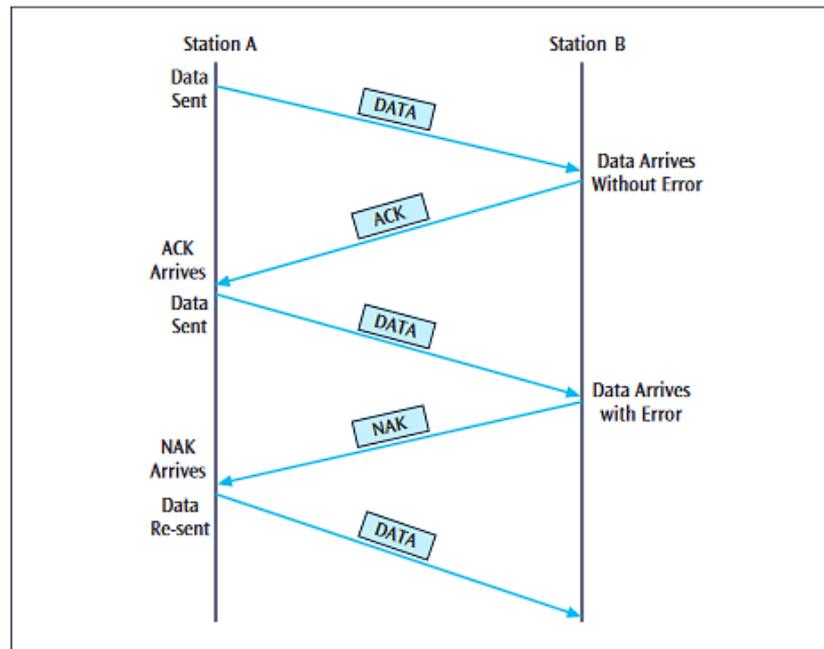
Kembalikan pesan

Opsi kedua—mengirim pesan kembali ke pemancar—mungkin merupakan bentuk pengendalian kesalahan yang paling umum. Mengembalikan pesan juga merupakan salah satu teknik pengendalian kesalahan pertama yang dikembangkan dan terkait erat dengan teknik pengendalian aliran tertentu. Ingat dari Bab Satu bahwa kontrol aliran adalah proses yang menjaga pemancar agar tidak mengirimkan terlalu banyak data ke penerima, sehingga buffer penerima meluap. Selama bertahun-tahun, dua versi dasar pengendalian kesalahan pengembalian pesan telah muncul: Stop-and-wait dan jendela geser. Mari kita lihat kontrol kesalahan Stop-and-wait terlebih dahulu.

Kontrol Kesalahan Berhenti-dan-Tunggu

Kontrol kesalahan stop-and-wait adalah teknik yang biasanya dikaitkan dengan protokol kontrol aliran stop-and-wait. Protokol ini dan teknik pengendalian kesalahannya adalah yang tertua, paling sederhana, dan karenanya paling ketat. Sebuah stasiun kerja (Stasiun A) mengirimkan satu paket data ke stasiun kerja lain (Stasiun B), lalu berhenti dan menunggu balasan dari Stasiun B. Ada empat hal yang dapat terjadi pada saat ini. Pertama, jika paket data tiba tanpa kesalahan, Stasiun B merespons dengan pengakuan positif, seperti ACK. (ACK adalah salah satu kode kontrol dalam rangkaian karakter ASCII dan diperkenalkan pada masa awal sistem transmisi Stop-and-wait.) Ketika Stasiun A menerima ACK, ia mengirimkan paket data berikutnya. Kedua, jika data datang dengan kesalahan, Stasiun B merespons dengan pengakuan negatif, seperti NAK atau REJ (untuk penolakan). Jika Stasiun A menerima NAK, ia akan mengirim ulang paket data sebelumnya. Gambar 6-8 menunjukkan contoh transaksi tersebut.

Ketiga, paket tiba di Stasiun B dalam keadaan tidak rusak, Stasiun B mengirimkan ACK, namun ACK tersebut hilang atau rusak. Karena Stasiun A harus menunggu suatu bentuk pengakuan, maka Stasiun A tidak akan dapat mengirimkan paket lagi. Setelah jangka waktu tertentu (disebut timeout), Stasiun A mengirim ulang paket terakhir. Namun sekarang jika paket ini tiba tanpa kerusakan di Stasiun B, Stasiun B tidak akan mengetahui bahwa paket tersebut adalah paket yang sama dengan paket terakhir yang diterima. Untuk menghindari kebingungan ini, paket-paket tersebut diberi nomor 0, 1, 0, 1, dan seterusnya. Jika Stasiun A mengirimkan paket 0, dan ACK untuk paket 0 hilang, Stasiun A akan mengirim ulang paket 0.



Gambar 6-8 Contoh dialog menggunakan kontrol kesalahan Stop-and-wait

Stasiun B akan melihat dua paket 0 berturut-turut (asli dan duplikat) dan menyimpulkan bahwa ACK dari paket 0 pertama telah hilang.

Keempat, Stasiun A mengirimkan paket, namun paket tersebut hilang. Karena paket tidak sampai di Stasiun B, Stasiun B tidak akan mengembalikan ACK. Karena Station A tidak menerima ACK, maka time out dan mengirim ulang paket sebelumnya. Misalnya, Stasiun A mengirimkan paket 1, kehabisan waktu, dan mengirim ulang paket 1. Jika paket 1 ini tiba di Stasiun B, Stasiun B merespons dengan ACK. Bagaimana Station A mengetahui apakah ACK menerima paket pertama atau kedua? Untuk menghindari kebingungan, ACK diberi nomor, sama seperti paketnya. Berbeda dengan paket (yang diberi nomor 0, 1, 0, 1, dan seterusnya), ACK diberi nomor 1, 0, 1, 0, dan seterusnya. Jika Stasiun B menerima paket 0, ia merespons dengan ACK1. ACK1 memberitahu Stasiun A bahwa paket berikutnya yang diharapkan adalah paket 1. Karena paket 0 baru saja tiba, maka paket 1 diharapkan berikutnya.

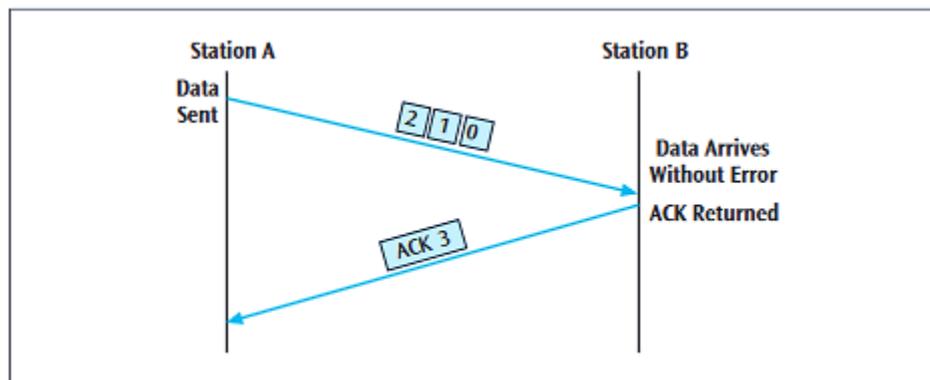
Salah satu kelemahan paling serius dari pengendalian kesalahan Stop-and-wait yang sederhana adalah tingkat inefisiensinya yang tinggi. Kontrol kesalahan stop-and-wait adalah protokol setengah dupleks, yang berarti hanya satu stasiun yang dapat mengirimkan pada satu waktu. Waktu yang terbuang oleh stasiun pemancar untuk menunggu pengakuan dapat lebih baik digunakan untuk mengirimkan paket tambahan. Tersedia teknik yang lebih efisien daripada Stop-and-wait. Salah satu protokol tersebut adalah teknik jendela geser.

Kontrol Kesalahan Jendela Geser

Kontrol kesalahan jendela geser didasarkan pada protokol jendela geser, yang merupakan skema kontrol aliran yang memungkinkan stasiun mengirimkan sejumlah paket data pada satu waktu sebelum menerima beberapa bentuk pengakuan. Protokol jendela geser telah ada sejak tahun 1970an, saat jaringan komputer mempunyai dua keterbatasan penting. Pertama, kecepatan jalur dan kekuatan pemrosesan jauh lebih rendah dibandingkan saat ini.

Oleh karena itu, stasiun pengirim data harus tidak mengirimkan data terlalu cepat dan membebani stasiun penerima. Kedua, memori lebih mahal, sehingga perangkat jaringan memiliki ruang buffer terbatas untuk menyimpan paket data masuk dan keluar. Karena keterbatasan ini, protokol jendela geser standar menetapkan ukuran jendela maksimumnya menjadi tujuh paket. Sebuah stasiun yang memiliki ukuran jendela maksimum 7 (seperti yang dimiliki beberapa sistem awal) hanya dapat mengirimkan tujuh paket data pada satu waktu sebelum harus berhenti dan menunggu pengakuan. Karena ukuran jendela 7 kecil, protokol jendela geser yang diperluas segera dibuat yang dapat mendukung 127 paket. Saat ini, protokol TCP yang digunakan di Internet dapat secara dinamis menyesuaikan ukuran jendelanya menjadi ribuan untuk kinerja optimal. Untuk mempermudah, contoh berikut akan mempertimbangkan protokol standar dengan ukuran jendela maksimum 7.

Untuk mengikuti aliran data dalam protokol jendela geser dengan ukuran jendela 7, paket diberi nomor 0, 1, 2, 3, 4, 5, 6, dan 7. Setelah paket nomor 7 dikirimkan, pengurutan nomor dimulai kembali pada 0. Meskipun paket diberi nomor 0 hingga 7, yang sesuai dengan delapan paket berbeda, hanya tujuh paket data yang dapat beredar (tidak diakui) pada satu waktu. (Alasannya akan segera terlihat.) Karena maksimal tujuh paket data dapat dikirimkan pada satu waktu, dua paket data dengan nomor yang sama (misalnya, keduanya bernomor 4) tidak akan pernah dapat dikirim pada waktu yang sama. . Jika pengirim mempunyai ukuran jendela maksimum 7 dan mengirimkan empat paket, pengirim masih dapat mengirimkan tiga paket lagi sebelum harus menunggu pengakuan. Jika penerima mengakui keempat paket sebelum pengirim mengirimkan data lagi, ukuran jendela pengirim sekali lagi kembali ke 7. Pertimbangkan skenario di mana pengirim mengirimkan lima paket dan berhenti.



Gambar 6-9 Contoh jendela geser

Penerima menerima lima paket dan mengakuinya. Sebelum pengakuan diterima, pengirim dapat mengirim dua paket lagi karena ukuran jendelanya adalah 7. Setelah menerima pengakuan, pengirim dapat mengirim tujuh paket tambahan sebelum harus berhenti lagi.

Pengakuan yang dikirimkan oleh penerima kepada pengirim juga diberi nomor. Dalam protokol jendela geser, pengakuan selalu berisi nilai yang sama dengan jumlah paket berikutnya yang diharapkan. Misalnya, jika pengirim, seperti ditunjukkan pada Gambar 6-9,

mengirimkan tiga paket bernomor 0, 1, dan 2, dan penerima ingin mengakui semuanya, maka penerima akan mengembalikan pengakuan (ACK) dengan nilai 3 karena paket 3 adalah paket berikutnya yang diharapkan penerima.

Mari kita kembali sekarang dan mempertimbangkan apa yang akan terjadi jika protokol mengizinkan delapan paket dikirim pada satu waktu. Asumsikan pengirim mengirimkan paket bernomor 0 sampai 7. Penerima menerima semuanya dan mengakui semuanya dengan mengirimkan pengakuan bernomor 0 (paket berikutnya diharapkan). Namun bagaimana jika tidak ada satu pun paket yang sampai di penerima? Penerima tidak akan merespons dengan pengakuan positif, dan pengirim tidak akan mendengar apa pun. Jika setelah masa tunggu yang singkat (batas waktu), pengirim menanyakan kepada penerima nomor paket berikutnya yang diharapkan, penerima akan menjawab dengan 0. Pengirim tidak akan pernah tahu apakah itu berarti semua paket telah diterima atau tidak ada paket sama sekali. diterima. Potensi kebingungan ini dapat menyebabkan pengirim mengirim ulang semua paket ketika tidak diperlukan, atau tidak mengirim ulang satu pun paket ketika penerima mencoba menunjukkan kesalahan.

Sekarang mari kita tambahkan kontrol kesalahan ke protokol jendela geser. Pada dasarnya ada empat hal yang dapat terjadi pada sebuah paket ketika dikirimkan:

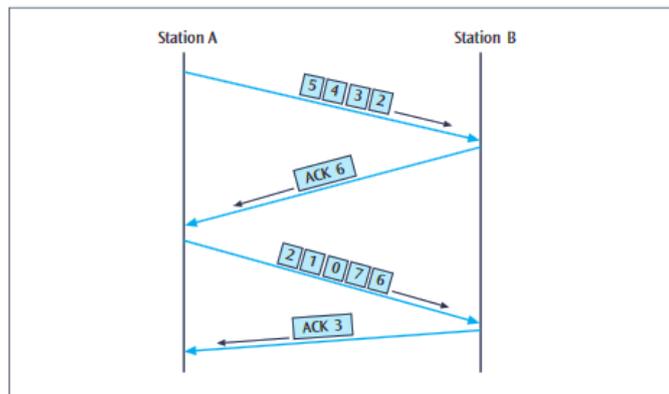
- Paket tiba tanpa kesalahan.
- Paket hilang (tidak pernah sampai).
- Paket rusak (tiba tetapi mengalami kesalahan checksum siklik).
- Paket tertunda (jika paket tertunda cukup lama, paket duplikat mungkin dikirimkan, sehingga menghasilkan dua salinan dari paket yang sama).

Protokol jendela geser dengan kontrol kesalahan harus mampu memperhitungkan masing-masing dari empat kemungkinan ini. Saat Anda terus membaca, mungkin ada gunanya mengingat perbedaan penting. Fungsi protokol jendela geser hanyalah untuk memberi tahu pemancar data apa yang diharapkan selanjutnya. Fungsi dari protokol jendela geser dengan kontrol kesalahan adalah untuk menentukan lebih lanjut apa yang akan terjadi jika terjadi kesalahan selama pengoperasian jendela geser.

Sementara kita memeriksa empat kemungkinan kesalahan selama transmisi, penting juga untuk mencatat perbedaan dalam cara protokol jendela geser yang berbeda memomori data. Protokol jendela geser yang lebih lama, seperti protokol Kontrol Tautan Data Tingkat Tinggi, memberi nomor pada paket yang dikirimkan, yang masing-masing dapat berisi ratusan byte data. Jadi, jika pemancar mengirim empat paket, paket-paket tersebut mungkin diberi nomor masing-masing 0, 1, 2, dan 3. Jika terjadi kesalahan pada suatu paket, penerima akan meminta agar paket tersebut dikirimkan kembali. Sebaliknya, protokol jendela geser yang lebih baru seperti TCP memberi nomor pada masing-masing byte. Dalam hal ini, jika pemancar mengirimkan paket dengan 400 byte data, byte tersebut mungkin, misalnya, diberi nomor 8001 hingga 8400. Jika terjadi kesalahan dengan paket tersebut, penerima akan menunjukkan bahwa paket tersebut memerlukan byte 8001 hingga 8400. ditransmisikan lagi. Mari kita lihat beberapa contoh yang mengilustrasikan empat skenario pengendalian kesalahan dasar yang mungkin terjadi dengan protokol jendela geser. Untuk skenario pertama, Anda akan melihat

contoh penomoran paket, namun secara umum, kita akan lebih berkonsentrasi pada contoh skema penomoran byte pada protokol TCP, karena ini adalah protokol yang lebih populer.

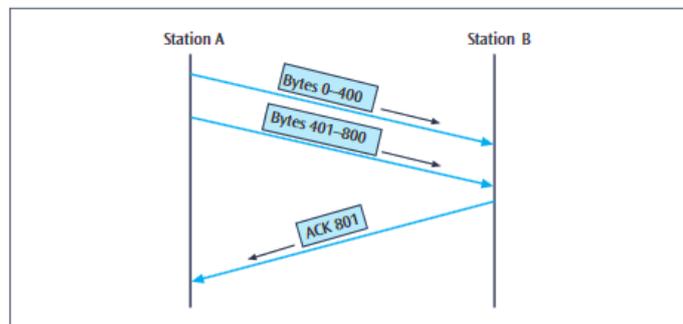
Dalam skenario pertama (ditunjukkan pada Gambar 6-10), satu atau lebih paket, diberi nomor satu per satu, dikirimkan, dan semuanya tiba tanpa kesalahan. Lebih khusus lagi, Stasiun A mentransmisikan empat paket bernomor 2, 3, 4, dan 5, dan Stasiun B menerimanya dan mengirimkan ACK 6 yang mengakui keempatnya. Perhatikan bahwa Stasiun B juga memberitahu Stasiun A paket apa yang diharapkan berikutnya (paket 6). Stasiun A merespons dengan mengirimkan lima paket lagi bernomor 6, 7, 0, 1, dan 2. Stasiun B menerima semua paket dengan mengembalikan ACK 3.



Gambar 6-10 Transfer data normal antara dua stasiun dengan penomoran paket

Jika protokol jendela geser berjumlah byte dan bukan paket, kita mungkin memiliki contoh seperti yang ditunjukkan pada Gambar 6-11. Stasiun A mengirimkan satu paket dengan byte 0–400, diikuti oleh paket kedua dengan byte 401–800. Stasiun B menerima kedua paket dan mengakui semua byte.

Perhatikan sekali lagi bahwa ACK memberitahu Stasiun A byte berikutnya yang diharapkan Stasiun B (801).

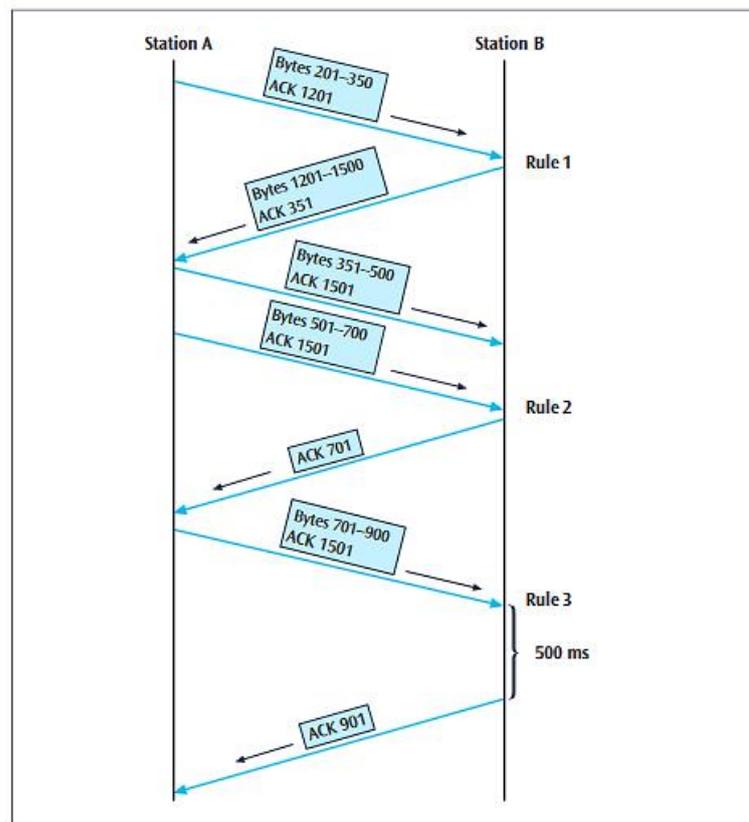


Gambar 6-11 Transfer data normal antara dua stasiun dengan penomoran byte

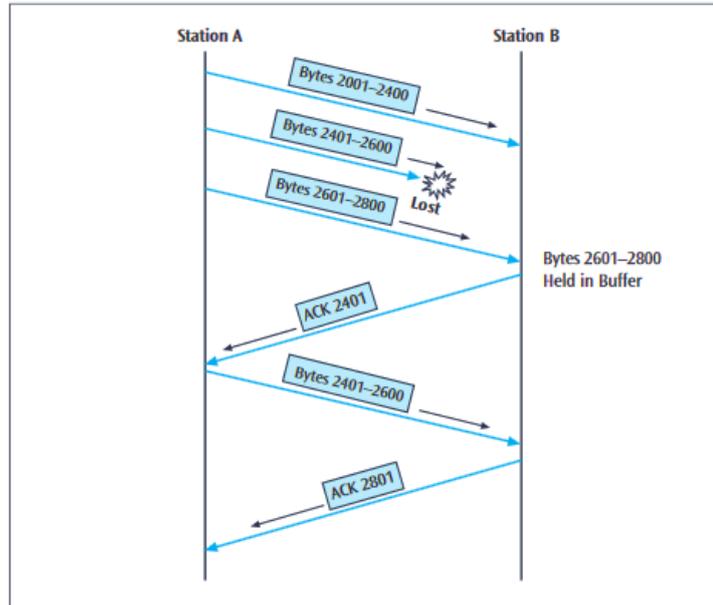
Sebuah pertanyaan menarik muncul: Apakah penerima harus mengakui data tersebut setiap kali ada sesuatu yang diterima? Atau dapatkah penerima menunggu beberapa saat untuk melihat apakah ada pesan lain yang masuk sebelum mengirimkan pengakuan? Dalam dunia

TCP/IP, stasiun penerima mengikuti beberapa aturan untuk menyelesaikan pertanyaan ini. Aturan pertama (ditunjukkan pada Gambar 6-12) adalah jika penerima baru saja menerima sejumlah data dan ingin mengirim data kembali ke pengirim, maka penerima harus menyertakan ACK bersama data yang akan dikirim. Ini disebut piggybacking, dan ini menyelamatkan penerima dari pengiriman pesan ACK terpisah. Aturan kedua adalah jika penerima tidak mempunyai data apa pun untuk dikembalikan ke pengirim, dan penerima baru saja mengakui penerimaan paket data yang dikirimkan sebelumnya, maka penerima harus menunggu 500 milidetik untuk melihat apakah paket lain tiba. Namun, jika paket kedua tiba sebelum waktu 500 milidetik berakhir, maka penerima harus segera mengirimkan ACK. Terakhir, aturan ketiga menyatakan bahwa jika penerima menunggu paket kedua tiba, dan 500 milidetik habis, maka penerima tidak menunggu paket kedua dan malah segera mengeluarkan ACK.

Apa yang terjadi jika sebuah paket hilang? Gambar 6-13 mengilustrasikan situasi di mana Stasiun A mengirimkan serangkaian paket dan paket kedua hilang dalam jaringan. Ketika penerima, Stasiun B, melihat paket ketiga di luar urutan, ia mengembalikan ACK dengan nomor urut yang diharapkan (byte 2401). Stasiun A melihat ada sesuatu yang salah dan mengirimkan kembali paket kedua. Hasil serupa akan terjadi jika paket kedua tiba, namun dengan kesalahan CRC. Dalam kedua kasus tersebut, paket dianggap “hilang”.

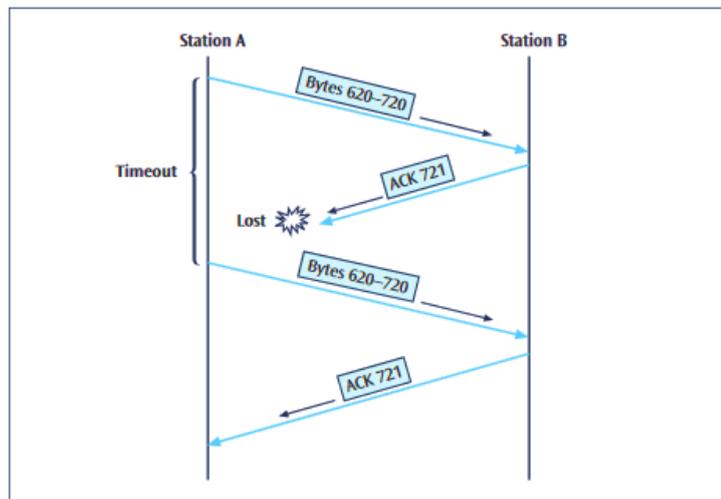


Gambar 6-12 Tiga contoh pengembalian pengakuan di TCP



Gambar 6-13 Paket A yang hilang dan respon Stasiun B

Apa yang terjadi jika sebuah paket tertunda, atau paket duplikat tiba di tujuan? Jika paket cukup tertunda sehingga datangnya tidak berurutan, penerima juga menganggap ini sebagai paket yang hilang dan mengirimkan ACK dengan nilai yang sesuai. Ketika paket tertunda atau paket duplikat tiba, tujuan akan melihat paket dengan nomor urut lebih kecil dari byte yang diakui sebelumnya dan membuang duplikatnya begitu saja.



Gambar 6-14 Pengakuan yang hilang dan transmisi ulang sebuah paket

Terakhir, apa yang terjadi jika pengakuan hilang? Ada dua kemungkinan skenario. Jika perintah pengakuan yang hilang segera diikuti oleh perintah pengakuan lain yang tidak hilang, tidak ada masalah yang terjadi karena pengakuan bersifat kumulatif (pengakuan kedua akan memiliki nomor paket yang sama atau lebih besar). Jika perintah pengakuan hilang dan tidak diikuti oleh perintah pengakuan berikutnya, stasiun pemancar pada akhirnya akan kehabisan waktu

dan menganggap paket sebelumnya sebagai paket yang hilang dan mengirimkannya kembali (Gambar 6-14).

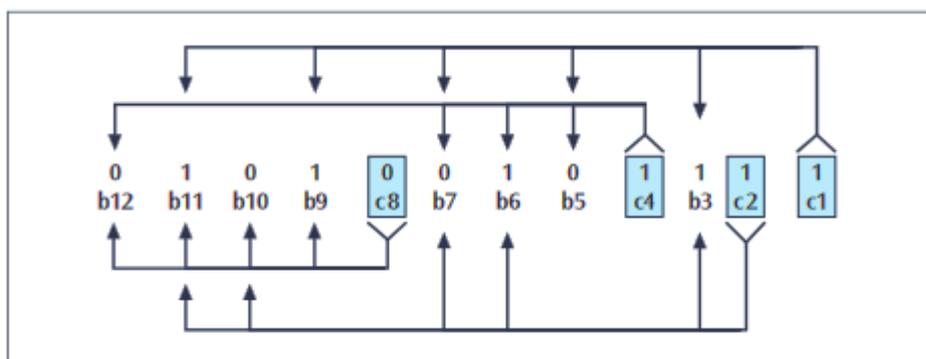
Perbaiki kesalahannya

Awal dari bagian pengendalian kesalahan ini mencantumkan tiga tindakan yang dapat dilakukan penerima jika paket kesalahan dianggap rusak: melemparkan frame/paket, mengembalikan pesan kesalahan, atau memperbaiki kesalahan. Memperbaiki kesalahan seperti ini merupakan solusi yang masuk akal. Paket data telah diterima, dan logika pendeteksi kesalahan telah menentukan bahwa telah terjadi kesalahan. Mengapa tidak memperbaiki kesalahan dan melanjutkan pemrosesan? Sayangnya, memperbaiki kesalahan tidaklah mudah.

Agar penerima dapat memperbaiki kesalahan—dalam proses yang disebut koreksi kesalahan maju—informasi berlebihan harus ada sehingga penerima mengetahui bit mana yang salah dan berapa nilai aslinya. Misalnya, jika Anda diberi data 0110110 dan diberi tahu bahwa pemeriksaan paritas mendeteksi kesalahan, dapatkah Anda menentukan bit mana yang rusak? Tidak, Anda tidak akan memiliki informasi yang cukup.

Untuk melihat keseluruhan masalahnya, pertimbangkan apa yang akan terjadi jika Anda mengirimkan tiga salinan identik untuk setiap bit. Misalnya, Anda mengirimkan 0110110 sebagai 000 111 111 000 111 111 000. Sekarang, mari kita korup 1 bit: 000 111 111 001 111 111 000. Bisakah Anda menentukan bit mana yang rusak? Jika Anda berasumsi bahwa hanya satu bit yang rusak, Anda dapat menerapkan apa yang dikenal sebagai prinsip aturan mayoritas dan menentukan bahwa bit kesalahan adalah 1 terakhir dalam kelompok keempat, 001. Namun perlu diperhatikan bahwa bahkan dalam contoh sederhana ini, koreksi kesalahan maju memerlukan transmisi tiga kali lipat jumlah data asli, dan hanya memberikan sedikit koreksi kesalahan. Tingkat batas overhead ini adalah penerapan koreksi kesalahan maju.

Jenis koreksi kesalahan maju yang lebih berguna adalah kode Hamming. Kode Hamming adalah kode yang dirancang khusus di mana bit pemeriksaan khusus telah ditambahkan ke bit data sehingga, jika terjadi kesalahan selama transmisi, penerima mungkin dapat memperbaiki kesalahan tersebut menggunakan bit pemeriksaan dan data yang disertakan. (Untuk mempelajari lebih lanjut tentang seluk-beluk teknis kode Hamming, lihat kotak Detail berjudul “Koreksi Kesalahan Maju dan Jarak Hamming.”) Misalnya, kita ingin mengirimkan karakter 8-bit: karakter 01010101 terlihat pada Gambar 6-15. Mari kita beri nomor pada bit karakter ini b12, b11, b10, b9, b7, b6, b5, dan b3. (Kami akan memberi nomor pada bit-bit tersebut dari kanan ke kiri, menyisakan ruang untuk bit-bit pengecekan yang akan segera ditambahkan.) Sekarang tambahkan ke bit-bit data ini bit-bit pengecekan berikut: c8, c4, c2, dan c1, di mana c8 menghasilkan paritas genap sederhana untuk bit b12, b11, b10, dan b9. Pengecekan bit c4 akan menghasilkan paritas genap sederhana untuk bit b12, b7, b6, dan b5. Pengecekan bit c2 akan menghasilkan paritas genap sederhana untuk bit b11, b10, b7, b6, dan b3. Terakhir, c1 akan menghasilkan paritas genap sederhana untuk bit b11, b9, b7, b5, dan b3. Perhatikan bahwa setiap bit pemeriksaan di sini memeriksa urutan bit data yang berbeda.



Gambar 6-15 Bit pengecekan kode Hamming yang dihasilkan dari data 01010101

Mari kita lihat lebih dekat bagaimana masing-masing bit pemeriksaan kode Hamming pada Gambar 6-15 bekerja. Perhatikan bahwa c_8 “mencakup” bit b_{12} , b_{11} , b_{10} , dan b_9 , yaitu 0101. Jika kita menghasilkan bit paritas genap berdasarkan keempat bit tersebut, kita akan menghasilkan 0 (ada bilangan genap 1). Jadi, c_8 sama dengan 0. c_4 mencakup b_{12} , b_7 , b_6 , dan b_5 , yaitu 0010, jadi c_4 sama dengan 1. c_2 mencakup b_{11} , b_{10} , b_7 , b_6 , dan b_3 , yaitu 10011, jadi c_2 sama dengan 1. c_1 mencakup b_{11} , b_9 , b_7 , b_5 , dan b_3 , yaitu 11001, jadi c_1 sama dengan 1. Konsekuensinya, jika kita memiliki data 01010101, kita akan menghasilkan bit pemeriksaan 0111, seperti yang ditunjukkan pada Gambar 6-15.

Koreksi Kesalahan Maju dan Jarak Hamming

Agar kode data seperti ASCII dapat melakukan koreksi kesalahan maju, bit redundan harus ditambahkan ke bit data asli. Bit-bit yang berlebihan ini memungkinkan penerima untuk melihat data yang diterima dan, jika ada kesalahan, memulihkan data asli menggunakan konsensus bit-bit yang diterima. Sebagai contoh sederhana, mari kita mengirimkan tiga salinan identik dari satu bit (operasi mayoritas). Jadi, untuk mengirim 1, 111 akan dikirimkan. Selanjutnya, pertimbangkan apa yang akan terjadi jika 3 bit yang diterima memiliki nilai 101. Dalam koreksi kesalahan maju, penerima akan berasumsi bahwa bit 0 seharusnya adalah 1 karena sebagian besar bit adalah 1. Untuk memahami bagaimana bit redundan tercipta, Anda perlu memeriksa jarak Hamming suatu kode, yang merupakan jumlah bit terkecil yang membedakan kode karakter. Jarak Hamming merupakan karakteristik suatu kode. Untuk membuat kode koreksi diri atau kode koreksi kesalahan penerusan, Anda harus membuat kode yang memiliki jarak Hamming yang sesuai.

Dalam kumpulan karakter ASCII, huruf B dalam biner adalah 1000010, dan huruf C adalah 1000011. Selisih antara B dan C adalah 1 bit—bit paling kanan. Jika Anda membandingkan semua karakter ASCII, Anda akan menemukan bahwa beberapa pasangan karakter berbeda satu bit, dan beberapa berbeda dua bit atau lebih. Karena jarak Hamming suatu kode didasarkan pada jumlah bit terkecil yang membedakan kode karakter, rangkaian karakter ASCII memiliki jarak Hamming 1.

Sayangnya, jika rangkaian karakter memiliki jarak Hamming 1, kesalahan tidak dapat dideteksi atau diperbaiki. Tanyakan pada diri Anda pertanyaan berikut: Jika penerima menerima karakter 1000010, bagaimana ia mengetahui dengan pasti bahwa ini adalah huruf B dan bukan huruf C dengan kesalahan 1-bit?

Ketika bit paritas ditetapkan ke ASCII, jarak Hamming menjadi 2. Karena bit paling kanan adalah bit paritas, karakter B, dengan asumsi paritas genap, menjadi 10000100, dan karakter C menjadi 10000111. Sekarang, 2 bit terakhir dari B harus berubah dari 00 menjadi 11 agar karakter B menjadi karakter C, dan perbedaan antara kedua karakter tersebut adalah dua bit. Sekarang jarak Hamming adalah 2, kesalahan bit tunggal dapat dideteksi, tetapi Anda masih tidak dapat memperbaiki kesalahan. Juga, jika karakter B ditransmisikan, tetapi satu bit dibalik karena kesalahan, kesalahan pemeriksaan paritas terjadi; namun, Anda masih belum bisa mengetahui karakter apa yang seharusnya. Misalnya, karakter B yang ditambah paritas genap adalah 10000100. Jika 1 bit diubah, seperti bit kedua, nilai binernya sekarang menjadi 11000100. Karakter ini akan menyebabkan pemeriksaan paritas, tetapi karakter aslinya apa? Salah satu bitnya bisa saja berubah, sehingga memungkinkan adanya banyak kemungkinan karakter asli. Anda dapat memperbaiki kesalahan bit tunggal dan mendeteksi kesalahan bit ganda ketika jarak Hamming dari kumpulan karakter minimal 3. Mencapai jarak Hamming 3 memerlukan tingkat redundansi yang lebih tinggi dan, akibatnya, biaya.

Karakter 12-bit ini sekarang dikirimkan ke penerima. Penerima menerima bit-bit tersebut dan melakukan empat pemeriksaan paritas pada bit pemeriksaan c8, c4, c2, dan c1. Jika tidak ada yang terjadi pada karakter 12-bit selama transmisi, keempat pemeriksaan paritas tidak akan menghasilkan kesalahan. Namun apa yang akan terjadi jika salah satu bit rusak dan menghasilkan nilai sebaliknya? Misalnya, bagaimana jika bit b9 rusak? Dengan b9 yang rusak, kita sekarang akan memiliki string 010000101111. Penerima akan melakukan empat pemeriksaan paritas, tapi kali ini akan ada kesalahan paritas. Lebih tepatnya, karena c8 memeriksa b12, b11, b10, b9, dan c8 (01000), maka akan terjadi kesalahan paritas. Seperti yang Anda lihat, ada jumlah ganjil 1 dalam string data, tetapi bit pengecekan mengembalikan 0. c4 memeriksa b12, b7, b6, b5, dan c4 (00101) dan, dengan demikian, tidak akan menghasilkan kesalahan paritas. c2 memeriksa b11, b10, b7, b6, b3, dan c2 (100111), dan tidak menghasilkan kesalahan paritas. c1 memeriksa bit b11, b9, b7, b5, b3, dan c1 (100011), yang akan menghasilkan kesalahan paritas. Perhatikan bahwa jika kita memeriksa bit pengecekan saja dan menunjukkan 1 jika terdapat kesalahan paritas dan 0 jika tidak ada kesalahan paritas, kita akan mendapatkan 1001 (kesalahan c8, c4 tanpa kesalahan, c2 tanpa kesalahan, kesalahan c1). 1001 adalah biner untuk 9, memberitahu kita bahwa bit yang salah berada di posisi kesembilan.

Meskipun ada biaya tambahan dalam penggunaan koreksi kesalahan maju, adakah aplikasi yang mendapat manfaat dari penggunaan teknologi ini? Dua kelompok besar aplikasi sebenarnya dapat memperoleh manfaat: transmisi televisi digital dan aplikasi yang mengirim data dalam jarak yang sangat jauh. Sinyal televisi digital menggunakan bentuk koreksi kesalahan maju yang disebut kode Reed-Solomon dan pengkodean Trellis. Perhatikan bahwa tidak mungkin meminta transmisi ulang sinyal TV jika terjadi kesalahan. Ini akan terlambat! Data perlu dikirimkan secara real time, sehingga perlu adanya koreksi kesalahan ke depan.

Pada contoh kedua, jika data harus dikirim melalui jarak jauh, akan memakan banyak biaya dan waktu untuk mengirimkan ulang paket yang datang karena kesalahan. Misalnya, waktu yang dibutuhkan NASA untuk mengirim pesan ke wahana Mars adalah beberapa menit.

Jika data tiba dalam keadaan kacau, diperlukan waktu beberapa menit lagi sebelum pengakuan negatif diterima, dan beberapa menit lagi sebelum data dapat dikirim ulang. Jika sejumlah besar paket data tiba dalam keadaan kacau, transmisi data ke Mars bisa menjadi proses yang sangat panjang dan membosankan.

6.6 DETEKSI KESALAHAN DALAM PRAKTIKNYA

Anda bekerja di sebuah perusahaan keuangan yang memiliki kantor di dua lokasi di sisi berlawanan dari wilayah metropolitan besar. Perusahaan ini memiliki banyak komputer yang terletak di kedua lokasi, dan komputer di satu gedung terus-menerus mengirimkan data ke komputer di gedung kedua. Saat ini, layanan telepon sewaan mentransfer semua data antar gedung dengan kecepatan sekitar 128.000 bit per detik. Anda telah diminta untuk menyelidiki pemilihan skema deteksi kesalahan. Haruskah Anda memilih pemeriksaan paritas yang lebih sederhana atau menggunakan checksum redundansi siklik yang lebih rumit? Mari kita pertimbangkan dua faktor saat kita mengambil keputusan: kemungkinan kesalahan tidak terdeteksi, dan jumlah tambahan bit pendeteksi kesalahan yang dikirimkan antara dua lokasi.

Pertama-tama, dengan mempertimbangkan kemungkinan kesalahan yang tidak terdeteksi, ingatlah bahwa paritas sederhana hanya mendeteksi kesalahan bit dalam jumlah ganjil. Bahkan sejumlah kesalahan bit pun tidak akan terdeteksi. Dengan demikian, hanya 50 persen dari seluruh kesalahan yang akan tertangkap, atau 50 persen dari seluruh frame yang dikirimkan dengan kesalahan tidak akan terdeteksi. Seberapa sering frame dikirimkan dengan kesalahan? Mari kita asumsikan tingkat kesalahan yang cukup konservatif yaitu satu frame dalam 10.000, atau dengan kata lain, tingkat kesalahan 10⁻⁴. Jika kesalahan hanya terjadi pada satu frame dalam 10.000 frame, dan kesalahan tersebut tidak terdeteksi separuh waktu, maka error akan muncul satu kali dalam setiap 20.000 frame. Karena frame yang menyertakan bit paritas biasanya panjangnya 8 bit, kesalahan tidak akan terdeteksi sekali dalam setiap 160.000 bit. Artinya jika kita mentransmisikan data dengan kecepatan 128.000 bit per detik, maka kesalahan yang tidak terdeteksi akan terjadi hampir setiap satu setengah detik.

Dengan menggunakan checksum redundansi siklik, skenario terburuknya adalah ledakan kesalahan yang panjangnya lebih dari $r + 1$, yang memiliki probabilitas tidak terdeteksi sama dengan $(\frac{1}{2})^r$. Diberikan polinomial pembangkit 16 bit, $(\frac{1}{2})^{16}$ sama dengan 0,000015258. Sekali lagi dengan asumsi bahwa frame dengan kesalahan terjadi sekali dalam setiap 10.000 frame (probabilitas 0,0001), $0,00001528 \times 0,0001$ sama dengan 0,000000001528. Mengambil kebalikannya, ini berarti 654.450.261 frame akan dikirimkan sebelum kesalahan terjadi. Jika kita berasumsi bahwa ukuran frame tipikal yang menggunakan checksum redundansi siklik adalah 1000 bit, $6,5445 \times 10^{11}$ bit akan dikirimkan sebelum kesalahan terjadi. Mentransmisikan pada 128.000 bit per detik, 5.112.892,7 detik akan berlalu sebelum terjadi kesalahan. Ini secara kasar berarti 59 hari penulanan terus menerus (24/7). Bandingkan dengan kesalahan yang tidak terdeteksi hampir setiap satu setengah detik menggunakan paritas.

Sekarang mari kita pertimbangkan berapa banyak bit pendeteksi kesalahan tambahan yang harus ditambahkan ke setiap transmisi. Untuk keseimbangan, mari kita asumsikan

karakter ASCII 7-bit standar. Untuk setiap karakter ASCII, satu bit paritas ditambahkan. Jadi, 1 dari setiap 8 bit yang dikirimkan adalah bit cek. Untuk checksum redundansi siklik, sisanya berukuran r . Sekali lagi dengan asumsi checksum berukuran 16 bit dan ukuran frame 1000 bit, 16 dari setiap 1000 bit (atau satu dari setiap 62,5 bit) adalah bit check. Itu hampir delapan kali lebih baik daripada paritas.

Kesimpulannya, checksum redundansi siklik menambahkan lebih sedikit bit pemeriksaan ke setiap frame dan memberikan tingkat deteksi kesalahan yang jauh lebih tinggi. Tidak ada keraguan bahwa, dengan dua faktor ini, checksum redundansi siklik lebih unggul daripada paritas.

RINGKASAN

- Kebisingan selalu hadir dalam jaringan komputer. Jika tingkat kebisingan terlalu tinggi, kesalahan akan terjadi selama transmisi data. Jenis-jenis noise antara lain white noise, impuls noise, crosstalk, echo, jitter, dan attenuation. Hanya derau impuls yang dianggap sebagai derau tidak kontinyu, sedangkan bentuk derau lainnya bersifat kontinyu.
- Di antara teknik-teknik untuk mengurangi kebisingan adalah dengan melindungi kabel dengan benar, mengenali kemungkinan konflik sinyal nirkabel, menggunakan peralatan digital modern, menggunakan repeater digital dan amplifier analog, dan mengamati kapasitas media yang disebutkan. Pilihan wajar lainnya untuk mengurangi kemungkinan kesalahan termasuk mengurangi jumlah perangkat dalam aliran transmisi, mengurangi panjang kabel, dan mengurangi kecepatan transmisi data.
- Tiga bentuk dasar deteksi kesalahan adalah paritas, checksum aritmatika, dan checksum redundansi siklik. Paritas sederhana menambahkan satu bit tambahan ke setiap karakter dan merupakan skema deteksi kesalahan yang sangat sederhana yang memiliki tingkat deteksi kesalahan yang rendah dan rasio bit pemeriksaan terhadap bit data yang relatif tinggi. Paritas longitudinal menambahkan seluruh karakter bit pemeriksaan ke dalam blok data dan meningkatkan deteksi kesalahan, namun masih mengalami tingkat deteksi kesalahan yang tidak memadai dan rasio bit pemeriksaan terhadap bit data yang relatif tinggi.
- Checksum aritmatika adalah skema pendeteksi kesalahan yang digunakan dengan Protokol Internet dan menghasilkan jumlah aritmatika dari semua karakter yang dikirimkan dalam sebuah pesan.
- Checksum redundansi siklik adalah skema pendeteksi kesalahan yang unggul dengan kemampuan hampir 100 persen dalam mengenali paket data yang rusak. Penghitungan sisa checksum cukup cepat bila dilakukan oleh perangkat keras, dan menambahkan bit pemeriksaan yang relatif sedikit ke paket data yang berpotensi besar.
- Setelah kesalahan terdeteksi, ada tiga opsi yang mungkin dilakukan: membuang frame/paket, mengembalikan pesan kesalahan, dan memperbaiki kesalahan. Opsi lempar bingkai/paket digunakan oleh beberapa teknologi transmisi baru, seperti relai bingkai. Frame relay mengasumsikan bahwa jalur serat optik akan digunakan, yang secara signifikan mengurangi kemungkinan kesalahan. Jika kesalahan memang terjadi, protokol

lapisan yang lebih tinggi akan mencatat kesalahan frame dan akan melakukan beberapa jenis pengendalian kesalahan. Pilihan untuk mengembalikan pesan kesalahan ke pemancar adalah respons paling umum terhadap kesalahan dan melibatkan penggunaan protokol Stop-and-wait dan protokol jendela geser.

- Protokol Stop-and-wait hanya mengizinkan satu paket dikirim dalam satu waktu. Sebelum paket lain dapat dikirim, pengirim harus menerima pengakuan positif. Protokol jendela geser memungkinkan banyak paket dikirim sekaligus. Penerima dapat mengakui beberapa paket dengan satu pengakuan.
- Koreksi kesalahan dimungkinkan jika data yang dikirimkan berisi informasi redundan yang cukup sehingga penerima dapat memperbaiki kesalahan dengan benar tanpa meminta informasi tambahan kepada pemancar. Bentuk pengendalian kesalahan ini memerlukan overhead dalam jumlah besar dan hanya digunakan dalam aplikasi khusus dimana transmisi ulang data tidak diinginkan.

PERTANYAAN

1. Apa itu white noise dan bagaimana pengaruhnya terhadap sinyal?
2. Apa yang dimaksud dengan kebisingan impulsif dan mengapa kebisingan tersebut paling mengganggu?
3. Apa itu crosstalk dan bagaimana pengaruhnya terhadap sinyal?
4. Apa itu gema dan bagaimana pengaruhnya terhadap transmisi data?
5. Apa itu jitter dan mengapa ini merupakan masalah sinyal digital?
6. Jenis kebisingan manakah yang diperkenalkan dalam bab ini yang bersifat kontinyu, dan manakah yang tidak kontinyu?
7. Apakah pelindungan yang tepat pada suatu medium akan meningkatkan atau menurunkan kemungkinan terjadinya kesalahan? Jelaskan alasan Anda.
8. Apa perbedaan antara paritas genap dan paritas ganjil?
9. Berapa rasio bit pemeriksaan terhadap bit data untuk paritas sederhana?
10. Berapa rasio bit pemeriksaan terhadap bit data untuk paritas longitudinal?
11. Jenis kesalahan apa yang tidak dapat dideteksi oleh paritas sederhana?
12. Jenis kesalahan apa yang tidak dapat dideteksi oleh paritas longitudinal?
13. Dengan checksum aritmatika, apa yang ditambahkan?
14. Apa yang dimaksud dengan polinomial pembangkit?
15. Jenis kesalahan apa yang tidak terdeteksi oleh cyclic checksum?
16. Praktek frame relay yang berupa pengendalian kesalahan?
17. Berapa banyak paket yang dapat dikirim sekaligus menggunakan kontrol kesalahan Stop-and-wait?
18. Apa fungsi ACK dalam pengendalian kesalahan Stop-and-wait?
19. Apa fungsi NAK dalam pengendalian kesalahan Stop-and-wait?
20. Dalam sistem komunikasi, apa yang dimaksud dengan batas waktu?
21. Mengapa ukuran jendela pada sistem jendela geser awal begitu kecil?
22. Apa dua cara berbeda untuk menomori barisan data?

23. Kondisi apa yang harus dipenuhi agar koreksi kesalahan dapat dilakukan?

LATIHAN SOAL

1. Jenis noise manakah yang paling sulit dihilangkan dari sinyal analog? Mengapa?
2. Jenis noise manakah yang paling sulit dihilangkan dari sinyal digital? Mengapa?
3. Jelaskan hubungan antara kabel twisted pair dan crosstalk.
4. Jenis kabel manakah yang paling rentan terhadap gema?
5. Mengingat karakter 0110101, bit apa yang akan ditambahkan untuk mendukung paritas genap?
6. Mengingat karakter 1010010, bit apa yang akan ditambahkan untuk mendukung paritas ganjil?
7. Hasilkan bit paritas dan bit paritas memanjang untuk paritas genap untuk karakter 0101010, 0011010, 0011110, 1111110, dan 0000110.
8. Diberikan pesan "Halo, selamat tinggal", tunjukkan checksum aritmatika desimal yang akan dibuat / dihasilkan.
9. Sebutkan jenis-jenis kesalahan yang dapat lolos dari sistem checksum redundansi siklik.
10. Sebutkan jenis-jenis kesalahan yang tidak dapat lolos dari sistem checksum redundansi siklik.
11. Mengapa semua polinomial penghasil CRC diakhiri dengan 1?
12. Dalam sistem kontrol kesalahan Stop-and-wait, Stasiun A mengirimkan paket 0, dan paket tersebut hilang. Apa yang terjadi selanjutnya?
13. Dalam sistem kendali kesalahan Stop-and-wait, Stasiun A mengirimkan paket 0, paket tersebut tiba tanpa kesalahan, dan ACK dikembalikan, namun ACK hilang. Apa yang terjadi selanjutnya?
14. Dalam sistem kontrol kesalahan jendela geser di mana setiap paket diberi nomor, Stasiun A mengirimkan paket 4, 5, 6, dan 7. Stasiun B menerimanya dan ingin mengakui semuanya. Apa yang dikirim kembali oleh Stasiun B ke Stasiun A?
15. Dalam sistem kontrol kesalahan jendela geser yang setiap byte diberi nomor, Stasiun A mengirimkan paket dengan byte bernomor 801 hingga 900. Jika paket tiba tanpa kesalahan, bagaimana tanggapan Stasiun B?
16. Dalam sistem kontrol kesalahan jendela geser, Stasiun A mengirimkan paket dengan byte 501–700, diikuti segera oleh paket dengan byte 701–900. Buat diagram skenario pengendalian kesalahan ini, dan tunjukkan respons yang akan dikirimkan Stasiun B jika tidak ada kesalahan.
17. Dalam sistem kontrol kesalahan jendela geser, Stasiun A mengirimkan paket dengan byte 501–700, diikuti segera oleh paket dengan byte 701–900. Buat diagram skenario pengendalian kesalahan ini, dan tunjukkan respons yang akan dikirimkan Stasiun B jika paket kedua hilang dalam jaringan.
18. Dalam sistem kontrol kesalahan jendela geser, Stasiun A mengirimkan paket dengan byte 501–700, diikuti segera oleh paket dengan byte 701–900. Buat diagram skenario

pengendalian kesalahan ini, dan tunjukkan respon yang akan dikirimkan Stasiun B jika kedua paket tiba, tetapi ada kesalahan checksum pada paket kedua.

19. Dalam sistem kontrol kesalahan jendela geser, Stasiun A mengirimkan tiga paket dengan byte masing-masing 0–100, 101–200, dan 201–300. Paket kedua dengan byte 101–200 disimpan di suatu tempat dalam jaringan cukup lama sehingga paket ketiga tiba sebelum yang kedua. Buatlah diagram skenario pengendalian kesalahan ini, dan tunjukkan respon yang akan dikirim oleh Stasiun B. Sekarang asumsikan bahwa lima detik setelah Stasiun B merespons, paket kedua muncul. Apa yang dilakukan Stasiun B sekarang?
20. Asumsikan protokol jendela geser memiliki bidang 3-bit untuk menampung ukuran jendela. Nilai 3-bit memberikan delapan kombinasi, dari 0 hingga 7. Lalu, mengapa pemancar dapat mengirimkan maksimal hanya tujuh paket pada satu waktu dan bukan delapan? Tunjukkan sebuah contoh.
21. Jika ukuran jendela geser 7-bit digunakan, berapa banyak paket yang dapat dikirim sebelum pemancar harus berhenti dan menunggu pengakuan?
22. Apakah kontrol kesalahan Stop-and-wait merupakan protokol setengah dupleks atau protokol dupleks penuh? Jelaskan tanggapan Anda.
23. Rancanglah kumpulan kode untuk angka 0 sampai 9 yang mempunyai jarak Hamming 2.
24. Suatu sistem akan mengirimkan byte 10010100. Tunjukkan empat bit pemeriksaan c_8 , c_4 , c_2 , dan c_1 yang akan ditambahkan ke byte ini.
25. String 12-bit 010111110010 dengan bit kode Hamming tertanam (c_8 , c_4 , c_2 , dan c_1) baru saja tiba. Apakah ada kesalahan? Jika iya, bit manakah yang error?
26. Buatlah kode Hamming 12-bit untuk karakter A dan 3.

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Perusahaan Anda mengirimkan catatan 500 karakter (byte) dengan kecepatan 400.000 bit per detik. Anda telah diminta untuk menentukan cara paling efisien untuk mengirimkan catatan ini. Jika sistem kendali kesalahan Stop-and-wait digunakan, berapa lama waktu yang dibutuhkan untuk mengirimkan 1000 rekaman? Jika kontrol kesalahan jendela geser digunakan dengan ukuran jendela 127, berapa lama waktu yang dibutuhkan untuk mengirimkan 1000 record? Jika rata-rata satu record dari setiap 200 record rusak, berapa lama waktu yang dibutuhkan untuk mengirimkan 1000 record? Apa kesimpulan Anda?
2. Atasan Anda telah mendengar banyak tentang checksum redundansi siklik tetapi tidak yakin bahwa ini jauh lebih baik daripada paritas sederhana. Anda mengutip beberapa angka dan kemungkinan deteksi kesalahan, tetapi itu tidak berarti apa-apa. Jika Anda bisa memberi lebih contoh nyata betapa bagusnya checksum redundansi siklik, Anda mungkin memenangkan hati bos. Ingat kembali probabilitas yang diberikan pada Tabel 6-4. Jika perusahaan Anda mengirimkan aliran data terus-menerus dengan kecepatan

- 128.000 bit per detik, berapa lama waktu yang dibutuhkan sebelum checksum redundansi siklik mengatasi kesalahan?
3. Mengingat teknologi jaringan saat ini, ukuran jendela geser 3-bit dan 7-bit tampaknya sangat membatasi. Berapa ukuran yang lebih masuk akal saat ini? Jelaskan alasan Anda.
 4. Dinyatakan dalam bab ini bahwa beberapa protokol baru mengadopsi bentuk kontrol kesalahan frame/packet. Apakah ini pilihan yang masuk akal? Jika ya, dapatkah Anda membuat contoh yang menganggap hal ini bukan pilihan yang masuk akal?
 5. Teknik pendeteksi kesalahan apa lagi yang tersedia? Bagaimana perbandingannya dengan checksum paritas dan redundansi siklik?
 6. Apa yang dimaksud dengan distorsi intermodulasi? Sinyal macam apa yang rentan terhadap bentuk distorsi ini?
 7. Temukan contoh kode Hamming lainnya dan jelaskan cara kerjanya.
 8. Jelaskan dua situasi di mana transmisi bebas kesalahan sangat penting dalam komunikasi.
 9. Diketahui data 10001010010 dan CRC yang menghasilkan polinomial 10011, tunjukkan sisa yang dihasilkan. Anda dapat menggunakan metode pembagian panjang atau metode register geser.
 10. Dengan menggunakan bahasa pemrograman pilihan Anda, tuliskan sebuah program yang memasukkan string karakter dan menghitung sisa checksum siklik menggunakan polinomial pembangkit tertentu.
 11. Apakah ada polinomial penghasil CRC selain yang tercantum dalam bab ini?

BAB 7

JARINGAN AREA LOKAL

BAGIAN 1

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Tentukan jaringan area lokal
- Buat daftar fungsi utama, aktivitas, dan area penerapan jaringan area lokal
- Sebutkan kelebihan dan kekurangan jaringan area lokal
- Identifikasi tata letak fisik dan logis dari jaringan area lokal
- Tentukan teknik kontrol akses media yang berbeda
- Kenali format frame IEEE 802 yang berbeda
- Jelaskan sistem jaringan area lokal kabel yang umum

MOBIL masa kini, menurut majalah *Network World*, memiliki daya komputasi yang lebih besar dibandingkan roket yang digunakan dalam pendaratan Apollo di bulan pada tahun 1970an. Meski mengejutkan, hal ini tidak sulit dipercaya. Mobil masa kini dapat mencatat transaksi berkendara seperti pengereman dan akselerasi; mengatur campuran udara dan bahan bakar; mengontrol rem antilock, kontrol anti slip, dan sistem suspensi; menyediakan sistem hiburan audio dan video depan dan belakang yang terpisah; dan memberi tahu pengemudi melalui video bawaan saat mobil hendak mundur melewati sepeda anak-anak.

Selain itu, pabrikan sedang merancang kendaraan dengan layanan pemantauan jarak jauh yang dapat membantu pemilik dalam menjadwalkan pemeliharaan preventif. Layanan radio satelit baru dapat digunakan untuk mengunduh sistem hiburan dan berita real-time. Sistem berkemampuan Bluetooth saat ini digunakan untuk menyediakan layanan telepon seluler hands-free, namun di masa depan juga akan menyediakan kontrol mobil yang diaktifkan dengan suara. Juga, misalkan mobil Anda berhenti di pinggir jalan pada malam yang gelap. Ada rencana untuk menciptakan sistem penghindaran tabrakan yang akan berkomunikasi antara mobil Anda dan kendaraan lain di jalan untuk mencegah tabrakan.

Inti dari sistem komunikasi ini adalah satu atau lebih jaringan area lokal. Faktanya, jaringan area lokal pada akhirnya akan mengambil alih banyak fungsi di dalam mobil. Jaringan area lokal berkecepatan rendah akan digunakan untuk mengontrol lampu, kipas angin, dan sistem yang bereaksi lambat lainnya. Jaringan berkecepatan lebih tinggi akan digunakan untuk mengontrol rem antilock, kontrol anti slip, dan kontrol mesin yang sesuai. Masih ada jaringan lain yang dapat digunakan untuk melakukan fungsi penting seperti pengembangan kantung udara saat terjadi tabrakan. Mengingat semua aplikasi yang ada dan mungkin diterapkan, mobil dengan cepat menjadi jaringan di atas roda.

Apakah jaringan area lokal begitu penting bagi kehidupan sehari-hari sehingga menjadi pilihan standar di mobil?

Jika pekerjaan Anda, rumah Anda, dan mobil Anda semuanya bergantung pada jaringan area lokal, apa yang mungkin terjadi selanjutnya?

7.1 PENDAHULUAN

Jaringan area lokal (LAN) adalah jaringan komunikasi yang menghubungkan berbagai perangkat komunikasi data dalam wilayah geografis kecil dan mentransmisikan data dengan kecepatan transfer data yang tinggi. Beberapa poin dalam definisi ini perlu dikaji lebih dekat. Yang dimaksud dengan “*perangkat komunikasi data*” mencakup komputer seperti komputer pribadi, stasiun kerja komputer, dan komputer mainframe, serta perangkat periferal seperti disk drive, printer, dan modem. Perangkat komunikasi data juga dapat mencakup item seperti sensor gerak, asap, dan panas; alarm kebakaran; sistem ventilasi; dan pengatur kecepatan motor. Perangkat terakhir ini sering ditemukan di lingkungan bisnis dan manufaktur di mana jalur perakitan dan robot biasanya digunakan.

Bagian berikutnya dari definisi, “*dalam wilayah geografis yang kecil,*” biasanya menyiratkan bahwa jaringan area lokal dapat berukuran sekecil satu ruangan, atau dapat meluas ke beberapa ruangan, ke beberapa lantai dalam sebuah gedung, dan bahkan ke beberapa gedung dalam satu gedung. satu kampus. Namun, wilayah geografis yang paling umum adalah satu ruangan atau beberapa ruangan dalam satu bangunan.

Terakhir, frasa terakhir dari definisi tersebut menyatakan bahwa jaringan area lokal mampu mentransmisikan data pada “*kecepatan transfer data yang tinggi.*” Meskipun jaringan area lokal awal hanya mengirimkan data dengan kecepatan 10 juta bit per detik, jaringan area lokal terbaru dapat mengirimkan data dengan kecepatan 10 miliar bit per detik atau lebih.

Mungkin keuntungan terkuat dari jaringan area lokal adalah kemampuannya memungkinkan pengguna untuk berbagi sumber daya perangkat keras dan perangkat lunak. Misalnya, versi jaringan dari program database populer dibeli dan diinstal pada jaringan area lokal. File yang berisi semua informasi database disimpan di lokasi pusat seperti server jaringan. Ketika pengguna jaringan area lokal mana pun ingin mengakses catatan dari program basis data tersebut, catatan tersebut dapat diambil dari server dan kemudian dikirim melalui jaringan area lokal ke stasiun kerja pengguna, di mana catatan tersebut dapat ditampilkan. Demikian pula, printer berkualitas tinggi dapat diinstal pada jaringan sehingga semua pengguna dapat berbagi akses ke perangkat yang relatif mahal ini.

Sejak jaringan area lokal pertama kali muncul pada tahun 1970an, penggunaannya telah meluas di lingkungan komersial dan akademis. Faktanya, sulit membayangkan kumpulan stasiun kerja komputer dalam lingkungan komputasi yang tidak menggunakan suatu bentuk jaringan area lokal. Banyak pengguna komputer individu mulai menginstal jaringan area lokal di rumah untuk menghubungkan dua komputer atau lebih. Sama seperti di lingkungan kantor, salah satu kekuatan pendorong di balik pemasangan jaringan area lokal di rumah adalah kemampuan berbagi periferal seperti printer berkualitas tinggi dan koneksi berkecepatan

tinggi ke Internet. Untuk lebih memahami fenomena ini, penting untuk mengkaji beberapa “lapisan” teknologi jaringan area lokal.

Bab ini dimulai dengan membahas fungsi utama jaringan area lokal serta kelebihan dan kekurangannya. Selanjutnya, tata letak fisik dasar (perangkat keras) atau topologi jaringan area lokal yang paling umum ditemukan dibahas, diikuti dengan survei protokol kontrol akses menengah (perangkat lunak) yang memungkinkan stasiun kerja mengirimkan data pada jaringan. Kami kemudian akan memeriksa produk jaringan area lokal yang paling umum, seperti berbagai versi Ethernet. Sebelum kita mulai memeriksa konfigurasi dasarnya, mari kita bahas fungsi utama serta kelebihan dan kekurangan jaringan area lokal.

7.2 FUNGSI UTAMA JARINGAN AREA LOKAL

Untuk lebih memahami kemampuan jaringan area lokal, mari kita periksa fungsi utamanya, dan beberapa aktivitas umum serta area penerapannya. Mayoritas pengguna mengharapkan jaringan area lokal menyediakan akses ke sumber daya perangkat keras dan perangkat lunak yang memungkinkan mereka melakukan satu atau lebih aktivitas berikut di lingkungan kantor, akademik, atau manufaktur: penyajian file, penyajian basis data dan aplikasi, penyajian cetak, Akses internet, email, transfer video dan musik, kontrol dan pemantauan proses, dan pemrosesan terdistribusi.

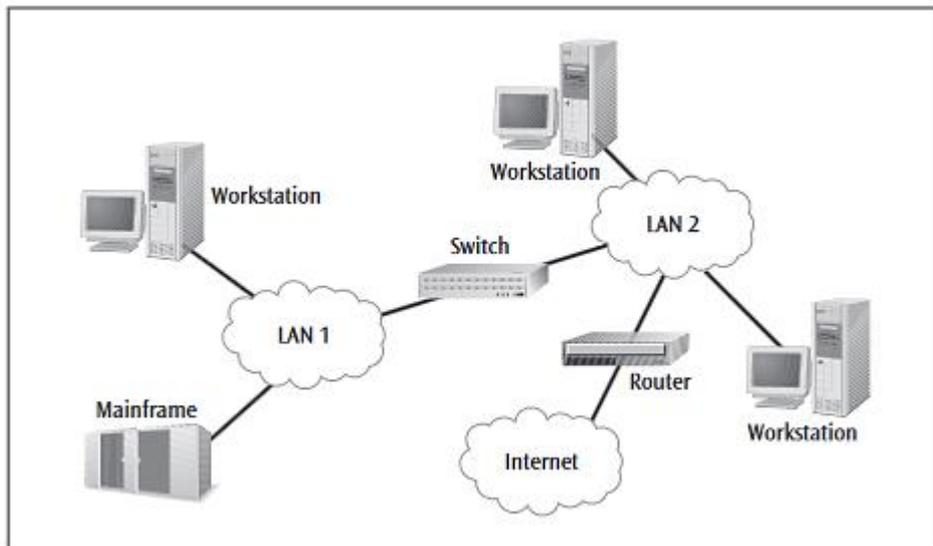
Jaringan area lokal melakukan penyajian file ketika terhubung ke stasiun kerja dengan drive disk penyimpanan besar yang bertindak sebagai repositori penyimpanan pusat, atau server file. Misalnya, ketika jaringan area lokal menawarkan akses ke aplikasi tingkat tinggi seperti aplikasi manajemen proyek komersial, jaringan menyimpan perangkat lunak manajemen proyek (atau sebagian darinya) di server file dan mentransfer salinannya ke server. Stasiun kerja yang sesuai sesuai permintaan.

Dengan menyimpan semua aplikasi di server—atau lebih mungkin, sebagian di server dan sebagian lagi di stasiun kerja klien—jaringan dapat mengontrol akses ke perangkat lunak dan dapat mengurangi jumlah penyimpanan disk yang diperlukan di setiap stasiun kerja pengguna. Untuk aplikasi ini. Sebagai contoh kedua, misalkan dua atau lebih pengguna ingin berbagi kumpulan data. Dalam hal ini, kumpulan data, seperti perangkat lunak aplikasi, akan disimpan di server file, sementara jaringan menyediakan akses kepada pengguna yang memiliki izin yang sesuai.

Jaringan area lokal juga dapat menyediakan akses ke satu atau lebih printer berkualitas tinggi. Perangkat lunak jaringan area lokal yang disebut server cetak memberi stasiun kerja otorisasi untuk mengakses printer tertentu, menerima dan mengantri pekerjaan pencetakan, mencetak lembar sampul, dan memungkinkan pengguna mengakses antrian pekerjaan untuk fungsi administratif rutin.

Sebagian besar jaringan area lokal menyediakan layanan pengiriman dan penerimaan email. Layanan email ini dapat beroperasi baik di dalam jaringan area lokal maupun antara jaringan area lokal dan jaringan lain, seperti Internet. Disimpan di suatu tempat di jaringan adalah database pesan email, baik lama maupun baru. Saat pengguna masuk untuk mengakses email mereka, pesan mereka disimpan dan diambil dari server email.

Jaringan area lokal dapat berinteraksi dengan jaringan area lokal lainnya, jaringan area luas (seperti Internet), dan komputer mainframe. Dengan demikian, jaringan area lokal adalah landasan yang menyatukan berbagai jenis sistem dan jaringan komputer. Sebuah perusahaan dapat menggunakan kemampuan antarmuka jaringan area lokal untuk memungkinkan karyawannya berinteraksi dengan orang-orang di luar perusahaan, seperti pelanggan dan pemasok. Misalnya, jika karyawan ingin mengirimkan pesanan pembelian ke vendor, mereka dapat memasukkan transaksi di stasiun kerja mereka. Transaksi ini akan melintasi jaringan area lokal perusahaan, yang akan terhubung ke jaringan area luas. Pemasok pada akhirnya akan menerima pesanan dengan terhubung ke jaringan area luas ini melalui jaringan area lokal mereka sendiri. Gambar 7-1 menunjukkan interkoneksi tipikal antara jaringan area lokal dan entitas lainnya.



Gambar 7-1 Jaringan area lokal yang menghubungkan jaringan area lokal lain, Internet, dan komputer mainframe

Merupakan hal yang umum untuk menghubungkan satu jaringan area lokal ke jaringan area lokal lainnya melalui perangkat seperti switch. Yang sama umum adalah interkoneksi jaringan area lokal ke jaringan area luas melalui router. Jaringan area lokal juga dapat dihubungkan ke komputer mainframe untuk memungkinkan kedua entitas berbagi sumber daya satu sama lain. Sebagian besar, jika tidak semua, jaringan area lokal saat ini menyediakan kemampuan mentransfer gambar video dan streaming video. Misalnya, jaringan area lokal memungkinkan pengguna untuk mentransfer gambar grafik resolusi tinggi, mentransfer aliran video, dan melakukan telekonferensi antara dua atau lebih pengguna.

Di lingkungan manufaktur dan industri, jaringan area lokal sering digunakan untuk memantau peristiwa manufaktur dan melaporkan serta mengendalikan kejadiannya. Jaringan area lokal menyediakan kontrol dan pemantauan proses. Jalur perakitan mobil yang menggunakan sensor untuk memantau mobil yang sebagian selesai dan mengendalikan robot untuk perakitan adalah contoh yang sangat baik dari jaringan area lokal yang menjalankan fungsi kontrol proses.

Tergantung pada jenis jaringan dan pilihan sistem operasi jaringan, jaringan area lokal dapat mendukung pemrosesan terdistribusi, di mana tugas dibagi lagi dan dikirim ke stasiun kerja jarak jauh di jaringan untuk dieksekusi. Seringkali, stasiun kerja jarak jauh ini menganggur; dengan demikian, tugas pemrosesan terdistribusi berarti “mencuri” waktu CPU dari mesin lain (dan sering disebut komputasi grid). Hasil eksekusi jarak jauh ini kemudian dikembalikan ke workstation asal untuk disebarluaskan atau diproses lebih lanjut. Dengan mendelegasikan tugas ke komputer yang paling mampu menangani tugas-tugas tertentu, pembagian tugas atau bagian tugas dapat meningkatkan kecepatan eksekusi.

Selain melakukan aktivitas umum ini, jaringan area lokal dapat menjadi alat yang efektif di banyak area aplikasi. Salah satu area aplikasi yang paling umum adalah lingkungan kantor. Jaringan area lokal di kantor dapat mendukung pengolah kata, operasi spreadsheet, fungsi database, akses email, akses Internet, penjadwalan janji temu elektronik, dan kemampuan pembuatan gambar grafis melalui berbagai platform dan ke sejumlah besar stasiun kerja. Dokumen yang sudah selesai dapat dikirim ke printer berkualitas tinggi untuk menghasilkan kop surat, buletin berdesain grafis, dan dokumen formal.

Area aplikasi umum kedua untuk jaringan area lokal adalah lingkungan akademik. Dalam lingkungan laboratorium, misalnya, jaringan area lokal dapat memberikan siswa akses ke alat yang diperlukan untuk menyelesaikan pekerjaan rumah, mengirim email, dan memanfaatkan Internet. Di ruang kelas, jaringan area lokal dapat memungkinkan profesor menyampaikan tutorial dan pelajaran dengan grafis dan suara berkualitas tinggi kepada siswa. Beberapa stasiun kerja dapat digunakan untuk memberikan instruksi kepada siswa sesuai kecepatan mereka sendiri, sementara instruktur memantau dan mencatat kemajuan setiap siswa di setiap stasiun kerja.

Area aplikasi umum ketiga untuk jaringan area lokal adalah manufaktur. Faktanya, jalur perakitan modern beroperasi secara eksklusif di bawah kendali jaringan area lokal. Saat produk bergerak ke jalur perakitan, sensor mengontrol posisi; robot melakukan operasi biasa, menuntut, atau berbahaya; dan sub-perakitan produk diinventarisasi dan dipesan. Jalur perakitan mobil modern merupakan sebuah tur teknologi yang menggabungkan banyak jaringan area lokal dan komputer mainframe.

Sekarang kita sudah familiar dengan aktivitas dan penerapan jaringan area lokal yang lebih umum, mari kita periksa beberapa kelebihan dan kekurangannya.

7.3 KEUNGGULAN DAN KEKURANGAN JARINGAN AREA LOKAL

Salah satu keuntungan terbesar dari jaringan area lokal adalah kemampuannya untuk berbagi sumber daya dengan cara yang ekonomis dan efisien. Sumber daya perangkat keras bersama dapat mencakup printer berkualitas tinggi, sistem tape-backup, plotter, CD juke-box, sistem penyimpanan massal, dan perangkat keras lainnya. Di sisi perangkat lunak, jaringan area lokal memungkinkan berbagi aplikasi komersial, aplikasi in-house, dan kumpulan data dengan satu atau semua stasiun kerja pengguna. Selain itu, sehubungan dengan komunikasi, setiap stasiun kerja di jaringan area lokal dapat mengirim dan menerima pesan ke dan dari stasiun kerja dan jaringan lain. Interkomunikasi ini memungkinkan pengguna untuk mengirim

email, mengakses halaman Web, mengirim pekerjaan cetak, dan mengambil catatan database. (Efek samping yang menarik dari jaringan area lokal adalah bahwa sebuah stasiun kerja dapat bertahan dari kegagalan jaringan jika stasiun kerja tersebut tidak bergantung pada perangkat lunak atau perangkat keras yang terdapat pada stasiun kerja lain atau pada server.) Keuntungan tambahannya adalah bahwa evolusi komponen dapat independen terhadap evolusi sistem, dan sebaliknya. Misalnya, jika stasiun kerja baru diinginkan, maka dimungkinkan untuk mengganti stasiun kerja lama dengan yang lebih baru dengan sedikit, jika ada, perubahan yang diperlukan pada jaringan itu sendiri. Demikian pula, jika satu atau lebih komponen jaringan menjadi usang, komponen jaringan dapat ditingkatkan tanpa mengganti atau mengubah stasiun kerja individual secara radikal.

Dalam kondisi tertentu, jaringan area lokal memungkinkan peralatan dari produsen berbeda untuk digabungkan dalam jaringan yang sama. Misalnya, dimungkinkan untuk membuat jaringan area lokal yang menggabungkan komputer pribadi tipe IBM dengan mikrokomputer Apple. Dua keuntungan lain dari jaringan area lokal adalah kecepatan transfer yang tinggi dan tingkat kesalahan yang rendah. Jaringan area lokal biasanya memiliki kecepatan transfer data dari 10 juta bit per detik hingga 10 miliar bit per detik. Karena tarif ini, dokumen dapat ditransfer melalui jaringan area lokal dengan cepat dan percaya diri. Terakhir, karena jaringan area lokal dapat dibeli langsung, seluruh jaringan dan semua stasiun kerja serta perangkat dapat dimiliki dan dipelihara secara pribadi. Dengan demikian, perusahaan dapat menawarkan layanan yang diinginkan dengan menggunakan perangkat keras dan perangkat lunak yang dianggap terbaik bagi karyawannya.

Namun menariknya, beberapa perusahaan mulai memandang pembelian peralatan sebagai suatu kerugian. Mendukung seluruh perusahaan dengan sumber daya komputasi yang tepat sangatlah mahal. Tidaklah membantu jika komputer mencapai ulang tahunnya yang pertama, ada komputer yang lebih baru, lebih cepat, dan lebih murah menunggu untuk dibeli. Oleh karena itu, beberapa perusahaan menyewa peralatan jaringan area lokal dan stasiun kerja komputer atau menyewa pihak ketiga untuk mendukung jaringan mereka.

Selain itu, jaringan area lokal memiliki sejumlah kelemahan. Pertama, perangkat keras jaringan area lokal, sistem operasi, dan perangkat lunak yang berjalan di jaringan bisa jadi mahal. Komponen LAN yang memerlukan pendanaan besar antara lain server jaringan, sistem operasi jaringan, sistem pengkabelan jaringan termasuk switch dan router, aplikasi berbasis jaringan, keamanan jaringan, serta dukungan dan pemeliharaan. Terlepas dari kenyataan bahwa jaringan area lokal dapat mendukung banyak jenis perangkat keras dan perangkat lunak, berbagai jenis perangkat keras dan perangkat lunak mungkin tidak dapat saling beroperasi. Misalnya, meskipun jaringan area lokal mendukung dua jenis sistem basis data yang berbeda, pengguna mungkin tidak dapat berbagi data antara kedua sistem basis data tersebut. Kerugian lainnya adalah potensi pembelian perangkat lunak dengan lisensi pengguna yang salah. Misalnya, hampir selalu ilegal untuk membeli salinan perangkat lunak untuk satu pengguna dan kemudian menginstalnya di jaringan area lokal agar dapat diakses oleh banyak pengguna. Untuk menghindari penggunaan perangkat lunak secara ilegal,

perusahaan harus mengetahui perjanjian lisensi khusus yang terkait dengan jaringan area lokal.

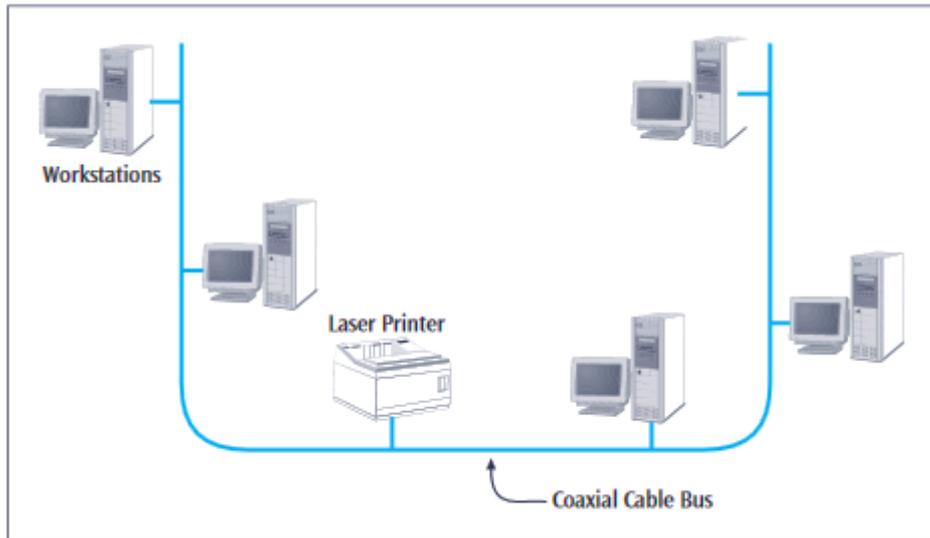
Kelemahan penting yang sering diabaikan di masa lalu adalah bahwa pengelolaan dan pengendalian jaringan area lokal memerlukan dedikasi dan layanan berjam-jam. Seorang manajer, atau administrator jaringan, dari jaringan area lokal harus terlatih dengan baik dan tidak berasumsi bahwa jaringan dapat mendukung dirinya sendiri hanya dengan beberapa jam perhatian per minggu. Oleh karena itu, jaringan area lokal memerlukan staf dan pengetahuan khusus, serta perangkat keras dan perangkat lunak diagnostik yang tepat. Sayangnya, berjam-jam waktu dukungan ini sering kali dihabiskan untuk melawan virus dan masalah keamanan jaringan lainnya (Bab Dua Belas dikhususkan sepenuhnya untuk masalah keamanan jaringan). Terakhir, jaringan area lokal hanya sekuat link terlemahnya. Misalnya, suatu jaringan mungkin sangat menderita jika server file tidak dapat melayani semua permintaan dari pengguna jaringan secara memadai. Setelah meningkatkan server, perusahaan mungkin menemukan bahwa pemasangan kabel tidak lagi mampu mendukung lalu lintas yang lebih tinggi. Setelah memperbaiki kabel, mungkin terlihat bahwa sistem operasi jaringan tidak lagi mampu menjalankan fungsi yang diperlukan. Peningkatan pada bagian jaringan dapat menyebabkan efek riak di seluruh jaringan, dan siklus peningkatan biasanya berlanjut hingga tiba waktunya untuk meningkatkan server lagi.

Mengingat semua kelebihan dan kekurangan yang terkait dengan jaringan area lokal, tidak mengherankan bahwa keputusan untuk memasukkan LAN ke dalam lingkungan yang ada memerlukan banyak perencanaan, pelatihan, dukungan, dan uang. Sekarang mari kita lihat lebih dekat bagaimana workstation di jaringan area lokal saling berhubungan untuk melayani aktivitas dan aplikasi yang dibahas sejauh ini.

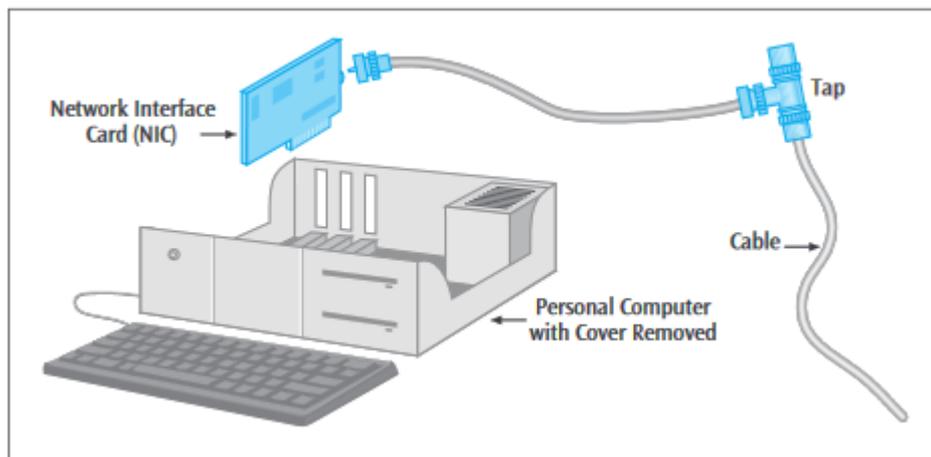
7.4 JARINGAN AREA LOKAL PERTAMA: BUS/TREE

Jaringan area lokal bus/tree, sering disebut bus LAN, adalah desain fisik pertama ketika LAN tersedia secara komersial pada akhir tahun 1970an. Ini pada dasarnya terdiri dari kabel sederhana, atau bus, yang menghubungkan semua perangkat. Sejak tahun 1970an, penggunaan bus sebagai konfigurasi jaringan area lokal telah berkurang hingga titik kepunahan. Namun menarik untuk dicatat bahwa sinyal televisi kabel masih dikirimkan melalui bus jaringan. Oleh karena itu, pemahaman tentang jaringan bus/pohon masih penting. Seperti yang ditunjukkan pada Gambar 7-2, bus hanyalah sebuah kabel koaksial linier yang digunakan oleh beberapa perangkat atau stasiun kerja.

Ketika suatu perangkat melakukan transmisi di bus, semua perangkat lain yang terhubung menerima transmisi. Menghubungkan ke kabel memerlukan perangkat sederhana yang disebut tap (Gambar 7-3). Keran ini merupakan perangkat pasif karena tidak mengubah sinyal dan tidak memerlukan listrik untuk beroperasi. Di ujung kabel stasiun kerja terdapat kartu antarmuka jaringan. Kartu antarmuka jaringan (NIC) adalah perangkat elektronik, terkadang dalam bentuk papan sirkuit komputer atau bagian dari papan sirkuit yang lebih besar, yang melakukan konversi sinyal dan operasi protokol yang diperlukan yang memungkinkan stasiun kerja mengirim dan menerima data di jaringan.



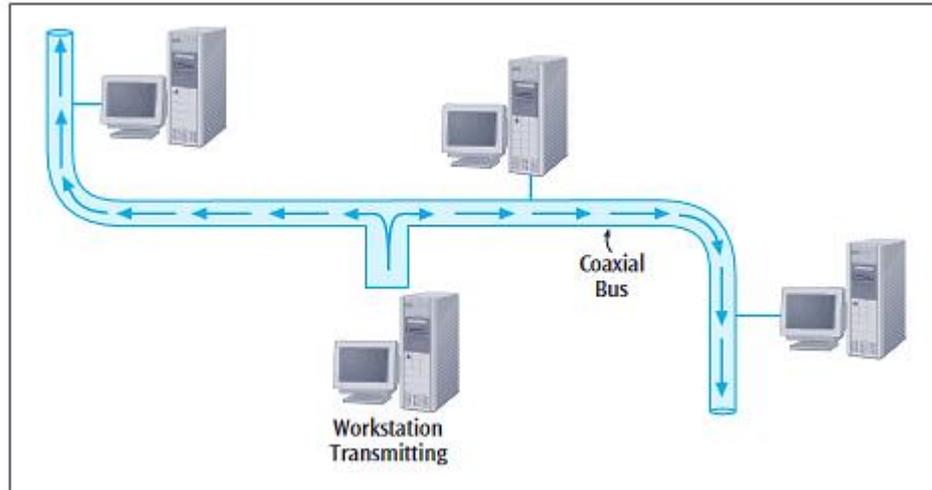
Gambar 7-2 Diagram sederhana topologi bus jaringan area lokal



Gambar 7-3 Ketuk yang digunakan untuk menghubungkan workstation dan kabel LAN

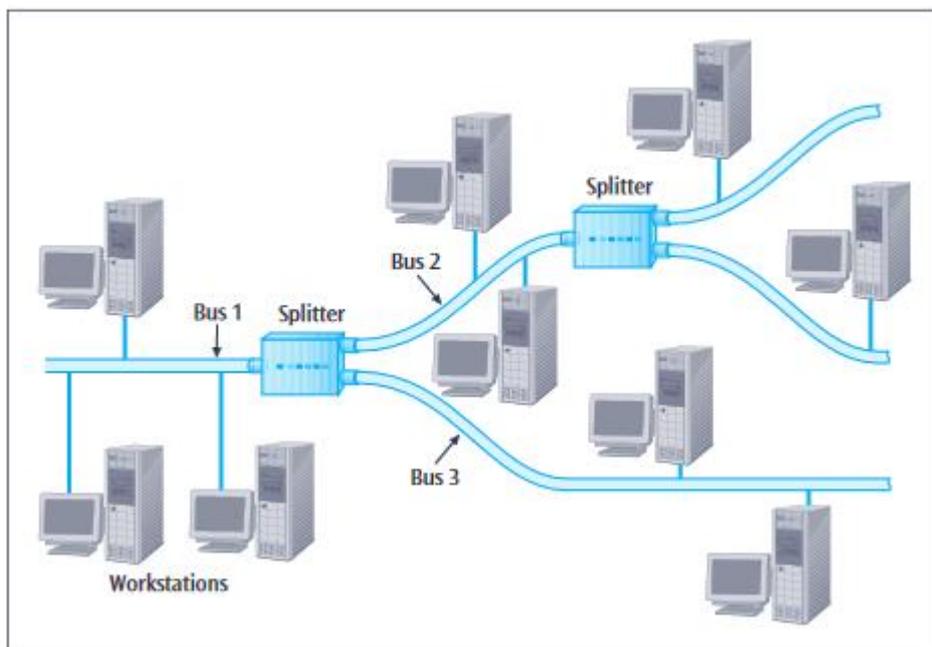
Dua teknologi pensinyalan berbeda dapat digunakan dengan jaringan bus: pensinyalan pita dasar dan pensinyalan pita lebar. (Ingat bahwa pensinyalan baseband dan pensinyalan broadband diperkenalkan di Bab Tiga selama diskusi tentang kabel koaksial.) Pensinyalan baseband biasanya menggunakan sinyal digital tunggal (seperti pengkodean Manchester) untuk mengirimkan data melalui bus. Sinyal digital tunggal ini menggunakan seluruh spektrum kabel; oleh karena itu, hanya satu sinyal pada satu waktu yang dapat ditransmisikan melalui kabel. Semua stasiun kerja harus menyadari bahwa stasiun kerja lain sedang melakukan transmisi, sehingga mereka tidak mencoba melakukan transmisi dan dengan demikian secara tidak sengaja menghancurkan sinyal pemancar pertama. Mengizinkan hanya satu stasiun kerja mengakses media pada satu waktu adalah tanggung jawab protokol kontrol akses media, yang akan dibahas secara rinci nanti di bab ini.

Karakteristik lain dari teknologi baseband yang perlu diperhatikan adalah transmisi baseband bersifat dua arah, yang berarti bahwa ketika sinyal ditransmisikan dari stasiun kerja tertentu, sinyal tersebut merambat menjauhi sumber di kedua arah pada kabel (Gambar 7-4).



Gambar 7-4 Propagasi dua arah dari sinyal baseband

Jenis teknologi persinyalan kedua yang digunakan pada jaringan area lokal bus adalah teknologi broadband (ingat bahwa hanya sistem televisi kabel yang masih menggunakan persinyalan broadband). Teknologi broadband menggunakan sinyal analog dalam bentuk multiplexing pembagian frekuensi untuk membagi media yang tersedia menjadi beberapa saluran. Setiap saluran mampu membawa satu aliran video, audio, atau data.



Gambar 7-5 Contoh sederhana topologi pohon broadband

Dimungkinkan juga untuk memisahkan dan menggabungkan kabel dan sinyal broadband untuk membuat konfigurasi yang lebih kompleks daripada bus linier tunggal. Topologi bus yang lebih kompleks yang terdiri dari beberapa segmen kabel yang saling berhubungan disebut pohon. Gambar 7-5 menunjukkan contoh jaringan pohon.

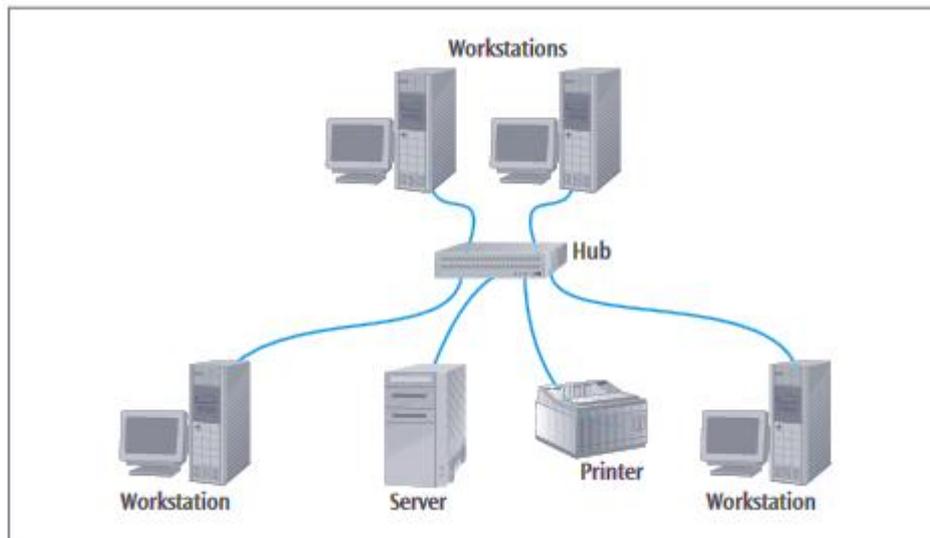
Semua jaringan bus—baik broadband atau baseband—memiliki kelemahan besar. Secara umum, sulit untuk menambahkan workstation baru jika saat ini tidak ada tap. Karena tidak ada keran, maka kabel harus dipotong, dan keran harus dipasang. Memotong kabel dan memasukkan keran akan mengganggu lalu lintas jaringan dan merupakan pekerjaan yang agak berantakan. Cara terbaik untuk menghindari hal ini adalah dengan mengantisipasi lokasi stasiun kerja dan meminta tim instalasi memasang semua keran yang diperlukan terlebih dahulu. Namun, seperti yang Anda duga, memprediksi jumlah dan lokasi keran secara pasti hampir mustahil dilakukan. Dengan diperkenalkannya teknologi baru, jaringan area lokal berbasis bus telah kehilangan popularitas hingga saat ini hanya ada sedikit LAN berbasis bus. Satu-satunya bus yang masih sering digunakan, seperti telah kita lihat, adalah bus yang menyalurkan sinyal video dan data dari televisi kabel. Salah satu alasannya adalah, jika Anda ingat, kabel koaksial merupakan media yang baik untuk mentransmisikan sinyal frekuensi tinggi dari televisi kabel.

Mari kita periksa teknologi yang menggantikan bus jaringan area lokal: bus kabel bintang.

7.5 LAN YANG LEBIH MODERN

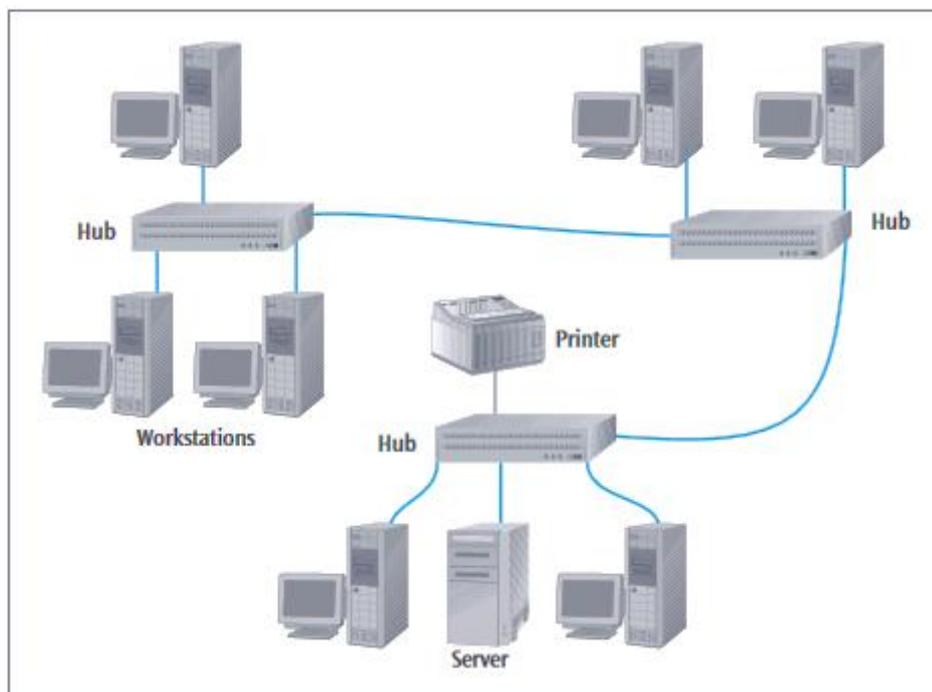
Konfigurasi paling populer untuk jaringan area lokal saat ini adalah LAN bus kabel bintang. Jaringan bus kabel bintang modern saat ini berfungsi seperti bus namun terlihat seperti bintang. Lebih tepatnya, jaringan secara logis bertindak sebagai bus, namun secara fisik terlihat seperti bintang. Desain logis suatu jaringan menentukan bagaimana data berpindah di sekitar jaringan dari stasiun kerja ke stasiun kerja lainnya. Rancangan fisik mengacu pada pola yang dibentuk oleh lokasi elemen-elemen jaringan, seperti yang terlihat jika digambar pada selembar kertas. Mari kita jelajahi rincian perbedaan penting ini lebih jauh.

Pada jaringan bus kabel bintang pertama, semua stasiun kerja terhubung ke perangkat pusat seperti hub, seperti terlihat pada Gambar 7-6. Hub adalah perangkat yang relatif tidak cerdas yang secara sederhana dan segera mentransmisikan kembali data yang diterimanya dari stasiun kerja mana pun ke semua stasiun kerja (atau perangkat) lain yang terhubung ke hub. Semua stasiun kerja mendengar data yang dikirimkan karena hanya ada satu saluran transmisi, dan semua stasiun kerja menggunakan satu saluran ini untuk mengirim dan menerima. Mengirim data ke semua stasiun kerja dan perangkat menghasilkan banyak lalu lintas tetapi menjaga pengoperasian tetap sederhana karena tidak ada perutean ke stasiun kerja tertentu. Jadi, sehubungan dengan desain logisnya, bus kabel bintang bertindak sebagai bus: Ketika stasiun kerja melakukan transmisi, semua stasiun kerja (atau perangkat) segera menerima data. Desain fisik jaringan, bagaimanapun, adalah sebuah bintang karena semua perangkat terhubung ke hub dan memancar ke luar dalam pola seperti bintang (bukan linier).



Gambar 7-6 Contoh sederhana jaringan area lokal bus kabel bintang

Hub di pusat jaringan bus kabel bintang hadir dalam berbagai desain. Ini dapat berisi dua hingga ratusan koneksi, atau port, demikian sebutannya. Jika, misalnya, Anda memiliki hub dengan 24 port, dan diinginkan lebih banyak, cukup mudah untuk menghubungkan dua hub atau lebih, atau membeli hub yang lebih besar. Gambar 7-7 menunjukkan bahwa untuk menghubungkan dua hub, Anda cukup menjalankan kabel dari konektor khusus di depan atau belakang hub pertama ke konektor khusus di depan atau belakang hub kedua. Banyak hub mendukung berbagai jenis media—twisted pair, kabel koaksial, dan kabel serat optik—untuk koneksi interhub ini.



Gambar 7-7 Interkoneksi tiga hub dalam jaringan area lokal bus kabel bintang

Kabel twisted pair telah menjadi media pilihan untuk LAN bus kabel bintang, sedangkan kabel serat optik biasanya digunakan sebagai konektor antara beberapa hub. Konektor di ujung kabel twisted pair adalah konektor RJ-45 modular yang mudah digunakan. Konektor RJ-45 sangat mirip, namun sedikit lebih lebar dari, konektor modular yang menghubungkan telepon ke soket dinding (konektor RJ-11). (Anda akan melihat ini ketika Anda memasukkan konektor RJ-11 ke jack RJ-45. Ini agak cocok, tetapi tidak akan berfungsi.) Kabel twisted pair dan konektor modular membuatnya lebih mudah untuk menambahkan workstation ke star- bus kabel dibandingkan bus kabel koaksial.

Banyak keuntungan dari LAN bus kabel bintang termasuk instalasi dan pemeliharaan yang sederhana, komponen berbiaya rendah (seperti hub dan kabel twisted pair), dan sejumlah besar produk yang kompatibel karena pangsa pasar yang besar. Mungkin satu-satunya kelemahan dari desain bus kabel bintang adalah jumlah lalu lintas yang harus ditangani oleh hubnya. Ketika dua atau lebih hub saling terhubung dan sebuah stasiun kerja mengirimkan data, semua stasiun kerja yang terhubung ke semua hub menerima data tersebut. Ini adalah contoh jaringan bersama. Semua perangkat di jaringan berbagi satu bandwidth. Seperti yang telah disebutkan, hub merupakan perangkat yang relatif tidak cerdas. Itu tidak memfilter bingkai data apa pun, dan tidak melakukan perutean apa pun. Ternyata, hal ini telah menjadi masalah besar pada LAN berbasis hub dan menyebabkan hampir semua hub diganti. Namun sebelum kita membahas pengganti hub, mari kita lihat perangkat lunak yang beroperasi melalui LAN berbasis hub.

Protokol kontrol akses menengah adalah perangkat lunak yang memungkinkan perangkat menempatkan data ke jaringan area lokal berbasis hub (serta jaringan lain yang memerlukan stasiun kerjanya bersaing untuk mendapatkan akses ke jaringan). Sampai beberapa tahun yang lalu, inti dari semua protokol kontrol akses menengah adalah sebagai berikut: Karena jaringan area lokal pada dasarnya adalah sebuah bus tunggal yang menggunakan teknologi baseband, maka sangat penting bahwa hanya satu stasiun kerja pada satu waktu yang diizinkan untuk mengirimkan datanya ke jaringan. - bekerja. Keharusan ini, seperti yang akan kita lihat sebentar lagi, telah berubah dengan diperkenalkannya switch (sebagai pengganti hub) dan koneksi full-duplex. Namun untuk saat ini, kami akan berkonsentrasi pada satu stasiun kerja yang melakukan transmisi pada satu waktu.

Dua kategori dasar protokol kontrol akses menengah untuk jaringan area lokal adalah:

- Protokol berbasis Collision (pertentangan), seperti operator merasakan akses ganda dengan deteksi tabrakan
- Protokol round-robin, seperti token passing

Protokol berbasis pertentangan

Protokol berbasis pertentangan pada dasarnya adalah protokol siapa cepat dia dapat: Stasiun pertama yang mengenali bahwa tidak ada stasiun lain yang mentransmisikan data dan menempatkan datanya ke media adalah stasiun pertama yang melakukan transmisi. Protokol berbasis pertentangan yang paling populer adalah Carrier Sense Multiple Access dengan Collision Detection (CSMA/CD). Protokol kontrol akses medium CSMA/CD ditemukan hampir

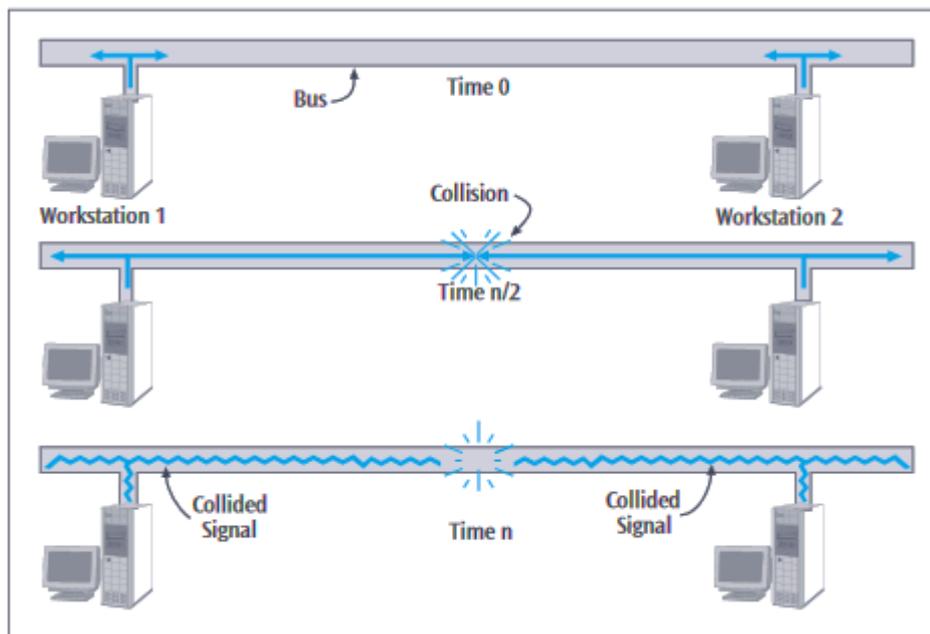
secara eksklusif pada jaringan area lokal bus dan bus kabel bintang, dan selama bertahun-tahun merupakan protokol kontrol akses medium yang paling banyak digunakan.

Nama protokol ini sangat panjang sehingga hampir dapat menjelaskan dirinya sendiri. Dengan protokol CSMA/CD, hanya satu workstation pada satu waktu yang dapat melakukan transmisi; dan karena itu, protokol CSMA/CD pada dasarnya adalah protokol setengah dupleks. Sebuah stasiun kerja mendengarkan medium—yakni, merasakan pembawa pesan pada medium tersebut—untuk mengetahui apakah ada stasiun kerja lain yang melakukan transmisi. Jika stasiun kerja lain sedang melakukan transmisi, stasiun kerja yang ingin melakukan transmisi akan menunggu dan mencoba lagi untuk melakukan transmisi. Lamanya waktu tunggu stasiun kerja bergantung pada jenis protokol CSMA/CD tertentu yang digunakan. Jika tidak ada stasiun kerja lain yang secara aktif melakukan transmisi, stasiun kerja tersebut mengirimkan datanya ke media. Protokol akses CSMA/CD dianalogikan dengan manusia yang melakukan percakapan di meja makan. Jika tidak ada yang berbicara, seseorang dapat berbicara. Jika seseorang sedang berbicara, semua orang akan mendengarnya dan menunggu. Jika dua orang mulai berbicara pada saat yang sama, mereka berdua akan segera berhenti (atau setidaknya orang yang sopan melakukannya) dan menunggu beberapa saat sebelum mencoba lagi.

Dalam kebanyakan situasi, data yang dikirim oleh stasiun kerja ditujukan untuk satu stasiun kerja lain, namun semua stasiun kerja di jaringan berbasis protokol CSMA/CD menerima data tersebut. (Sekali lagi, kita akan melihat bahwa hal ini tidak lagi berlaku pada jaringan area lokal yang diaktifkan.) Hanya stasiun kerja yang dituju (stasiun kerja dengan alamat yang dituju) yang akan melakukan sesuatu dengan data. Semua stasiun kerja lainnya akan membuang kerangka data.

Saat data sedang dikirim, stasiun kerja pengirim terus mendengarkan media, mendengarkan transmisinya sendiri. Dalam kondisi normal, workstation seharusnya hanya mendengar datanya sendiri yang sedang dikirim. Namun, jika stasiun kerja mendengar suara sampah, maka diasumsikan telah terjadi tabrakan. Tabrakan terjadi ketika dua atau lebih stasiun kerja mendengarkan media pada saat yang sama, tidak mendengar apa pun, dan kemudian mengirimkan datanya pada saat yang sama.

Sebenarnya, kedua stasiun kerja tidak perlu memulai transmisi pada saat yang bersamaan agar tabrakan dapat terjadi. Pertimbangkan situasi di mana dua stasiun kerja berada di ujung bus yang berlawanan. Sebuah sinyal merambat dari satu ujung bus ke ujung lainnya dalam waktu n . Sebuah stasiun kerja tidak akan mendengar tabrakan sampai datanya, rata-rata, menempuh separuh jalan bus, bertabrakan dengan sinyal stasiun kerja lain, dan kemudian disebarkan kembali ke bus ke stasiun pertama (Gambar 7-8). Interval ini, selama sinyal merambat ke bawah dan ke belakang bus, disebut jendela tumbukan. Selama jendela tabrakan ini, workstation mungkin tidak mendengar transmisi, berasumsi secara salah bahwa tidak ada orang yang melakukan transmisi, dan kemudian mengirimkan datanya.



Gambar 7-8 Dua stasiun kerja di ujung bus yang berlawanan mengalami tabrakan

Jika jaringan mengalami sedikit lalu lintas, kemungkinan terjadinya tabrakan kecil. Peluang terjadinya tabrakan meningkat secara dramatis ketika jaringan berada di bawah beban berat dan banyak stasiun kerja mencoba mengaksesnya secara bersamaan. Penelitian telah menunjukkan bahwa ketika lalu lintas pada jaringan CSMA/CD meningkat, tingkat tabrakan meningkat, yang selanjutnya menurunkan layanan jaringan. Jika workstation mendeteksi adanya tabrakan, maka workstation akan segera menghentikan transmisinya, menunggu beberapa waktu secara acak, dan kemudian mencoba lagi. Jika terjadi tabrakan lagi, workstation akan menunggu sekali lagi. Karena tabrakan ini, jaringan CSMA/CD yang sibuk jarang melebihi 40 persen throughput. Dengan kata lain, jaringan CSMA/CD yang sibuk membuang 60 persen waktunya untuk menangani tabrakan dan overhead lainnya. Banyak pengguna menganggap angka ini tidak dapat diterima dan mempertimbangkan modifikasi terhadap CSMA/CD standar, seperti menggunakan switch dan bukan hub.

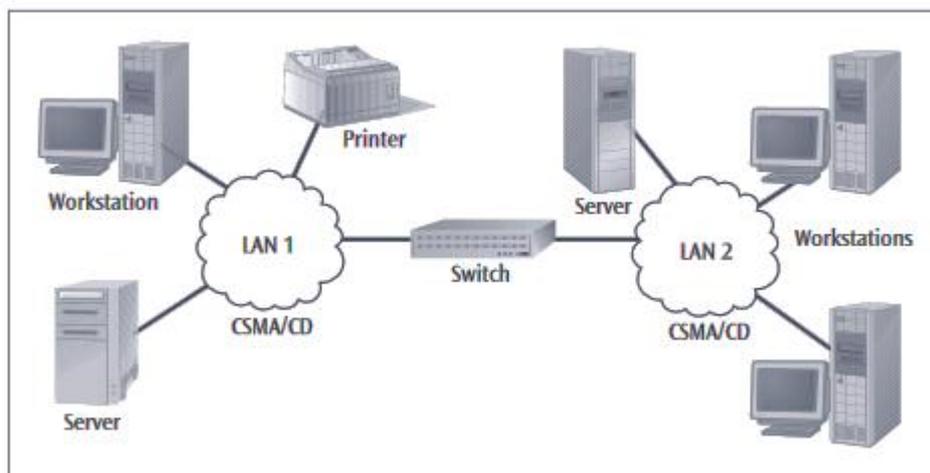
Karena berapa kali stasiun kerja harus menunggu tidak diketahui, maka tidak mungkin untuk menentukan secara pasti kapan stasiun kerja diperbolehkan mengirimkan datanya tanpa tabrakan. Dengan demikian, CSMA/CD adalah protokol nondeterministik. Protokol nondeterministik adalah protokol yang tidak dapat menghitung waktu transmisi pada stasiun kerja. Jika aplikasi Anda harus memiliki workstation yang mengirimkan data pada waktu yang diketahui, Anda mungkin ingin mempertimbangkan protokol kontrol akses medium selain bentuk dasar CSMA/CD ini.

Apa yang bisa kita lakukan untuk mengurangi jumlah tabrakan? Kita perlu mengganti hub kita dengan switch.

7.6 SWITCH

Hub adalah perangkat sederhana yang hampir tidak memerlukan overhead untuk beroperasi. Tapi itu juga tidak efisien. Ketika suatu jaringan mengalami tingkat lalu lintas yang tinggi, hub menambah masalah dengan mengambil frame yang masuk dan mengirimkannya kembali ke semua koneksi. Sebaliknya, switch menggunakan alamat dan kekuatan pemrosesan untuk mengarahkan frame keluar dari port tertentu, sehingga mengurangi jumlah lalu lintas di jaringan.

Switch, seperti hub, dapat digunakan untuk menghubungkan beberapa workstation pada satu LAN atau untuk menghubungkan beberapa LAN. Baik untuk menghubungkan beberapa jaringan area lokal atau beberapa stasiun kerja, switch mempunyai satu fungsi utama: mengarahkan frame data hanya ke penerima yang dituju. Oleh karena itu, switch perlu mengetahui di mana semua perangkat berada sehingga dapat mengirimkan data melalui link yang sesuai. Ia tidak mengirimkan frame keluar semua link, seperti yang dilakukan hub (kecuali frame datanya adalah pesan siaran). Jadi, saklar bertindak sebagai filter. Filter memeriksa alamat tujuan dari sebuah frame dan meneruskan frame tersebut dengan tepat, tergantung pada beberapa informasi alamat yang disimpan dalam switch. Switch akan sangat mengurangi jumlah lalu lintas pada jaringan yang saling terhubung dengan membuang frame yang tidak harus diteruskan.

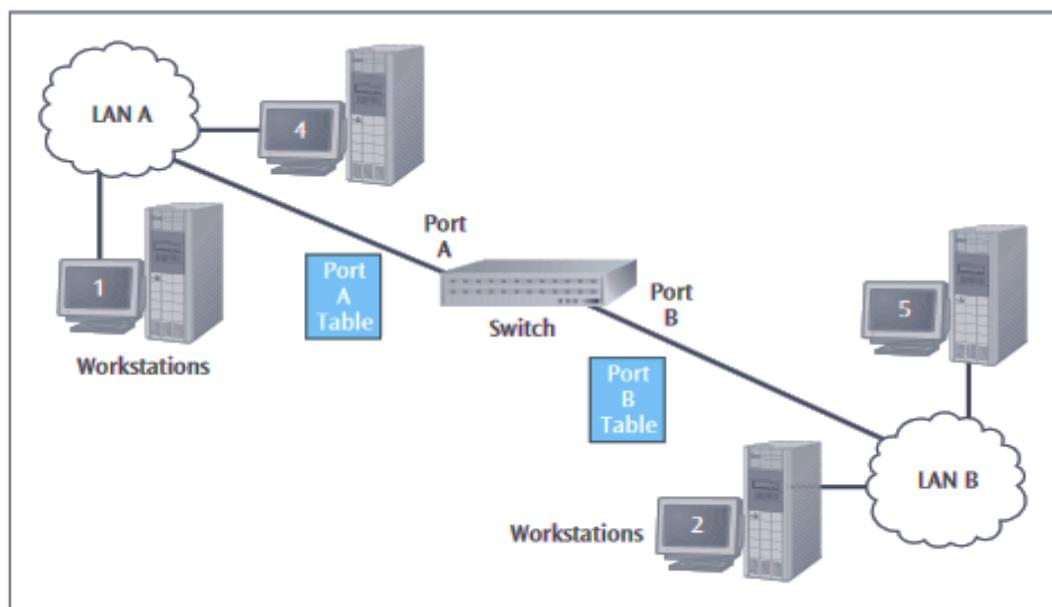


Gambar 7-9 Sebuah saklar yang menghubungkan dua jaringan area lokal

Mari kita periksa fungsi penyaringan ini lebih dekat (Gambar 7-9). Saat frame data bergerak melintasi jaringan area lokal pertama dan memasuki switch, switch memeriksa alamat sumber dan tujuan yang disimpan dalam frame. Alamat frame ini ditetapkan ke NIC ketika NIC diproduksi. (Semua perusahaan yang memproduksi NIC telah sepakat untuk menggunakan formula yang memastikan bahwa setiap NIC di dunia memiliki alamat NIC yang unik.) Switch, menggunakan beberapa bentuk logika internal, menentukan apakah alamat tujuan bingkai data milik stasiun kerja di jaringan saat ini. Jika ya, switch tidak melakukan apa-apa lagi dengan frame tersebut karena sudah berada pada jaringan yang sesuai. Jika alamat tujuan bukan merupakan alamat pada jaringan saat ini, switch meneruskan frame tersebut ke

jaringan area lokal berikutnya, dengan asumsi bahwa frame tersebut ditujukan untuk stasiun di jaringan tersebut.

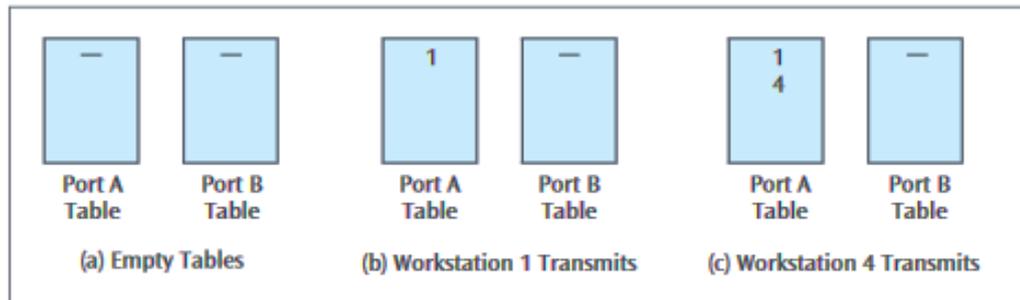
Bagaimana switch mengetahui alamat apa yang ada di jaringan mana? Apakah seorang teknisi duduk dan mengetikkan alamat setiap NIC pada setiap jaringan yang saling terhubung? Tidak mungkin. Kebanyakan saklar bersifat transparan, yang berarti mereka belajar sendiri. Setelah instalasi, switch mulai mengamati alamat frame dalam transmisi pada jaringan saat ini dan membuat tabel port internal yang akan digunakan untuk membuat keputusan penerusan di masa depan. Switch membuat tabel port internal dengan menggunakan suatu bentuk pembelajaran mundur—yakni dengan mengamati lokasi asal frame. Jika sebuah frame berada pada jaringan saat ini, switch mengasumsikan bahwa frame tersebut berasal dari suatu tempat di jaringan tersebut. Switch mengambil alamat sumber dari frame dan menempatkannya ke dalam tabel internal. Setelah mengamati lalu lintas selama beberapa saat, switch memiliki tabel alamat stasiun kerja untuk jaringan tersebut. Jika sebuah frame tiba di switch dengan alamat tujuan yang tidak cocok dengan alamat mana pun dalam tabel, switch menganggap frame tersebut ditujukan untuk stasiun kerja di jaringan lain dan meneruskan frame tersebut ke jaringan berikutnya.



Gambar 7-10 Sebuah saklar yang menghubungkan dua jaringan area lokal dengan tabel port internal untuk setiap port

Untuk contoh bagaimana saklar transparan belajar, periksa Gambar 7-10 dan skenario berikut. Switch khusus ini mempunyai dua port yang aktif: satu untuk LAN A dan yang kedua untuk LAN B. Saat switch pertama kali diaktifkan, tabel port internalnya—satu untuk Port A dan satu lagi untuk Port B—kosong. Gambar 7-11(a) menunjukkan kedua tabel awalnya kosong. Sekarang misalkan Workstation 1 mentransmisikan sebuah frame yang ditujukan untuk Workstation 4. Karena jaringan ini merupakan jaringan penyiaran, frame tersebut dikirim ke semua perangkat di jaringan, termasuk switch. Switch mengekstrak alamat

Workstation 1 dan menaruhnya di tabel Port A. Ia baru mengetahui bahwa Workstation 1 berada di LAN A, seperti yang ditunjukkan pada Gambar 7-11(b). Namun, switch masih belum mengetahui alamat Workstation 4. Meskipun Workstation 4 juga berada di LAN A, switch tidak mengetahui fakta ini karena tidak ada entri dari frame masuk dalam tabel Port A untuk Workstation 4. Akibatnya, switch tidak perlu meneruskan frame keluar Port B ke LAN B.



Gambar 7-11 Dua tabel port internal dan entri barunya

Sekarang misalkan Workstation 4 mengembalikan sebuah frame ke Workstation 1. Switch mengekstrak alamat Workstation 4 dan menempatkannya di tabel Port A, seperti yang ditunjukkan pada Gambar 7-11(c). Frame ditujukan untuk Workstation 1, dan switch melihat bahwa ada entri untuk Workstation 1 di tabel Port A. Sekarang, switch mengetahui Workstation 1 ada di LAN A dan tidak meneruskan frame ke LAN B. Selain itu, jika Workstation 1 mengirimkan frame lain ke Workstation 4, switch akan melihat bahwa Workstation 4 ada di LAN A (karena entri dalam tabel Port A) dan tidak akan meneruskan frame ke LAN B.

Jika Workstation 1 mengirimkan frame ke Workstation 5, switch tidak akan mengenali alamat Workstation 5 karena tidak ada entri di tabel Port A, dan switch akan meneruskan frame tersebut ke LAN B. Switch akan melakukan fungsi pembelajaran yang sama untuk LAN B dan perbarui tabel Port B. Dengan demikian, switch mempelajari di mana stasiun kerja berada dan kemudian menggunakan informasi tersebut untuk keputusan penerusan di masa depan.

Contoh di atas menunjukkan switch hanya menggunakan dua port aktif: satu untuk setiap jaringan. Pada kenyataannya, switch dapat memiliki banyak port yang aktif. Misalnya, Anda dapat memiliki LAN dengan 50 workstation, masing-masing terhubung ke port pada switch. Untuk mendukung masing-masing port ini secara efisien, perangkat keras utama switch—yang disebut backplane—harus cukup cepat untuk mendukung agregat atau total bandwidth semua port. Misalnya, jika sebuah switch mempunyai delapan port 100 Mbps, backplane harus mendukung total 800 Mbps. Backplane ini mirip dengan bus di dalam komputer mikro. Ini memungkinkan Anda untuk menyambungkan satu atau lebih kartu sirkuit tercetak. Setiap kartu sirkuit mendukung satu port, atau koneksi, ke workstation atau perangkat lain. Jika kartu sirkuit dapat ditukar dalam keadaan panas, kartu dapat dimasukkan dan dikeluarkan saat daya ke unit masih menyala. Kemampuan ini memungkinkan pemeliharaan sakelar dengan cepat dan mudah. Saat lalu lintas masuk pada setiap port, tabel diperbarui untuk mencerminkan alamat sumber frame yang diterima. Kemudian, ketika

sebuah frame akan dikirim ke workstation lain, tabel alamat penerusan ini dikonsultasikan dan frame tersebut dikirim ke port yang optimal.

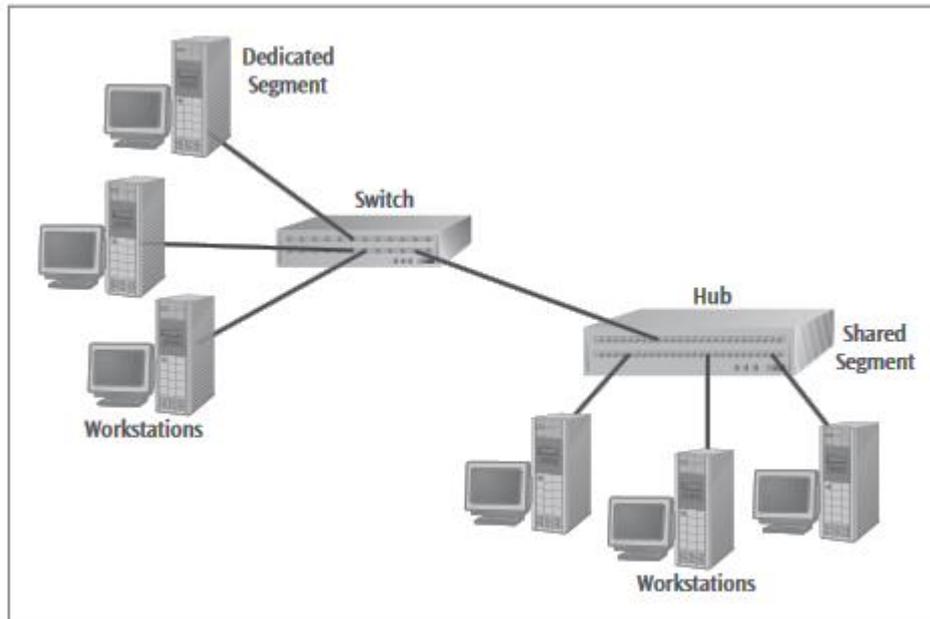
Switch dapat secara signifikan mengurangi lalu lintas interkoneksi dan meningkatkan throughput jaringan atau segmen yang saling terhubung tanpa memerlukan pemasangan kabel tambahan atau penataan ulang perangkat jaringan. Seperti yang Anda mungkin ingat, jaringan area lokal berbasis hub mengalami tabrakan. Dengan mengurangi jumlah paket yang tidak perlu dikirimkan, sebuah switch dapat menyebabkan jumlah tabrakan menurun. Ketika jumlah tabrakan menurun, keseluruhan throughput jaringan akan meningkat.

Keuntungan penting lainnya dari switch adalah ia dirancang untuk bekerja jauh lebih cepat dibandingkan hub; hal ini terutama berlaku untuk sakelar yang menggunakan arsitektur cut-through. Dalam arsitektur cut-through, frame data mulai keluar dari switch segera setelah frame tersebut mulai memasuki switch. Dengan kata lain, saklar potong tidak menyimpan bingkai data dan kemudian meneruskannya. Sebaliknya, perangkat store-and-forward menahan seluruh frame untuk waktu yang singkat sementara berbagai bidang frame diperiksa, sebuah prosedur yang mengurangi throughput jaringan secara keseluruhan. Kemampuan cut-through ini memungkinkan switch melewati frame data dengan sangat cepat, sehingga meningkatkan throughput jaringan secara keseluruhan. Kerugian utama dari arsitektur cut-through adalah potensi perangkat meneruskan frame yang salah. Misalnya, jika sebuah frame telah rusak, perangkat store-and-forward akan memasukkan frame tersebut, melakukan checksum siklik, mendeteksi kesalahan, dan melakukan beberapa bentuk pengendalian kesalahan. Namun, perangkat cut-through sangat cepat sehingga ia mulai meneruskan frame sebelum bidang cyclic checksum dapat dihitung. Jika ada kesalahan checksum siklik, sudah terlambat untuk melakukan apa pun. Bingkai sudah dikirim. Jika terlalu banyak frame rusak yang dilewatkan ke seluruh jaringan, integritas jaringan akan terganggu. Namun baru-baru ini, produsen telah membuat peralihan store-and-forward yang sangat cepat yang menyaingi kecepatan cut-through.

Switch mempunyai satu kesamaan fisik dengan hub. Jika Anda memutuskan untuk memasang saklar di jaringan area lokal, seringkali semudah mencabut hub dan mencolokkan saklar di tempat hub. Namun logikanya, switch tidak seperti hub. Switch dapat memeriksa alamat frame dan, berdasarkan isi alamat, mengarahkan frame keluar ke jalur yang sesuai. Jika hub hanya mengeluarkan salinan frame dari semua koneksi, switch menggunakan kecerdasan untuk menentukan koneksi terbaik untuk transmisi keluar.

Tergantung pada kebutuhan pengguna, switch dapat menghubungkan dua jenis segmen jaringan CSMA/CD yang berbeda: segmen bersama dan segmen khusus. Dalam jaringan segmen bersama, sebuah switch dapat dihubungkan ke sebuah hub (atau beberapa hub), yang kemudian menghubungkan beberapa workstation. Karena workstation pertama kali dihubungkan ke sebuah hub, mereka semua berbagi satu saluran, atau bandwidth, dari hub, yang membatasi kecepatan transfer masing-masing stasiun. Dalam jaringan segmen khusus, seperti yang ditunjukkan pada Gambar 7-12, sebuah switch dapat dihubungkan langsung ke satu atau lebih workstation. Setiap stasiun kerja kemudian memiliki koneksi pribadi atau khusus. Koneksi khusus ini meningkatkan bandwidth untuk setiap workstation

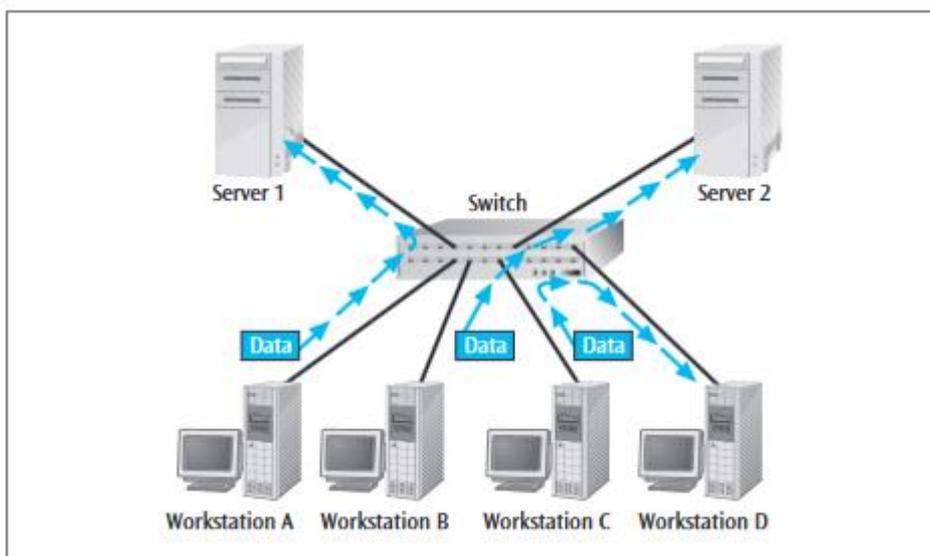
melebihi bandwidth jika workstation dihubungkan ke hub. Workstation yang tersambung ke hub tidak memiliki koneksi khusus ke jaringan. Mereka harus berbagi bandwidth dengan workstation lain yang terhubung ke hub tersebut.



Gambar 7-12 Workstation terhubung ke segmen khusus atau segmen bersama

Mengisolasi pola lalu lintas dan menyediakan banyak akses

Apakah segmen bersama atau khusus terlibat, tujuan utama dari switch adalah untuk mengisolasi pola lalu lintas tertentu dari pola lalu lintas lain atau dari sisa jaringan.



Gambar 7-13 Sebuah switch dengan dua server memungkinkan akses simultan ke masing-masing server

Pertimbangkan situasi di mana dua server, bersama dengan sejumlah workstation, terhubung ke sebuah switch (Gambar 7-13). Jika Workstation A ingin mengirimkan ke Server 1, switch meneruskan paket data/frame langsung ke Server 1 dan ke tempat lain di jaringan. Workstation B, C, dan D tidak menerima frame data dari Workstation A. Selanjutnya, Workstation A dapat mentransmisikan ke Server 1 pada saat yang sama dengan Workstation B mentransmisikan ke Server 2. Terakhir, switch dapat mengakomodasi tingkat transmisi data yang tinggi. Interkomunikasi antara dua server tanpa mengirimkan data ke stasiun kerja mana pun di jaringan. Karena banyak jaringan area lokal memiliki komunikasi antar server tingkat tinggi, penggunaan switch ini dapat secara efektif mengurangi lalu lintas jaringan secara keseluruhan.

Sakelar dupleks penuh

Salah satu kelemahan utama jaringan area lokal CSMA/CD dengan hub adalah adanya tabrakan. Karena stasiun kerja tidak dapat mengirimkan data jika ia mendengar stasiun kerja lain sedang melakukan transmisi, jaringan CSMA/CD adalah sistem setengah dupleks. Ingatlah bahwa sistem setengah dupleks memungkinkan pengirim dan penerima untuk berbicara, tetapi tidak pada saat yang bersamaan. Bandwidth jaringan CSMA/CD akan berlipat ganda jika merupakan sistem full-duplex di mana pengirim dan penerima dapat berbicara secara bersamaan. Selain itu, tidak akan ada tabrakan pada masing-masing segmen, yang akan menyederhanakan algoritma CSMA/CD. Sakelar dupleks penuh memungkinkan jaringan CSMA/CD untuk mengirim dan menerima data secara bersamaan ke dan dari stasiun kerja. Bagaimana workstation di jaringan CSMA/CD dapat mengirim dan menerima sinyal secara bersamaan? Gunakan dua pasang kabel: Kirim sinyal kirim pada sepasang kabel dan sinyal terima pada sepasang kabel lainnya.

Apa yang diperlukan untuk mendukung koneksi full-duplex pada jaringan area lokal? Pada dasarnya, ada tiga syarat yang harus dipenuhi. Pertama, NIC di stasiun kerja harus mampu mendukung, dan kemudian dikonfigurasi untuk mendukung, koneksi dupleks penuh. Demikian pula, saklar harus dikonfigurasi untuk koneksi dupleks penuh. Terakhir, kabel yang menghubungkan NIC workstation ke switch juga harus mampu mendukung koneksi dupleks penuh. Ethernet 10-Mbps dan Ethernet 100-Mbps memerlukan dua pasang (empat kabel) antara workstation dan switch untuk mendukung koneksi dupleks penuh. Karena kecepatan transmisinya yang jauh lebih tinggi, Ethernet 1000-Mbps memerlukan empat pasang kabel. Karena sambungan antara stasiun kerja dan saklar tidak terlalu panjang (biasanya kurang dari 100 meter), dan kabel yang digunakan biasanya berupa pasangan terpilin (twisted pair), seharusnya tidak terlalu sulit untuk menerapkan sambungan dupleks penuh. Faktanya, jika Anda memasang LAN baru dan juga memasang kabelnya, proses untuk memastikan bahwa setiap kabel memiliki satu set standar delapan kabel (menggunakan konektor RJ-45) sangatlah sederhana. Bahkan jika Anda tidak menggunakan kedelapan kabel sekarang, Anda akan memiliki kabel tersebut untuk peningkatan di masa mendatang.

Jelas bahwa switch merupakan alat yang ampuh untuk mensegmentasi jaringan area lokal dan dengan demikian mengurangi jumlah lalu lintas secara keseluruhan. Sebagai hasil dari pengurangan lalu lintas, LAN yang menggunakan switch adalah jaringan yang lebih efisien

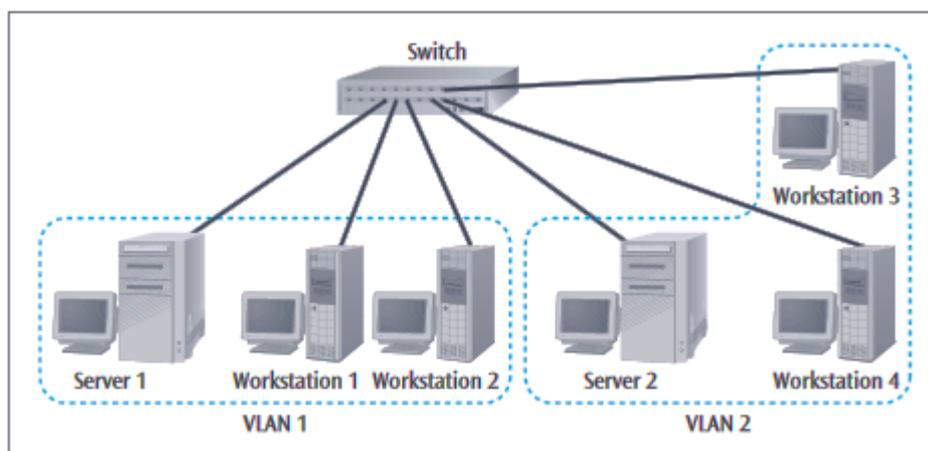
dengan kinerja jaringan yang lebih baik. Selain itu, karena throughput jaringan secara keseluruhan meningkat, waktu responsnya ketika pengguna meminta layanan menjadi lebih cepat.

Sakelar dupleks penuh telah menjadi sangat umum di banyak jaringan sehingga tabrakan dapat dihilangkan dan perangkat lunak jaringan tidak perlu mendengarkan sebelum melakukan transmisi—dengan demikian, CSMA/CD pada dasarnya telah menjadi MA (akses ganda).

LAN Virtual

Salah satu aplikasi yang lebih menarik untuk jaringan segmen khusus dan switch adalah membuat LAN virtual. LAN virtual, atau VLAN, adalah subkelompok logis dalam jaringan area lokal yang dibuat melalui sakelar dan perangkat lunak, bukan dengan memindahkan kabel secara manual dari satu perangkat jaringan ke perangkat lainnya. Misalnya, jika sebuah perusahaan ingin membuat kelompok kerja karyawan untuk mengerjakan proyek baru, personel pendukung jaringan dapat membuat VLAN untuk kelompok kerja tersebut. Meskipun karyawan dan stasiun kerja komputer mereka mungkin tersebar di seluruh gedung, switch LAN dan perangkat lunak VLAN dapat digunakan untuk membuat “jaringan di dalam jaringan.” Karena stasiun kerja ini terhubung ke jaringan segmen khusus, mereka akan mengalami lebih sedikit (jika ada) tabrakan ketika mereka melakukan transmisi ke stasiun kerja lain dalam grup di jaringan virtual baru, dan waktu responsnya akan lebih cepat. Selain itu, karena hanya workstation yang menjadi anggota VLAN yang akan menerima frame, bandwidth dioptimalkan, dan keamanan jaringan ditingkatkan.

Misalnya, perhatikan Gambar 7-14, di mana dua VLAN telah dikonfigurasi. VLAN 1 memiliki Server 1, Workstation 1, dan Workstation 2. VLAN 2 memiliki Server 2, Workstation 3, dan Workstation 4. Perangkat yang ada di VLAN 1 tidak dapat mengakses perangkat yang ada di VLAN 2, begitu pula sebaliknya karena berada di VLAN yang berbeda. Meski terdengar membatasi, hal ini meningkatkan kecepatan dan keamanan penerusan.



Gambar 7-14 Sebuah saklar dengan dua VLAN dikonfigurasi

Standar IEEE 802.1Q dirancang untuk memungkinkan beberapa perangkat saling berkomunikasi dan bekerja sama untuk membuat LAN virtual. Dengan menggunakan standar

ini, perangkat atau tautan Ethernet juga dapat dibagikan oleh beberapa VLAN. Untuk mencapai hal ini, sebuah tag (bidang empat byte) dimasukkan ke dalam frame Ethernet oleh switch yang terlibat.

Untuk membantu pemeliharaan, semua operasi 802.1Q dapat dilakukan dari jarak jauh. Daripada mengirim teknisi ke lemari kabel untuk memindahkan kabel stasiun kerja dari satu switch ke switch lainnya, switch yang sesuai dengan 802.1Q dapat dikonfigurasi dari jarak jauh oleh administrator jaringan. Dengan demikian, workstation dapat dipindahkan dari satu VLAN ke VLAN lainnya hanya dengan perubahan perangkat lunak sederhana. Kebanyakan switch modern dapat memiliki alamat IP yang ditetapkan padanya, sehingga administrator jaringan dapat melakukan perubahan VLAN melalui Internet.

Agregasi tautan

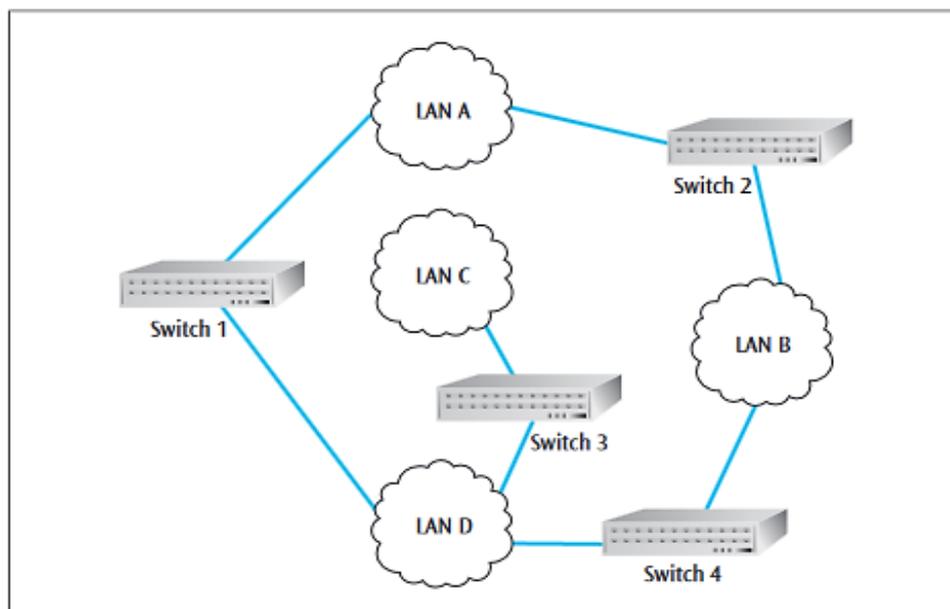
Terkadang satu link tidak menyediakan bandwidth yang cukup antara perangkat dan switch. Atau bagaimana jika Anda ingin memberikan link cadangan antara perangkat dan switch yang sama? Agregasi tautan memungkinkan Anda menggabungkan dua atau lebih jalur data, atau tautan, menjadi satu tautan berkecepatan lebih tinggi. Meskipun sejumlah protokol kepemilikan telah muncul selama bertahun-tahun, satu standar untuk Ethernet diciptakan untuk mendukung agregasi tautan: IEEE 802.3ad-2000. Standar IEEE ini dapat menggabungkan sebanyak delapan link menjadi satu link “gemuk”, sehingga memungkinkan kapasitas transfer data yang jauh lebih tinggi antara dua perangkat. Untuk memanfaatkan tautan tambahan, standar ini berupaya menyeimbangkan aliran secara merata di semua tautan bersama. Kami mengatakan “percobaan” karena jika ada aliran frame atau paket yang termasuk dalam percakapan tertentu, akan lebih efisien untuk menyimpan paket-paket tersebut secara berurutan melalui satu tautan, daripada menyebarkannya melalui banyak tautan. Dengan demikian, agregasi tautan dapat mengenali urutan paket dan tidak akan menyebarkannya ke banyak tautan. Agregasi tautan juga dapat digunakan jika terjadi kegagalan tautan. Jika dua atau lebih link digabungkan dan salah satu link tersebut gagal, switch dapat pulih dari kegagalan link dalam waktu kurang dari satu detik. Terakhir, agregasi tautan juga dapat digunakan untuk mengizinkan beberapa tautan paralel ke server. Hal ini dapat berguna jika server tertentu memiliki permintaan yang tinggi dan mengalami penundaan karena semua permintaan melintasi satu link. Dengan agregasi link, permintaan server dapat tersebar di beberapa link, sehingga menggandakan atau melipatgandakan kapasitas server (dengan asumsi bahwa server memiliki perangkat keras dan perangkat lunak yang diperlukan untuk mendukung beberapa permintaan secara bersamaan).

Algoritma spanning tree

Banyak bisnis dan sekolah memiliki beberapa jaringan area lokal untuk mendukung sejumlah besar pengguna yang tersebar di wilayah geografis yang luas. Selain itu, sering kali diinginkan untuk menghubungkan jaringan-jaringan ini sedemikian rupa sehingga interkomunikasi di seluruh kampus dapat terjadi. Seperti yang telah kita lihat sejauh ini, cara terbaik untuk melakukan interkoneksi menghubungkan jaringan area lokal ini dengan switch. Sebagai contoh, mari kita perhatikan interkoneksi jaringan seperti yang ditunjukkan pada Gambar 7-15. Setelah memeriksa tata letak jaringan lebih dekat, kita melihat fenomena

menarik: Ada koneksi melingkar dari Switch 1 ke LAN A ke Switch 2 ke LAN B ke Switch 4 ke LAN D kembali ke Switch 1. Mengapa hal ini dilakukan? Mungkin para insinyur jaringan sedang mencoba membuat sistem yang memiliki setidaknya dua cara yang mungkin untuk mengakses sebagian besar jaringan area lokal, jika terjadi kegagalan komponen. Atau mungkin begitulah cara jaringan-jaringan itu saling terhubung. Apakah ini sebuah masalah? Sebenarnya, ada beberapa hal yang bisa salah. Mari kita lihat salah satu yang lebih jelas. (Pembaca yang cerdas mungkin dapat menemukan masalah lain.)

Bayangkan sebuah perangkat di LAN A mengirimkan frame ke Switch 1. Alamat tujuan ada di LAN D, namun switch belum melihat alamat tujuan, sehingga alamat tersebut tidak ada di tabel switch/port mana pun. Karena Switch 1 tidak mengenali alamat tujuan, maka frame diteruskan ke LAN D. Frame kemudian tiba di Switch 4. Sekali lagi, switch tidak mengenali alamat tujuan, sehingga frame diteruskan ke LAN B, di mana ia tiba di Switch 2. Karena tidak mengenali alamat tujuan, switch meneruskan frame ke LAN A. Karena LAN A terhubung ke Switch 1, Switch 1 akan menerima frame; dan tidak mengenali alamat tujuan, Switch 1 akan meneruskan frame tersebut ke LAN D, dan seterusnya.

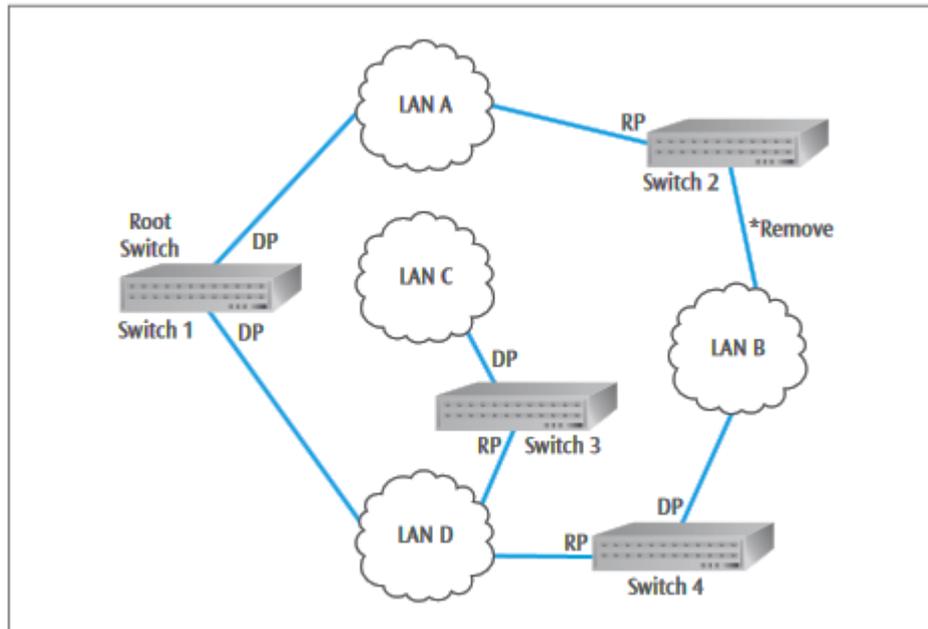


Gambar 7-15 Interkoneksi melingkar jaringan area lokal dan switch

Bagaimana kita bisa menghentikan siklus passing frame ini? Hal ini dapat dipatahkan hanya dengan memutus interkoneksi melingkar LAN dan switch. Namun kami tidak ingin memutus interkoneksi sirkular secara fisik. Mungkin ada alasan untuk strategi interkoneksi seperti itu (seperti yang telah disebutkan). Sebagai gantinya, mari kita program saklar untuk menemukan interkoneksi melingkar dan kemudian memutus perulangan dengan memodifikasi tabel penerusan. Perangkat lunak yang melakukan hal ini disebut algoritma spanning tree, atau Spanning Tree Protocol (STP). Protokol pada dasarnya terdiri dari empat langkah. Pertama, tentukan saklar root (Gambar 7-16). Kedua, kunjungi setiap switch (kecuali switch root). Di setiap switch, identifikasi port/koneksi yang mengarahkan Anda kembali ke switch root dalam

jumlah hop paling sedikit. Tandai setiap port dengan simbol RP (untuk root port). Ketiga, kunjungi setiap jaringan area lokal. Di setiap jaringan, identifikasi port/koneksi yang membawa Anda kembali ke switch root dalam jumlah hop paling sedikit. Tandai setiap port dengan simbol DP (untuk port yang ditunjuk). Terakhir, port yang tersisa tanpa penunjukan RP atau penunjukan DP dapat dihapus.

Yang kami maksud dengan “dihapus” adalah memperbarui tabel penerusan internal sehingga data tidak diteruskan antara Switch 2 dan LAN B menggunakan port/koneksi ini.



Gambar 7-16 Interkoneksi jaringan yang menunjukkan saklar root, port root, port yang ditunjuk, dan koneksi yang dihapus.

Meskipun Protokol Spanning Tree bekerja dengan baik, ada satu kelemahannya: Diperlukan waktu antara 30 dan 50 detik untuk menghitung ulang algoritma spanning tree jika terjadi kegagalan jaringan/perubahan topologi. Untuk mengatasi masalah ini, Rapid Spanning Tree Protocol (RSTP) dikeluarkan pada tahun 2001, yang dapat menghitung ulang algoritma spanning tree dalam waktu sekitar 6 detik.

Kualitas pelayanan

Salah satu elemen terakhir yang didukung oleh switch jaringan area lokal, dan relatif baru, adalah kualitas layanan. Ketika jaringan area lokal dibuat, semua frame pada dasarnya dibuat sama. Protokol ini sering disebut sebagai protokol first-come, first-served. Tidak masalah apakah jaringan mengirimkan email berprioritas rendah atau merupakan bagian dari streaming video berprioritas tinggi. Setiap perangkat (dan frame) bersaing dengan perangkat lain (dan frame) untuk transmisi melalui media. Bentuk awal dari jaringan area lokal—token ring—memiliki sistem prioritas, namun jaringan ini mengalami sejumlah kekurangan lain dan akhirnya dikalahkan oleh Ethernet. Menariknya, Ethernet nirkabel memberikan tingkat prioritas, yang akan kita bahas di bab berikutnya. Namun Ethernet berkabel tidak pernah memiliki kemampuan untuk menangani jenis lalu lintas tertentu dengan tingkat prioritas yang

lebih tinggi atau lebih rendah sampai IEEE menciptakan standar 802.1p pada pertengahan tahun 1990an. Sederhananya, bidang Priority Code Point (PCP) tiga-bit ditambahkan ke header frame Ethernet oleh perangkat yang berpartisipasi. Bidang PCP tiga-bit ini dapat menentukan delapan nilai berbeda, atau tingkat prioritas, sebagai berikut:

Nilai PCP	Jenis Lalu Lintas
0	Best effort
1	Latar Belakang (Prioritas rendah)
2	Excelent Effort
3	Aplikasi Kritis
4	Video
5	Suara
6	Kontrol Internetwork
7	Kontrol Jaringan (Prioritas tinggi)

Bagaimana sistem menggunakan nilai-nilai PCP (prioritas) ini tidak ditentukan oleh standar dan diserahkan kepada personel jaringan.

7.7 ETHERNET KABEL

Dalam 20 tahun terakhir, ada sekitar empat sistem jaringan area lokal yang populer: Ethernet, IBM Token Ring, Fiber Distributed Data Interface, dan Ethernet nirkabel. IBM Token Ring dan Fiber Distributed Data Interface sudah hampir hilang dari dunia LAN, jadi kami tidak akan membahasnya saat ini. Jika Anda tertarik untuk mempelajari lebih lanjut tentang salah satu sistem ini, lihat situs Web penulis. Kita akan memeriksa dua jaringan area lokal yang tersisa: Ethernet berkabel (di bab ini) dan Ethernet nirkabel (di bab berikutnya).

Ethernet adalah sistem jaringan area lokal pertama yang tersedia secara komersial dan, tidak diragukan lagi, tetap menjadi sistem LAN paling populer saat ini. Versi kabel Ethernet terutama didasarkan pada topologi bus kabel bintang dan pada dasarnya menggunakan protokol akses media CSMA/CD. Karena Ethernet sangat populer dan telah ada sejak lama, Ethernet telah berkembang menjadi beberapa bentuk yang berbeda. Untuk menghindari kekacauan massal, IEEE menciptakan seperangkat standar individual khusus untuk jaringan area lokal Ethernet atau CSMA/CD, semuanya di bawah kategori 802.3. Mari kita periksa berbagai protokol 802.3 dengan lebih detail. Untuk referensi Anda, standar 802.3 yang akan dibahas dirangkum dalam Tabel 7-1.

Standar 802.3 asli mencakup 10Base5, 10Base2, 1Base5, dan 10BaseT. Standar 10Base5 adalah salah satu standar Ethernet pertama yang disetujui. Istilah “Base” adalah singkatan dari sinyal baseband yang menggunakan pengkodean Manchester. Ingatlah bahwa sinyal baseband adalah sinyal digital. Karena tidak ada multiplexing sinyal digital pada setiap baseband LAN, hanya ada satu saluran informasi pada jaringan. Angka “10” dari 10Base5 mewakili kecepatan transmisi 10 Mbps, dan angka “5” mewakili panjang segmen kabel maksimum 500 meter. (Perhatikan bahwa standar ini, seperti standar yang terkait dengan

media yang dilakukan, didasarkan pada sistem metrik; jika berlaku, standar yang setara dalam bahasa Inggris akan disediakan.) 10Base2 (dijuluki Cheapernet) dirancang untuk memungkinkan jaringan yang lebih murah dengan menggunakan lebih sedikit- komponen mahal. Jaringan 10Base2 dapat mengirimkan sinyal digital 10-Mbps melalui kabel koaksial, tetapi hanya untuk jarak maksimum 200 meter (nilai "2" di 10Base2). 1Base5 adalah sistem yang dirancang untuk kabel twisted pair, tetapi dengan kecepatan transfer data hanya 1-Mbps untuk jarak 500 meter. Karena kemajuan teknologi, 10Base5, 10Base2, dan 1Base5 punah. Standar 10-Mbps yang sangat populer adalah 10BaseT. Sistem 10BaseT mentransmisikan sinyal baseband (digital) 10-Mbps melalui twisted pair dengan panjang maksimum 100 meter per segmen. Banyak bisnis, sekolah, dan rumah menggunakan 10BaseT (dan kemudian 100BaseT) sebagai jaringan area lokal mereka.

Salah satu standar paling umum untuk Ethernet broadband (analog) adalah spesifikasi 10Broad36. Menggunakan kabel koaksial untuk mengirimkan sinyal analog, 10Broad36 mengirimkan data dengan kecepatan 10 Mbps untuk jarak segmen maksimum 3600 meter. Perhatikan jarak yang lebih jauh karena penggunaan kabel koaksial dan sinyal analog. Dan karena sinyal broadband dapat mendukung banyak saluran, 10Broad36 mengirimkan banyak saluran data secara bersamaan, masing-masing mendukung aliran transmisi 10-Mbps. Terlalu banyak pakar jaringan yang menganggap kabel koaksial dan sinyal analog terlalu sulit untuk digunakan. Menurut beberapa laporan industri, tidak ada yang memasang sistem 10Broad36 baru. Tampaknya, beberapa saluran data secara bersamaan tidak cukup untuk menyelamatkan 10Broad36.

Ketika Ethernet 10-Mbps pertama kali tersedia, ini merupakan protokol cepat untuk banyak jenis aplikasi. Namun, seperti kebanyakan teknologi berbasis komputer, kecepatannya tidak bertahan lama. Menanggapi permintaan akan sistem Ethernet yang lebih cepat, IEEE menciptakan protokol Ethernet 802.3u 100-Mbps. Standar Ethernet 100-Mbps yang dijelaskan dalam paragraf ini disebut Fast Ethernet untuk membedakannya dari standar 10-Mbps. 100BaseTX dirancang untuk mendukung sinyal baseband 100-Mbps menggunakan dua pasang pasangan terpilin tanpa pelindung Kategori 5. Seperti rekannya 10BaseT, 100BaseTX dirancang untuk segmen 100 meter. Hal ini mirip dengan sistem 10BaseT yang menggunakan kabel twisted pair dan hub dengan beberapa koneksi workstation. 100BaseT4 dibuat untuk mendukung kabel kategori lama. Dengan demikian dapat beroperasi pada kabel pasangan terpilin Kategori 3 atau 4, serta pasangan terpilin tak berpelindung Kategori 5/5e/6. Ia juga mentransmisikan sinyal baseband 100-Mbps untuk jarak maksimum 100 meter, namun sekarang sudah punah. Terakhir, 100BaseFX adalah standar yang dibuat untuk sistem serat optik. Ini dapat mendukung sinyal baseband 100-Mbps menggunakan dua helai serat tetapi untuk jarak yang lebih jauh: 1000 meter.

Rangkaian standar Ethernet berikutnya yang akan dikembangkan didasarkan pada kecepatan transmisi 1000- Mbps, atau 1 gigabit (1 miliar bit) per detik. Standar ini mendefinisikan Gigabit Ethernet (IEEE 802.3z), yang telah menjadi salah satu teknologi terkini untuk jaringan area lokal berkecepatan tinggi. Standar gigabit pertama—1000BaseSX—mendukung interkoneksi cluster yang relatif dekat stasiun kerja dan perangkat lain yang

menggunakan kabel serat optik multimode. 1000BaseLX dirancang untuk pemasangan kabel jarak jauh di dalam gedung dan menggunakan kabel serat optik mode tunggal atau serat multimode. 1000BaseCX dirancang untuk kabel jumper jarak pendek (0,1 hingga 25 meter) menggunakan kawat tembaga seimbang. Standar yang lebih baru, disebut 1000BaseT, mampu menggunakan spesifikasi kabel Kategori 5e atau Kategori 6. Lebih tepatnya, 1000BaseT menggabungkan sinyal bertingkat canggih untuk mengirimkan data melalui empat pasang kabel CAT 5e/CAT 6.

Standar Ethernet yang lebih baru adalah Ethernet 10-Gbps. Standar Ethernet 10-Gbps (mentransfer dengan kecepatan 10 miliar bit per detik) disetujui oleh IEEE pada bulan Juli 2002. Standar ini juga dikenal sebagai IEEE 802.3ae, 10G Ethernet, atau 10-Gigabit Ethernet. Standar 10-Gbps yang asli telah berubah menjadi beberapa standar sekunder, seperti 10GBase-SR untuk pemasangan kabel jarak pendek dan 10GBase-LR untuk pemasangan kabel jarak jauh. Sebagian besar standar sekunder ini melibatkan kabel serat optik sebagai media untuk jarak pendek dan menengah. Namun, beberapa standar baru berbasis tembaga mulai bermunculan. Salah satu standar tersebut, 10GBase-CX4, melibatkan pemasangan kabel yang mirip dengan pemasangan kabel yang digunakan di InfiniBand sepanjang 15 meter. Standar tembaga kedua, 10GBase-T, akan menggunakan variasi baru pada CAT 6 yang disebut CAT 6a dan memungkinkan jarak transmisi hingga 100 meter. Selain itu, ada beberapa proposal lagi, Ethernet 40-Gbps dan 100-Gbps, yang saat ini masih dalam tahap rancangan.

Tabel 7-1 merangkum berbagai standar Ethernet yang baru saja diperkenalkan. Tabel tersebut mencakup kecepatan transmisi maksimum, jenis sinyal (baik baseband, yang sesuai dengan sinyal digital, atau broadband, yang sesuai dengan analog), jenis kabel, dan panjang segmen maksimum tanpa repeater.

Salah satu peningkatan tambahan pada Ethernet adalah Power over Ethernet (PoE) (standar IEEE 802.3af). Misalkan Anda ingin menempatkan NIC pada suatu perangkat, tetapi Anda tidak ingin atau tidak dapat menghubungkan perangkat tersebut ke sumber listrik. Misalnya, Anda ingin memasang kamera pengintai yang mentransfer sinyalnya terlebih dahulu melalui Ethernet dan kemudian melalui Internet. Biasanya, Anda akan memasang kamera dan kemudian memasang sambungan Ethernet dan sambungan listrik. Namun dengan PoE, Anda dapat mengirimkan daya listrik melalui koneksi Ethernet, yang dapat digunakan untuk memberi daya pada kamera. Meskipun hal ini terdengar menjanjikan, salah satu kelemahannya adalah kemampuan untuk menyediakan daya yang cukup bagi hub atau switch Ethernet sehingga daya tersebut kemudian dapat didistribusikan melalui jalur Ethernet ke berbagai perangkat.

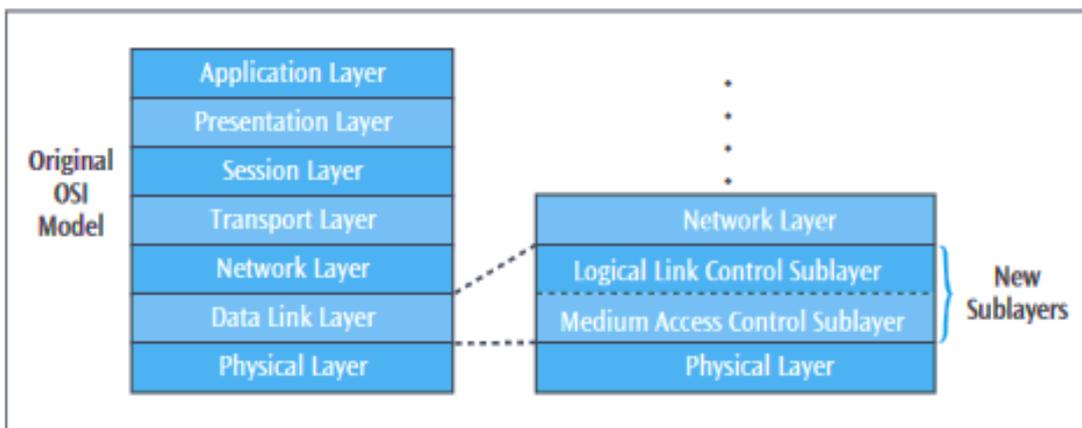
Tabel 7.1 Ringkasan Standar Ethernet

Ethernet Standard	Kecepatan Transfer Maksimum	Tipe Sinyal	Tipe Kabel	Panjang Segmen maksimum
10BaseT	10 Mbps	Baseband	Twisted Pair	100 m
100BaseTX	100 Mbps	Baseband	2-pair Kategori 5 atau UTP	100 m
1000BaseFX	100 Mbps	Baseband	Fiber Optic	1000 m

1000BaseSX	1000 Mbps	Baseband	Fiber Optic	300 m
1000BaseLX	1000 Mbps	Baseband	Fiber Optic	100 m
1000BaseCX	1000 Mbps	Baseband	Tembaga Spesial	25 m
1000BaseT	1000 Mbps	Baseband	Twisted pair – 4 Pasang	100 m
10GBase-fiber	10 Gbps	Baseband	Fiber Optic	Macam-macam panjang
10GBase-T	10 Gbps	Baseband	CAT 6	55-100 m
10GBase-CX4	10 Gbps	Baseband	Axial Kembar	~ 30 Meter

7.8 FORMAT BINGKAI ETHERNET KABEL

Ketika ISO menciptakan model OSI pada tahun 1970an, jaringan area lokal baru saja mulai muncul. Untuk lebih mendukung sifat unik jaringan area lokal dan untuk menciptakan seperangkat standar industri, IEEE menghasilkan serangkaian protokol dengan nama 802 (beberapa di antaranya telah Anda temui dalam bacaan Anda). Salah satu hal pertama yang dilakukan protokol IEEE 802 adalah membagi lapisan data link menjadi dua sublapisan: sublapisan kontrol akses menengah dan sublapisan kontrol tautan logis (Gambar 7-17). Sublapisan kontrol akses menengah (MAC) bekerja lebih dekat dengan lapisan fisik dan berisi header, alamat komputer (fisik), kode pendeteksi kesalahan, dan informasi kontrol. Karena kedekatannya dengan lapisan fisik, tidak ada pembagian yang jelas antara sublapisan MAC dan lapisan fisik. Sublapisan kontrol tautan logis (LLC) terutama bertanggung jawab untuk pengalamatan logis dan menyediakan informasi kontrol kesalahan dan kontrol aliran.

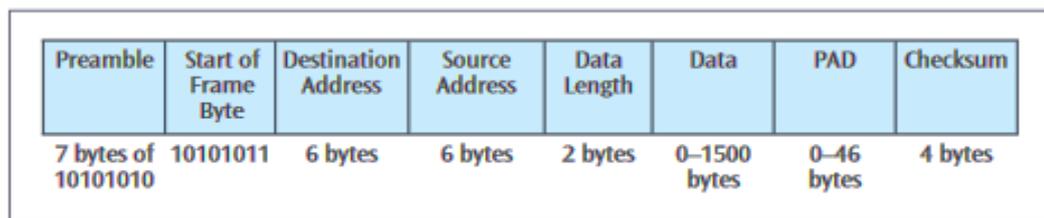


Gambar 7-17 Modifikasi model OSI untuk membagi lapisan data link menjadi dua sublapisan

Sublapisan kontrol akses media mendefinisikan tata letak atau format bingkai data, yang disebut bingkai. Ada sejumlah format frame yang berbeda tergantung pada jenis jaringan area lokal. Misalnya, LAN CSMA/CD memiliki satu format frame, sedangkan LAN token ring yang sekarang sudah tidak berfungsi memiliki format lain. Dalam format bingkai ini terdapat bidang untuk deteksi kesalahan, pengalamatan stasiun kerja, dan berbagai jenis informasi kontrol. Dengan demikian, sublapisan MAC adalah lapisan yang sangat penting ketika menggambarkan jaringan area lokal.

Standar IEEE 802.3 untuk CSMA/CD, yang secara keseluruhan maksud dan tujuannya sama dengan Ethernet, menggunakan format frame seperti ditunjukkan pada Gambar 7-18.

(Secara teknis, Ethernet adalah versi merek dagang dari standar IEEE 802.3 CSMA/CD. Meskipun ada beberapa perbedaan kecil di antara keduanya, untuk tujuan kami, kami akan menganggapnya setara.) Pembukaan dan permulaan frame bidang byte digabungkan untuk membentuk tanda 8-byte yang dikunci oleh penerima untuk sinkronisasi yang tepat. Alamat tujuan dan alamat sumber adalah alamat 6-byte dari komputer penerima dan komputer pengirim. Lebih tepatnya, setiap kartu antarmuka jaringan di dunia memiliki alamat unik 6-byte (48-bit). Ketika CSMA/CD mengirimkan data ke komputer tertentu, ia menciptakan sebuah frame dengan alamat NIC yang sesuai dengan komputer yang dituju. Panjang data hanyalah panjang bidang data dalam byte, yang merupakan entri berikut. Ukuran maksimum bidang data adalah 1500 byte, atau karakter. Bidang PAD menambahkan karakter ke bingkai (melapisi bingkai). Bingkai ukuran minimum yang dapat ditransmisikan oleh stasiun mana pun adalah 64 byte. Frame yang lebih pendek dari 64 byte dianggap kerdil, atau fragmen frame, yang dihasilkan dari tabrakan (di LAN non-switched sebelumnya), dan ini secara otomatis dibuang. Jadi, jika stasiun kerja mencoba mengirimkan frame yang bidang datanya sangat pendek, karakter PAD ditambahkan untuk memastikan bahwa panjang frame keseluruhan setidaknya sama dengan 64 byte. Terakhir, bidang checksum adalah checksum redundansi siklik 4-byte.



Gambar 7-18 Format bingkai untuk IEEE 802.3 CSMA/CD

Diskusi kita tentang teknologi jaringan area lokal dimulai dengan pemeriksaan jenis topologi jaringan utama: bus dan bus kabel bintang. (Kita akan membahas tipe ketiga di bab berikutnya: nirkabel.) Kemudian bentuk utama dari protokol kontrol akses menengah—CSMA/CD—diperkenalkan. Terakhir, kami mengalihkan perhatian kami ke produk sebenarnya atau sistem jaringan area lokal yang ditemukan di lingkungan komputer pada umumnya. Mari kita akhiri bab ini dengan beberapa contoh instalasi jaringan area lokal yang sebenarnya.

Contoh Instalasi LAN

Hannah adalah spesialis komputer untuk usaha kecil di sisi barat Chicago. Perusahaannya saat ini memiliki sekitar 35 hingga 40 pekerja, masing-masing memiliki tempat kerja sendiri. Para karyawan menggunakan komputer terutama untuk pengolah kata, spreadsheet, dan pekerjaan database sesekali. Pemilik perusahaan ingin memperbarui layanan komputer dengan menawarkan aplikasi berikut kepada karyawan:

- Email internal
- Akses bersama ke printer laser hitam-putih dan berwarna berkualitas tinggi
- Akses ke database terpusat

Setelah mendengar permintaan dari pemilik, Hannah menyimpulkan bahwa cara terbaik untuk menawarkan layanan ini adalah dengan memasang jaringan area lokal. Karena semua workstation hanya berumur satu sampai dua tahun, maka tidak perlu diganti dan semuanya sudah berisi NIC untuk LAN. Namun jaringan juga memerlukan kabel, server, dan perangkat lunak untuk menghubungkan workstation ke jaringan area lokal. Jaringan area lokal mana yang harus dipasang Hannah? Setelah membaca literatur dan berbicara dengan beberapa rekan spesialis komputer, Hannah membuat daftar kemungkinan sistem jaringan area lokal berikut ini:

1. CSMA/CD 100Mbps (Ethernet)
2. CSMA/CD 1000Mbps (Ethernet)
3. CSMA/CA Nirkabel (Ethernet)

Ethernet 100-Mbps sepertinya merupakan kandidat yang bagus. Ini adalah sistem jaringan area lokal paling populer dan, oleh karena itu, memiliki harga terendah yang tersedia. Selain itu, mendapatkan dukungan teknis seharusnya tidak menjadi masalah, begitu pula menemukan perangkat keras dan perangkat lunak yang cocok. Jaringan Ethernet dapat dengan mudah mendukung 40 pengguna, namun tabrakan mungkin menjadi masalah jika hub digunakan. Jika pengguna menaruh permintaan tinggi pada jaringan, mereka mungkin melihat beberapa masalah kinerja dan mengeluh. Ini adalah saat yang tepat untuk mempertimbangkan switch Ethernet untuk menghilangkan tabrakan dan meningkatkan throughput. Meskipun kandidat pertama ini sepertinya merupakan pilihan yang baik, Hannah tidak ingin menghilangkan solusi lain yang berpotensi baik, jadi dia terus mengevaluasi daftarnya.

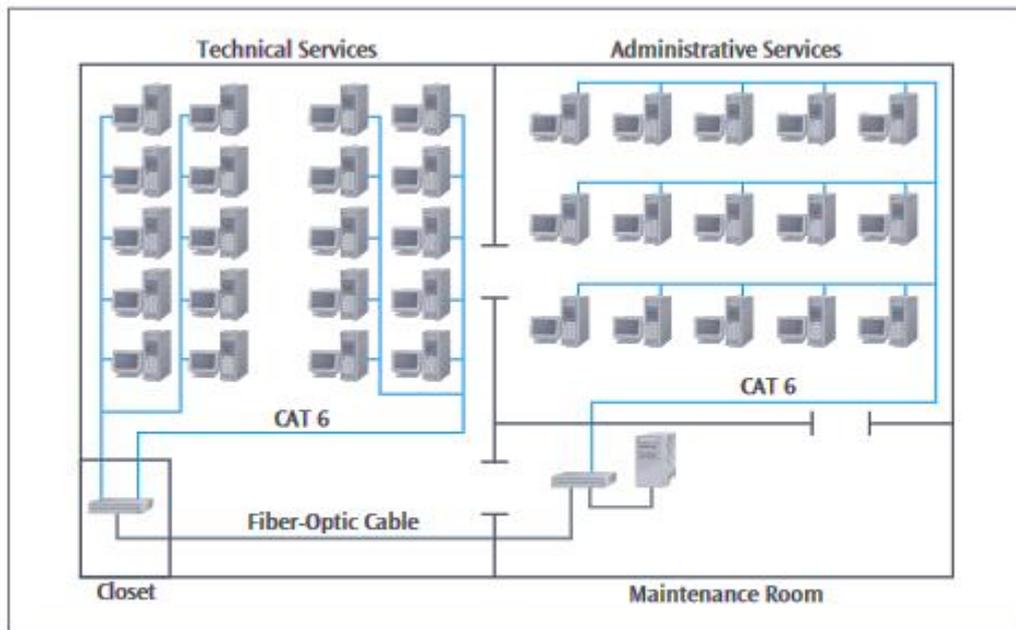
Mungkinkah Ethernet 1000-Mbps menjadi solusi yang lebih baik? Biaya Ethernet 1000-Mbps dibandingkan dengan Ethernet 100-Mbps akan jauh lebih tinggi, terutama ketika berhadapan dengan switch 1000-Mbps. Ditambah lagi, ada masalah bahwa stasiun kerja standar tidak mengalami peningkatan kinerja yang signifikan ketika terhubung ke Ethernet 1000-Mbps. Mengingat ukuran perusahaan Hannah dan anggarannya yang terbatas serta kebutuhan jaringan yang relatif tidak rumit, Ethernet 100-Mbps mungkin merupakan solusi yang lebih ekonomis.

Terakhir, ada solusi Ethernet nirkabel. Sayangnya, Hannah belum mengetahui banyak tentang Ethernet nirkabel. Jadi dia harus memikirkan solusi ini untuk saat ini. Hannah memutuskan untuk menggunakan CSMA/CD kabel 100-Mbps menggunakan switch. Dia bisa saja memilih hub dibandingkan switch namun takut akan permintaan penggunanya dan fakta bahwa hub menyebabkan tabrakan akan membenarkan biaya tambahan untuk switch. Harga peralatan 100-Mbps cukup masuk akal, dan sistem ini cukup mudah dipasang dan dipelihara.

Hal berikutnya yang harus diputuskan Hannah adalah bagaimana mengkonfigurasi sistem. Dia mengetahui bahwa NIC di setiap stasiun kerja dihubungkan ke sebuah saklar, dan merupakan hal yang umum untuk memesan saklar yang mendukung 24 stasiun kerja. Karena Layanan Teknis memiliki 20 karyawan dengan stasiun kerja, dan sekitar 15 karyawan lagi dengan stasiun kerja ditugaskan ke Layanan Administratif di sebelahnya, Hannah memutuskan untuk menghubungkan 20 komputer Layanan Teknis ke satu saklar dan 15 komputer Layanan

Administratif ke saklar kedua. mengalihkan. Kedua saklar tersebut kemudian saling berhubungan.

Ruang kantor, yang sekarang memiliki konfigurasi seperti pada Gambar 7-19, menentukan beberapa keputusan Hannah selanjutnya. Pasangan terpilin tanpa pelindung kategori 6 seharusnya berfungsi dengan baik sebagai kabel antara stasiun kerja dan hub. Hal ini karena jarak di sini tidak perlu lebih dari 100 meter (328 kaki), dan tidak ada peralatan yang menghasilkan kebisingan elektromagnetik dalam jumlah besar. Untuk menghubungkan kedua sakelar tersebut, Hannah memutuskan untuk memasang kabel serat optik karena jarak antar sakelar mungkin mendekati batas twisted pair 100 meter.



Gambar 7-19 Diagram pengkabelan ruang kantor Hannah menunjukkan penempatan switch dan server

Ketika router tiba, Hannah menginstal dan memrogramnya. Dia terkejut melihat betapa terlibatnya router. Dia dengan cepat mengetahui bahwa sebagian besar router beroperasi dalam mode tanpa hak istimewa dan mode dengan hak istimewa. Dalam mode tanpa hak istimewa, pengguna hanya dapat diperlihatkan beberapa pengaturan router. Dalam mode istimewa, pengguna dapat diperlihatkan semua pengaturan router dan mengkonfigurasi router. (Karena Hannah adalah satu-satunya administrator jaringan, dia memilih mode istimewa.) Konfigurasi router mencakup penamaan router, penunjukan server DNS, pengaturan kata sandi untuk akses ke mode hak istimewa, penetapan alamat IP untuk setiap port, dan memberitahukan router untuk melakukan routing statis atau routing dinamis. Setelah router beroperasi dengan benar dan Hannah membuat perubahan yang diperlukan pada stasiun kerja masing-masing karyawan, karyawan tersebut diberitahu bahwa mereka sekarang memiliki akses ke Internet dari stasiun kerja kantor mereka.

Setelah semua sistem aktif dan berjalan, dan karyawan memiliki akses ke Internet, jaringan area lokal dan penggunaan Internet perusahaan mulai berkembang. Ketika karyawan

mulai mempelajari kemungkinan berbagi file lokal, database, dan printer, serta mengakses sejumlah besar materi yang tersedia di Internet, semakin banyak permintaan yang ditempatkan pada jaringan area lokal dan server. Waktu respons jaringan menjadi semakin lambat, dan karyawan mulai mengeluh. Sekarang saatnya untuk memeriksa jaringan dan melakukan upgrade.

Setelah beberapa jam mengamati dan berbincang dengan karyawan, Hannah menyimpulkan bahwa kira-kira separuh karyawan cukup banyak menggunakan database bisnis, dan separuh lainnya banyak menggunakan Internet. Hampir semua orang melakukan pengolahan kata dan beberapa bekerja dengan spreadsheet, namun pekerjaan ini tidak memberikan kontribusi signifikan terhadap beban jaringan yang berat. Namun, penggunaan email sangat berat dan memerlukan lebih banyak ruang penyimpanan di server.

Untuk mengakomodasi lalu lintas email yang padat, Hannah memutuskan terlebih dahulu bahwa dia memerlukan server baru untuk menangani email saja. Jika dia dapat menjaga lalu lintas database di server database dan lalu lintas email di server email, arus lalu lintas akan meningkat. Dengan demikian, server baru ditambahkan di Ruang Pemeliharaan di sebelah server asli.

Peningkatan yang dilakukan Hannah pada jaringan bekerja dengan sangat baik. Kemacetan jaringan berkurang. Baik pengguna email maupun pengguna database merasakan pengurangan waktu tunggu yang wajar. Namun karena penggunaan komputer dan penggunaan jaringan yang terkait hampir selalu meningkat seiring waktu, solusi Hannah kemungkinan besar hanya bersifat sementara hingga masalah berikutnya muncul. Meskipun demikian, rekan kerja Hannah puas dengan pertunjukan ini.

RINGKASAN

- Jaringan area lokal adalah jaringan komunikasi yang menghubungkan berbagai perangkat komunikasi data dalam area kecil dan mentransfer data dengan kecepatan transfer tinggi dengan tingkat kesalahan yang sangat rendah. Fungsi utama LAN adalah untuk memungkinkan berbagi data, perangkat lunak, dan periferal, dan untuk menyediakan layanan umum seperti penyajian file, penyajian cetak, dukungan untuk surat elektronik, dan pengendalian proses dan pemantauan di lingkungan kantor, akademik, dan manufaktur.
- Jaringan area lokal memiliki banyak keunggulan, termasuk pembagian sumber daya, evolusi komponen dan jaringan yang terpisah, kecepatan transfer data yang tinggi, dan tingkat kesalahan yang rendah. Jaringan area lokal juga memiliki banyak kelemahan, termasuk biaya yang relatif tinggi, tingkat pemeliharaan yang tinggi, dan kebutuhan peningkatan yang terus-menerus.
- Jaringan area lokal dapat dikonfigurasi sebagai bus kabel bintang atau jaringan nirkabel.
- Bus kabel bintang telah menggantikan LAN bus baseband dan bus broadband.
- Agar stasiun kerja dapat menempatkan data ke jaringan area lokal, jaringan tersebut harus memiliki protokol kontrol akses medium. Dua bentuk dasar dari protokol kontrol

akses menengah adalah berbasis pertentangan, seperti CSMA/CD, yang ditemukan pada jaringan area lokal bus kabel bintang, dan CSMA/CA, yang ditemukan pada jaringan area lokal nirkabel.

- CSMA/CD bekerja berdasarkan sistem siapa cepat dia dapat, mendukung koneksi half-duplex dan full-duplex, dan jelas merupakan protokol akses yang paling populer, namun mengalami tabrakan frame data selama periode penggunaan tinggi ketika hub dipekerjakan.
- Untuk menstandarisasi protokol kontrol akses medium, IEEE menciptakan standar jaringan seri 802.
- Jenis sistem jaringan area lokal yang paling populer adalah Ethernet (CSMA/CD) dan Ethernet nirkabel. LAN Ethernet memiliki variasi produk terbanyak dan terus mendominasi pasar jaringan area lokal.
- Hub adalah perangkat yang menghubungkan beberapa stasiun kerja dalam jaringan area lokal dan menyiarkan datanya ke semua perangkat yang terhubung.
- Switch dapat memberikan penurunan lalu lintas interkoneksi yang signifikan dan meningkatkan throughput jaringan yang saling terhubung, namun tetap menggunakan kabel dan adaptor konvensional. Switch menggantikan hub dan mengisolasi arus lalu lintas antar segmen jaringan dengan memeriksa alamat frame yang ditransmisikan dan mengarahkan frame ke port yang sesuai.
- Sebuah switch bersifat transparan karena ia membangun tabel penerusannya sendiri dengan mengamati arus lalu lintas di jaringan, sebuah proses yang disebut sebagai pembelajaran mundur.
- Switch yang menggunakan arsitektur cut-through adalah kebalikan dari perangkat store-and-forward, dimana frame data meninggalkan switch segera setelah frame data mulai memasuki switch.
- Switch dapat membuat segmen bersama di mana semua stasiun kerja mendengar semua lalu lintas, atau segmen khusus di mana stasiun kerja lain tidak mendengar lalu lintas lokal. Switch juga dapat dibuat untuk beroperasi dalam mode full-duplex dan dapat digunakan untuk membuat LAN virtual. Switch juga dapat menggabungkan beberapa jalur secara bersamaan, dan menyediakan Spanning Tree Protocol serta tingkat kualitas layanan tertentu.
- Router menghubungkan jaringan area lokal dengan jaringan area luas. Fungsi router yang paling umum adalah merutekan paket data antara dua jaringan, salah satunya menggunakan alamat di sublapisan kontrol akses media, sedangkan jaringan lainnya menggunakan alamat di lapisan selain sublapisan kontrol akses media. Router memberi semua pengguna di jaringan area lokal akses ke jaringan luar. Router bekerja lebih lambat dibandingkan switch dan memerlukan lebih banyak pemrosesan karena mereka harus menggali lebih dalam ke dalam bingkai data untuk informasi kontrol.

PERTANYAAN

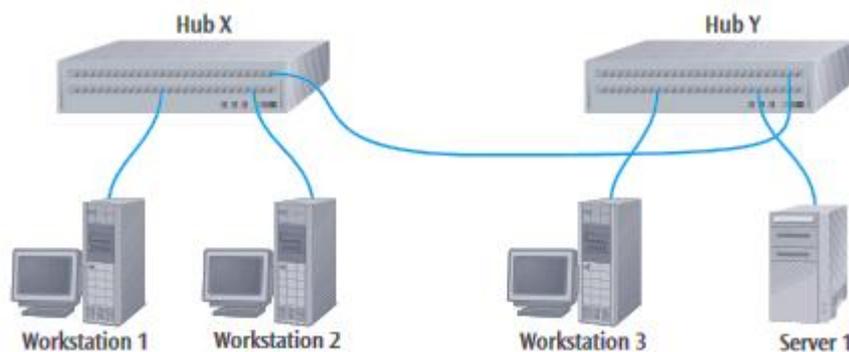
1. Apa definisi jaringan area lokal?
2. Buat daftar aktivitas utama dan area penerapan jaringan area lokal.
3. Sebutkan kelebihan dan kekurangan jaringan area lokal.
4. Apa tata letak dasar jaringan area lokal? Sebutkan dua keunggulan yang dimiliki setiap tata letak dibandingkan tata letak lainnya.
5. Apa yang dimaksud dengan “perangkat pasif”?
6. Apa yang dimaksud dengan “sinyal dua arah”?
7. Apa perbedaan utama antara teknologi baseband dan teknologi broadband?
8. Apa tujuan hub?
9. Apa perbedaan antara desain fisik dan desain logis?
10. Apa yang dimaksud dengan protokol kontrol akses menengah?
11. Apa prinsip dasar pengoperasian CSMA/CD?
12. Apa yang dimaksud dengan protokol “nondeterministik”?
13. Apa kepanjangan dari istilah “100BaseT”?
14. Apa perbedaan antara Fast Ethernet dan Ethernet biasa?
15. Apa saja standar Ethernet 10 Gbps terbaru?
16. Apa keunggulan utama daya dibandingkan Ethernet? Apa kelemahan utamanya?
17. Bagaimana cara kerja saklar transparan?
18. Apa tujuan dari LAN virtual?
19. Bagaimana cara saklar merangkum pesan untuk transmisi? (Untuk penyegaran mengenai enkapsulasi, lihat Bab Satu.)
20. Jika mengacu pada hub atau switch, apa itu port?
21. Apa fungsi dasar saklar?
22. Apa perbedaan saklar dengan hub?
23. Apa yang dimaksud dengan arsitektur cut-through?
24. Apa perbedaan saklar dupleks penuh dengan saklar setengah dupleks?
25. Apa yang dimaksud dengan agregasi tautan?

LATIHAN

1. Properti apa yang membedakan jaringan area lokal dari bentuk jaringan lainnya?
2. Jelaskan contoh sistem bus broadband.
3. Apakah hub merupakan perangkat pasif atau perangkat aktif? Menjelaskan.
4. Standar Ethernet mana (10 Mbps, 100 Mbps, 1000 Mbps, 10 Gbps) memungkinkan untuk media twisted pair? Apa nama standar IEEE yang sesuai?
5. Jika suatu jaringan digambarkan sebagai 1000BaseT, buatlah daftar semua yang Anda ketahui tentang jaringan itu.
6. Dalam format frame IEEE 802.3, bidang PAD digunakan untuk apa? Berapa ukuran paket minimum?
7. Misalkan Workstation A ingin mengirimkan pesan “HELLO” ke Workstation B. Kedua workstation berada pada jaringan area lokal IEEE 802.3. Workstation A memiliki alamat

biner 1, dan Workstation B memiliki alamat biner 10. Tampilkan frame sublapisan MAC yang dihasilkan (dalam biner) yang ditransmisikan. Jangan menghitung CRC; buat saja satu.

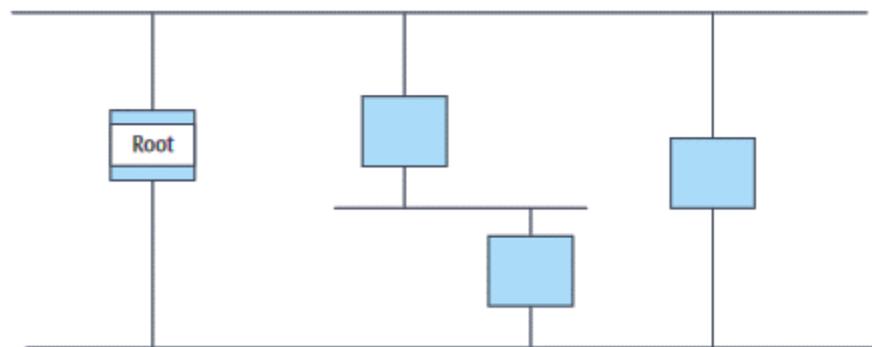
8. Apa perbedaan antara representasi fisik LAN bus kabel bintang dan representasi logisnya?
9. Apa persamaan hub dengan saklar? Bagaimana mereka berbeda?
10. Apakah hub dan switch dapat dipertukarkan? Menjelaskan.
11. a. Jaringan area lokal yang ditunjukkan pada Gambar 7-21 memiliki dua hub (X dan Y) yang menghubungkan workstation dan server. Stasiun kerja dan server mana yang akan menerima salinan paket jika stasiun kerja/server berikut mengirimkan pesan?:
 - Workstation 1 mengirim pesan ke Workstation 3.
 - Workstation 2 mengirim pesan ke Server 1.
 - Server 1 mengirim pesan ke Workstation 3.
- b. Ganti Hub Y dengan saklar. Sekarang stasiun kerja dan server mana yang akan menerima salinan paket jika stasiun kerja/server berikut mengirimkan pesan?:
 - Workstation 1 mengirim pesan ke Workstation 3.
 - Workstation 2 mengirim pesan ke Server 1.
 - Server 1 mengirim pesan ke Workstation 3.



Gambar 7-21 Contoh jaringan

12. Saklar transparan disisipkan di antara dua jaringan area lokal: ABC dan XYZ. Jaringan ABC memiliki Stasiun Kerja 1, 2, dan 3, dan Jaringan XYZ memiliki Stasiun Kerja 4, 5, dan 6. Kedua tabel penerusan dimulai dengan kosong. Tampilkan isi dari dua tabel penerusan di switch saat paket berikut dikirimkan:
 - a. Workstation 2 mengirimkan paket ke Workstation 3.
 - b. Workstation 2 mengirimkan paket ke Workstation 5.
 - c. Workstation 1 mengirimkan paket ke Workstation 2.
 - d. Workstation 2 mengirimkan paket ke Workstation 3.
 - e. Workstation 2 mengirimkan paket ke Workstation 6.
 - f. Workstation 6 mengirimkan paket ke Workstation 3.
 - g. Workstation 5 mengirimkan paket ke Workstation 4.
 - h. Workstation 2 mengirimkan paket ke Workstation 1.

- i. Workstation 1 mengirimkan paket ke Workstation 3.
 - j. Workstation 1 mengirimkan paket ke Workstation 5.
 - k. Workstation 5 mengirimkan paket ke Workstation 4.
 - l. Workstation 4 mengirimkan paket ke Workstation 5.
13. Berikan contoh situasi di mana LAN virtual mungkin merupakan alat yang berguna dalam lingkungan bisnis. Bagaimana dengan lingkungan pendidikan?
 14. Apa yang dimaksud dengan saklar atau perangkat terputus? Apa kelemahan utama dari saklar potong-melalui? Apakah ada cara untuk mengatasi kelemahan saklar potong tanpa kehilangan kelebihanannya? Pertahankan jawaban Anda.
 15. Berikan contoh bisnis umum yang meniru perbedaan antara jaringan segmen bersama dan jaringan segmen khusus.
 16. Peralihan perusahaan Anda antara dua jaringannya baru saja terputus. Anda memiliki router tergeletak di meja Anda yang saat ini tidak digunakan. Akankah router berfungsi menggantikan saklar yang rusak? Menjelaskan.
 17. Jaringan CSMA/CD terhubung ke Internet melalui router. Seorang pengguna di jaringan CSMA/CD mengirimkan email ke pengguna di Internet. Tunjukkan bagaimana pesan email dikapsulasi saat meninggalkan jaringan CSMA/CD, memasuki router, dan kemudian meninggalkan router.
 18. Berdasarkan jaringan berikut (Gambar 7-22), tunjukkan bagaimana Spanning Tree Protocol akan menghilangkan jalur siklik.



Gambar 7-22 Jaringan hipotetis dengan jalur siklik

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Sebuah department store ritel berukuran kira-kira persegi, 35 meter (100 kaki) di setiap sisinya. Setiap dinding memiliki dua pintu masuk dengan jarak yang sama. Terletak di setiap pintu masuk adalah mesin kasir tempat penjualan. Sarankan solusi jaringan area lokal yang menghubungkan kedelapan mesin kasir. Gambarkan diagram yang menunjukkan ruangan, lokasi semua mesin kasir, kabel, saklar, dan server. Jenis kabel apa yang Anda sarankan?
2. Anda bekerja di sebuah perusahaan periklanan kecil dengan sekitar 200 karyawan. Di seluruh perusahaan tersebar sejumlah stasiun kerja komputer terpisah yang melakukan pemrosesan kata, desain grafis, operasi spreadsheet, dan analisis pasar. Atasan Anda

telah meminta Anda untuk mempertimbangkan memasang beberapa bentuk jaringan area lokal untuk mendukung pengoperasian komputer. Buatlah daftar kemungkinan aplikasi komputer yang dapat beroperasi melalui jaringan area lokal dan akan mendukung fungsi karyawan dan bisnis sehari-hari. Jenis jaringan area lokal apa yang mungkin Anda sarankan?

Apa topologinya? Metode kontrol akses menengah? Peralatan pendukung seperti apa (saklar, server) yang mungkin Anda perlukan? Di mana peralatan pendukung tersebut akan ditempatkan?

3. Sebuah perusahaan besar memiliki banyak departemen berbeda yang bertempat di kompleks perkantoran besar di kota.

Setiap departemen memiliki database informasi lokalnya sendiri. Perusahaan ingin membiarkan semua karyawan di seluruh perusahaan mengakses database ini. Jenis jaringan apa yang Anda rekomendasikan untuk situasi seperti ini?

4. Anda bekerja di sebuah perusahaan yang sangat kecil dengan hanya selusin karyawan. Lima workstation komputer perlu terhubung ke Internet. Buat daftar opsi yang tersedia. Apa kelebihan dan kekurangan masing-masing pilihan? Apa rekomendasi Anda?

5. Setelah putaran terakhir reorganisasi perusahaan, Anda sekarang memiliki enam divisi internal, bukan tujuh. Departemen teknologi mencoba untuk mengatur tata letak jaringan dengan menjaga pengguna di setiap divisi pada segmen jaringannya masing-masing, namun departemen tersebut bosan mengatur ulang kabel-kabel di lemari untuk mengakomodasi perubahan ini. Apa saran Anda agar departemen teknologi menggunakannya untuk mendukung enam divisi internal?

6. Anda bekerja di perusahaan yang terdiri dari tiga departemen: dukungan umum, pemasaran, dan penjualan. General support menempati lantai satu, sedangkan pemasaran dan penjualan berada di lantai dua. Dukungan umum memiliki 28 stasiun kerja, pemasaran memiliki 10 stasiun kerja, dan penjualan memiliki 30 stasiun kerja. Beberapa aplikasi mengharuskan data ditransfer antar departemen, namun umumnya setiap departemen memiliki aplikasinya masing-masing. Setiap orang memerlukan akses ke Internet, Internet internal perusahaan (intranet), dan email. Rancang solusi jaringan area lokal untuk perusahaan ini.

Tampilkan lokasi semua stasiun kerja dan perangkat yang saling terhubung, seperti hub, sakelar, dan router, jika ada yang digunakan.

Tampilkan juga koneksi ke layanan telepon luar yang menyediakan akses Internet. Jenis kabel jaringan area lokal apa yang Anda rekomendasikan? Jenis topologi dan protokol jaringan area lokal apa yang Anda rekomendasikan? Gambarlah denah lantai untuk setiap lantai. Jika memungkinkan, tampilkan kedua denah lantai dalam satu halaman.

Gunakan asumsi berikut:

- a. Hub dan switch yang tersedia memiliki maksimal 24 port.
- b. Beberapa aplikasi perangkat lunak dan kumpulan data besar berada di server departemen.
- c. Untuk mendukung email diperlukan server.

- d. Untuk menunjang intranet perusahaan diperlukan server.
 - e. Perusahaan tidak memiliki anggaran yang tidak terbatas namun bersedia berinvestasi pada teknologi yang berkualitas.
7. Temukan situs Web IEEE (atau lainnya) dan laporkan kemajuan terkini dalam standar 802. Apakah ada standar tambahan untuk Ethernet >10 Gbps atau LAN nirkabel? Apakah ada usulan baru untuk sistem yang tidak disebutkan dalam bab ini? Jelaskan apa yang Anda temukan.
 8. Selain protokol CSMA/CD, terdapat protokol CSMA. Pada sistem apa protokol CSMA digunakan? Mengapa CSMA lebih disukai daripada CSMA/CD dalam sistem ini?
 9. Apakah ada jaringan lokal lainnya yang benar-benar terlupakan? Jika ya, apa yang menyebabkan kematian mereka? Apakah itu teknologi, keuangan, atau politik?
 10. Selain kecepatan transmisi, apakah Gigabit Ethernet sama dengan Ethernet 10-Mbps? Jelaskan tanggapan Anda.
 11. Apakah ada rencana untuk Ethernet 100 Gbps?
 12. Menggunakan Internet, selidiki Ethereal (Wireshark). Unduh salinannya dan gunakan untuk mengamati beberapa lalu lintas pada koneksi Ethernet.
 13. Dengan menggunakan Internet atau sumber eksternal lainnya, kumpulkan literatur tentang switch Ethernet. Apa spesifikasinya (seperti kecepatan port, jumlah port, jenis kabel yang didukung, kecepatan backplane, dll.) dari switch?
 14. Buat peta jaringan area lokal perusahaan atau sekolah Anda. Apakah ada hub? Di mana letak hubnya? Apakah ada saklar? Jika ya, di mana letak sakelarnya? Apakah ada router? Tunjukkan di mana lokasinya.

BAB 8

JARINGAN AREA LOKAL

BAGIAN II

TUJUAN

Setelah membaca bab ini, Anda diharapkan dapat:

- Mencantumkan komponen dasar jaringan area lokal nirkabel
- Mengidentifikasi fungsi utama sistem operasi jaringan
- Mengidentifikasi fitur dasar sistem operasi jaringan masa lalu dan masa kini, termasuk Novell NetWare/OES, Windows Server, UNIX, Linux, dan Mac OS X Server
- Mengenali pentingnya server dan berbagai jenis server yang tersedia
- Mengidentifikasi berbagai tingkatan RAID
- Mengidentifikasi contoh umum perangkat lunak utilitas jaringan dan perangkat lunak Internet
- Mencantumkan berbagai komponen lisensi perangkat lunak
- Mengidentifikasi berbagai jenis perangkat pendukung yang umum ditemukan pada jaringan area lokal

PADA TAHUN 1998, Departemen Kehakiman AS dan Jaksa Agung dari 18 negara bagian mengajukan gugatan antimonopoli terhadap Microsoft Corporation. Yang menjadi masalah adalah persyaratan untuk menyertakan peramban web Microsoft, Internet Explorer, dalam sistem operasi Windows. Kekhawatiran kedua adalah bahwa praktik bisnis Microsoft membatasi inovasi. Klaimnya adalah bahwa praktik perusahaan dalam menggabungkan rangkaian aplikasi telah menyebabkan penurunan keberagaman, sehingga memusatkan pangsa pasar pada rangkaian aplikasi Microsoft.

Setelah pertarungan pengadilan yang panjang dan sering kali tidak menyenangkan, Pengadilan Distrik AS untuk Distrik Columbia memutuskan Microsoft bersalah pada tanggal 3 April 2000, dan memerintahkan perusahaan untuk membagi menjadi dua perusahaan: perusahaan sistem operasi dan perusahaan aplikasi. Pada saat itu, hal ini disamakan dengan pembubaran AT&T pada tahun 1984, ketika AT&T harus menjual perusahaan telepon lokalnya tetapi diizinkan untuk mempertahankan layanan telepon jarak jauh dan pusat penelitiannya (Bell Labs). Namun, pada musim panas tahun 2001, pengadilan banding federal menolak perintah hakim Pengadilan Distrik untuk membubarkan Microsoft. Meskipun demikian, putusan federal tersebut tetap menegakkan inti kasus pemerintah bahwa Microsoft telah melanggar Undang-Undang Antimonopoli Sherman. Pengadilan banding membuka kemungkinan pembubaran, tetapi para hakim mempersempit tuduhan antimonopoli terhadap Microsoft—meningkatkan peluang penyelesaian di luar pengadilan.

Namun, ini bukanlah akhir dari cerita. Pada tanggal 24 Maret 2004, Komisi Eropa memerintahkan Microsoft untuk membayar denda sebesar \$613 juta, merilis versi sistem

operasi Windows tanpa perangkat lunak Windows Media Player, dan mengungkapkan detail kode perangkat lunak Windows dan dengan demikian memudahkan perusahaan perangkat lunak lain untuk memproduksi perangkat lunak yang kompatibel. Microsoft berjanji untuk mengajukan banding atas putusan ini tetapi kalah pada tanggal 17 September 2007, dan setuju untuk membayar. Sayangnya, itu bukanlah akhir bagi Microsoft. Uni Eropa kembali mendenda Microsoft pada tanggal 27 Februari 2008, dengan menyatakan bahwa Microsoft masih belum menyelesaikan masalah perangkat lunak tersebut. Kali ini, perusahaan mungkin akan merugi Rp. 14.4 Trilyun.

Apa itu sistem operasi?

Apa itu sistem operasi jaringan? Apakah keduanya sama?

Pilihan apa saja yang tersedia saat memilih sistem operasi jaringan?

Apakah sistem operasi begitu penting sehingga dapat menyebabkan salah satu perusahaan terbesar di AS bangkrut?

8.1 PENDAHULUAN

Bab Tujuh memulai pembahasan tentang jaringan area lokal dengan memperkenalkan topologi dasar yang mendukung sebagian besar jaringan area lokal dan teknik kontrol akses media yang memungkinkan stasiun kerja mengirimkan data ke jaringan area lokal berkabel. Hub, switch, dan router adalah tiga alat dasar yang menghubungkan perangkat dalam jaringan area lokal dan menghubungkan jaringan area lokal dengan jaringan lain. Bab ini akan menyimpulkan pembahasan tentang jaringan area lokal dengan terlebih dahulu memperkenalkan jaringan area lokal nirkabel dan kemudian perangkat lunak yang mengoperasikan dan mendukung jaringan area lokal.

Meskipun ada banyak jenis perangkat lunak jaringan—seperti alat diagnostik dan pemeliharaan, utilitas, dan lingkungan pengembangan pemrograman—sistem operasi jaringan dan perangkat lunak pendukung jaringan adalah dua yang paling penting. Sistem operasi jaringan sangat penting jika jaringan akan memungkinkan banyak pengguna untuk berbagi sumber daya. Sistem operasi jaringan menyediakan perlindungan kata sandi bagi pengguna pada akun mereka dan administrator jaringan dengan layanan yang membantu mereka mengendalikan akses ke sumber daya jaringan serta menggunakan dan mengelola jaringan. Sistem operasi jaringan area lokal, seperti perangkat keras yang mendukungnya, terus berkembang menjadi alat yang lebih canggih dan rumit setiap hari. Sistem operasi jaringan yang paling populer mencakup Microsoft Windows Server 2008, UNIX, Linux, dan Mac OS X Server.

Bab ini akan menguraikan setiap fitur dan kemampuan dasar sistem operasi ini, dan membandingkan kelebihan dan kekurangannya.

Setelah membahas sistem operasi jaringan, kita akan membahas beberapa komponen perangkat keras dan perangkat lunak yang mendukung sistem operasi jaringan. Komponen pertama adalah server, yang merupakan perangkat utama yang menyimpan dan menjalankan sistem operasi jaringan.

Seperti sistem operasi jaringan, perangkat lunak pendukung jaringan merupakan alat yang penting. Aplikasi pendukung yang paling umum mencakup perangkat lunak antivirus, perangkat lunak antispam, perangkat lunak antispysware, perangkat lunak cadangan, perangkat lunak perlindungan kerusakan, perangkat lunak pemantauan jaringan, perangkat lunak akses jarak jauh, perangkat lunak penilaian keamanan, dan perangkat lunak uninstall. Kita juga akan membahas beberapa perangkat lunak pendukung Internet, seperti peramban web dan perangkat lunak server web. Kita akan menindaklanjuti pembahasan ini dengan pengantar berbagai perjanjian lisensi perangkat lunak yang berlaku untuk perangkat lunak jaringan.

Terakhir, jaringan area lokal memerlukan berbagai jenis perangkat pendukung. Seperti yang Anda lihat di Bab Tujuh, hub, switch, dan router merupakan perangkat pendukung penting untuk segmentasi dan interkoneksi jaringan area lokal. Perangkat pendukung lain yang akan dibahas dalam bab ini meliputi catu daya tak terputus, tape drive, printer, konverter media, perangkat penyimpanan jaringan, dan stasiun kerja. Masing-masing perangkat ini akan diperkenalkan, beserta contoh yang menunjukkan cara penggunaan perangkat tersebut.

8.2 ETHERNET NIRKABEL

Jaringan area lokal yang tidak didasarkan terutama pada kabel fisik tetapi menggunakan transmisi nirkabel antar stasiun kerja adalah LAN nirkabel, atau Ethernet nirkabel. Dengan memasang pemancar/penerima ke kartu antarmuka jaringan khusus pada stasiun kerja atau laptop, dan perangkat keras serupa pada perangkat yang disebut titik akses, dimungkinkan untuk mengirimkan data antara stasiun kerja dan jaringan dengan kecepatan hingga jutaan bit per detik. Selain itu, stasiun kerja dapat ditempatkan di mana saja dalam jangkauan transmisi yang dapat diterima. Jangkauan yang dapat diterima ini bervariasi tergantung pada teknologi nirkabel yang digunakan tetapi biasanya berkisar antara beberapa kaki dan beberapa ratus kaki. Anda dapat berpendapat bahwa LAN nirkabel pada dasarnya adalah topologi bintang karena stasiun kerja nirkabel biasanya memancarkan dan mengirimkan data ke titik akses.

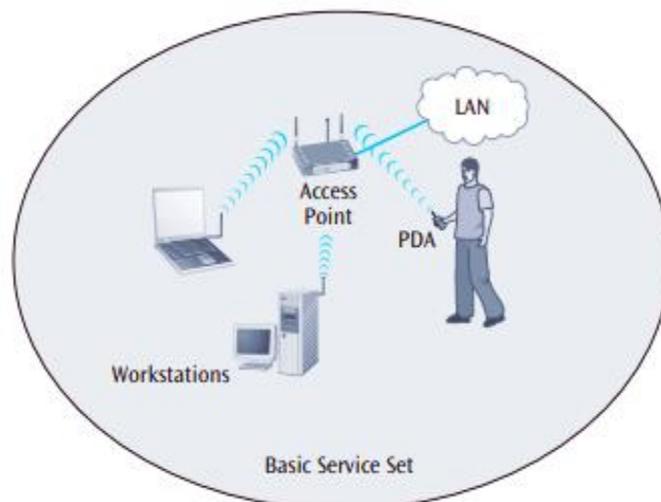
Perhatikan bahwa sebagian besar jaringan area lokal nirkabel sebenarnya merupakan kombinasi dari teknologi nirkabel dan kabel. Bagian nirkabel terdiri dari laptop/notebook/netbook, komputer desktop, printer nirkabel dan stasiun permainan, perangkat genggam seperti ponsel dan tablet, dan titik akses. Di ujung lain titik akses ini (yang rinciannya akan segera diperiksa) terdapat jaringan area lokal berkabel. Bagian berkabel berisi kabel Kategori 5e/6 yang biasa beserta berbagai kombinasi hub, switch, router, dan server.

Jelas, salah satu keuntungan terkuat dari LAN nirkabel adalah tidak diperlukannya kabel bagi perangkat pengguna untuk berkomunikasi dengan jaringan. Hal ini menjadikan LAN nirkabel solusi yang sempurna untuk berbagai aplikasi. Pertimbangkan lingkungan di mana tidak mungkin untuk memasang kabel, seperti di tengah gudang, atau di lantai bursa saham. LAN nirkabel juga akan berfungsi dengan baik di gedung bersejarah, atau gedung dengan dinding beton atau marmer tebal, di mana mengebor lubang melalui dinding, langit-langit, atau lantai tidak diinginkan atau sulit. Banyak kantor bisnis telah menggabungkan jaringan

area lokal nirkabel karena alasan lain juga. Misalkan seorang karyawan sedang duduk di biliknya mengerjakan laptopnya melalui koneksi nirkabel. Tiba-tiba, karyawan tersebut dipanggil ke sebuah rapat. Ia mengambil laptopnya, berjalan ke ruang rapat, dan terus bekerja melalui koneksi nirkabel. Demikian pula, banyak kampus perguruan tinggi dan sekolah menengah atas telah menyiapkan LAN nirkabel, sehingga siswa dapat mengakses operasi jaringan sambil duduk di kelas, bekerja di perpustakaan, atau menikmati hari yang indah di lapangan.

Untuk membuat jaringan area lokal nirkabel, beberapa komponen dasar diperlukan. Komponen pertama adalah perangkat pengguna (juga disebut stasiun nirkabel), seperti komputer laptop, stasiun kerja, atau perangkat genggam. Perangkat pengguna memiliki NIC khusus yang menerima dan mengirimkan sinyal nirkabel. Komponen kedua adalah jaringan area lokal berkabel. Ini adalah komponen jaringan konvensional yang mendukung stasiun kerja, server, dan protokol kontrol akses media standar. Sebagian besar jaringan nirkabel terhubung ke jaringan area lokal berkabel. Komponen ketiga adalah titik akses, atau router nirkabel, yang merupakan komponen yang berkomunikasi dengan perangkat pengguna nirkabel. Titik akses pada dasarnya adalah perangkat antarmuka antara perangkat pengguna nirkabel dan jaringan area lokal berkabel. Titik akses juga bertindak sebagai sakelar/jembatan dan mendukung protokol kontrol akses media.

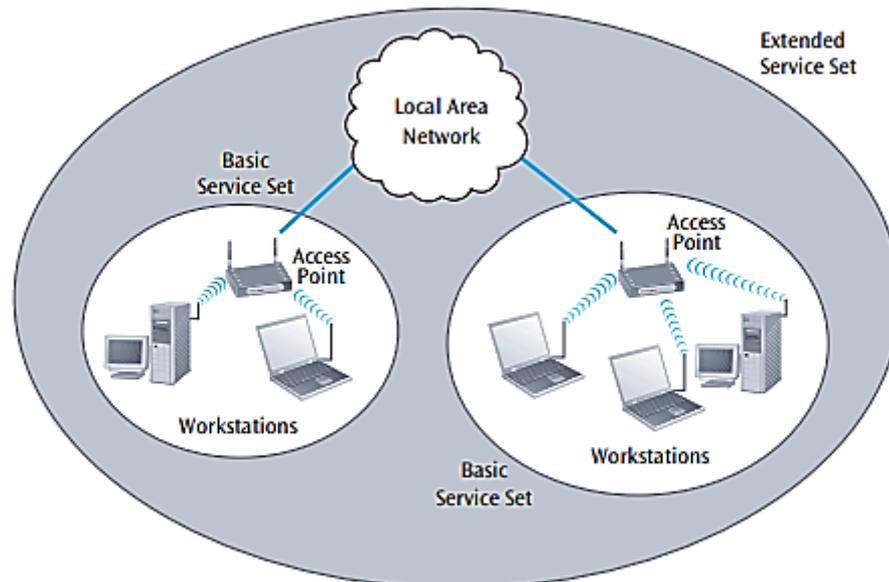
Jaringan area lokal nirkabel biasanya ditemukan dalam tiga konfigurasi dasar. Yang pertama adalah LAN nirkabel sel tunggal (Gambar 8-1). Di bagian tengah sel terdapat titik akses, yang terhubung ke LAN kabel. Semua perangkat pengguna berkomunikasi dengan satu titik akses ini dan bersaing untuk mendapatkan rangkaian frekuensi yang sama. Standar LAN nirkabel menyebut sel ini sebagai Basic Service Set (BSS).



Gambar 8-1 Konfigurasi LAN nirkabel sel tunggal

Tipe kedua dari konfigurasi LAN nirkabel adalah tata letak multisel (Gambar 8-2). Dalam konfigurasi ini, beberapa sel didukung oleh beberapa titik akses, seperti dalam jaringan telepon seluler. Perangkat pengguna berkomunikasi dengan titik akses terdekat dan dapat berpindah dari satu sel ke sel lainnya. Cara lain yang membuat konfigurasi ini mirip dengan

jaringan telepon seluler adalah bahwa setiap sel menggunakan serangkaian frekuensi yang berbeda untuk komunikasi antara perangkat pengguna dan titik akses. Istilah LAN nirkabel untuk kumpulan beberapa Set Layanan Dasar adalah Set Layanan Diperluas (ESS).



Gambar 8-2 Konfigurasi LAN nirkabel multi-sel

Konfigurasi LAN nirkabel ketiga adalah tata letak peer-to-peer, atau ad hoc. Dengan konfigurasi ini, tidak ada titik akses di pusat sel. Setiap perangkat pengguna berkomunikasi langsung dengan perangkat pengguna lainnya. Konfigurasi seperti ini dapat ditemukan dalam rapat bisnis di mana semua perangkat pengguna mentransmisikan dan berbagi informasi pada saat yang sama. Karena adanya komunikasi antar semua klien, LAN ad-hoc bekerja paling baik dengan sejumlah kecil perangkat.

Standar LAN Nirkabel

Ketika LAN nirkabel pertama kali muncul, organisasi lambat menerimanya. Untuk meningkatkan penerimaan, rangkaian protokol IEEE 802 diciptakan untuk mendukung berbagai jenis jaringan area lokal nirkabel yang ada. Sebagai bagian dari upaya ini, persetujuan standar nirkabel IEEE 802.11 pada bulan Juni 1997 sangat membantu standarisasi jaringan nirkabel dan mempercepat pertumbuhan serta penerimaannya. Pada dasarnya, spesifikasi 802.11 mendefinisikan tiga jenis koneksi lapisan fisik yang berbeda untuk menyesuaikan harga, kinerja, dan operasi dengan aplikasi tertentu. Jenis lapisan fisik pertama mendefinisikan transmisi inframerah. Inframerah, seperti yang mungkin Anda ingat dari Bab Tiga, berbasis garis pandang dan tidak dapat menembus dinding yang kokoh. Kecepatan transmisi untuk nirkabel inframerah berkisar antara 1 hingga 2 Mbps. Jenis lapisan fisik kedua mendefinisikan teknologi yang dapat mengirimkan sinyal aman (spread spectrum) dan dapat mengirimkan data pada kecepatan hingga 2 Mbps di lingkungan yang tenang dan 1 Mbps di lingkungan yang bising untuk jarak hingga 800 kaki. Jenis lapisan fisik ketiga juga menyebarkan spektrum tetapi menggunakan frekuensi hopping dan dapat mengirimkan data pada 2 Mbps sejauh 300 kaki.

Seperti yang kita lihat di Bab Tiga, sejak diperkenalkannya IEEE 802.11, protokol LAN nirkabel IEEE lainnya telah muncul. IEEE 802.11b, yang diratifikasi pada bulan September 1999, dapat mengirimkan data pada kecepatan teoritis 11 Mbps (karena gangguan, kecepatan aktual kira-kira setengah dari kecepatan teoritis) menggunakan sinyal 2,4 GHz.

Banyak pengguna yang merasa kecepatan data 802.11 sebesar 2 Mbps terlalu lambat merasa gembira melihat produk 802.11b beredar di pasaran. Nama lain untuk 802.11b (serta standar LAN nirkabel 802.11 lainnya) adalah Wi-Fi (wireless fidelity). IEEE 802.11g, diperkenalkan pada tahun 2002, mengirimkan data pada kecepatan teoritis 54 Mbps (sekali lagi, kecepatan aktual sekitar setengahnya) menggunakan frekuensi 2,4 GHz yang sama yang digunakan dalam 802.11b. Juga diperkenalkan pada tahun 2002 adalah IEEE 802.11a, yang mampu mendukung kecepatan transmisi teoritis 54-Mbps (sekali lagi, kecepatan aktual sekitar setengahnya) menggunakan rentang frekuensi 5-GHz.

Penambahan terbaru pada pasar LAN nirkabel adalah standar IEEE 802.11n. 802.11n memiliki kecepatan data maksimum teoritis 600 Mbps dengan kecepatan data aktual sekitar 100 hingga 145 Mbps. Untuk mendukung kecepatan tinggi tersebut, standar baru ini menggunakan teknologi yang disebut multiple input multiple output. Multiple input multiple output (MIMO) adalah teknik di mana perangkat seluler dan titik akses memiliki beberapa antena pintar yang membantu mengurangi interferensi dan pantulan sinyal.

Protokol nirkabel yang lebih baru memang hadir dengan beberapa karakteristik menarik. Rentang frekuensi 5-GHz tinggi yang digunakan dalam IEEE 802.11a membutuhkan begitu banyak daya sehingga laptop dan perangkat portabel mengalami kesulitan mengirimkan sinyal ini untuk jangka waktu yang lama. Kedua, jarak transmisi untuk rentang frekuensi yang lebih tinggi lebih pendek daripada rentang frekuensi yang lebih rendah. Perkiraan saat ini (dan kasar) menempatkan jarak transmisi maksimum 802.11b dan 802.11g (2,4 GHz) pada sekitar 45 meter (150 kaki) di dalam ruangan dan 90 meter (300 kaki) di luar ruangan, dan 802.11a (5 GHz) pada sekitar sepertiga dari 802.11b dan g. Dengan demikian, sebuah perusahaan akan membutuhkan sekitar tiga kali lebih banyak titik akses untuk rentang 5 GHz daripada untuk rentang 2,4 GHz, yang akan meningkatkan biaya pemasangan dan pemeliharaan perusahaan. Untuk lebih memperumit masalah, panjang gelombang yang lebih pendek dari 5 GHz juga mengalami masalah saat menembus dinding, lantai, dan furnitur. Hal ini juga dapat memengaruhi keputusan perusahaan untuk beralih ke produk rentang frekuensi yang lebih tinggi. Di sisi positifnya, rentang 5 GHz 802.11a mengalami lebih sedikit gangguan sinyal dari perangkat seperti oven microwave dan dengan demikian seharusnya mampu menghasilkan kecepatan transmisi yang lebih tinggi. Melihat beberapa produk 802.11n terkini, kami melihat beberapa yang mampu mentransmisikan hingga 90 meter (300 kaki) di dalam ruangan dan 279 meter (900 kaki) di luar ruangan.

Area minat tambahan lainnya terkait dengan LAN nirkabel terkait dengan keamanan. (Meskipun seluruh Bab Dua Belas dikhususkan untuk keamanan, kami akan membahas sedikit tentang keamanan LAN nirkabel.) Keamanan pada LAN nirkabel awalnya disediakan oleh Wired Equivalent Privacy (WEP). Meskipun WEP didasarkan pada teknik enkripsi yang relatif modern, banyak kritikus merasa bahwa itu tidak cukup kuat untuk menghentikan

penyadapan: Kuncinya terlalu kecil dan tidak dapat diubah. Banyak pengguna merasa bahwa karena kelemahan WEP, tidak ada gunanya menggunakannya, sehingga membuka transmisi LAN nirkabel mereka kepada siapa pun yang berada dalam jangkauan.

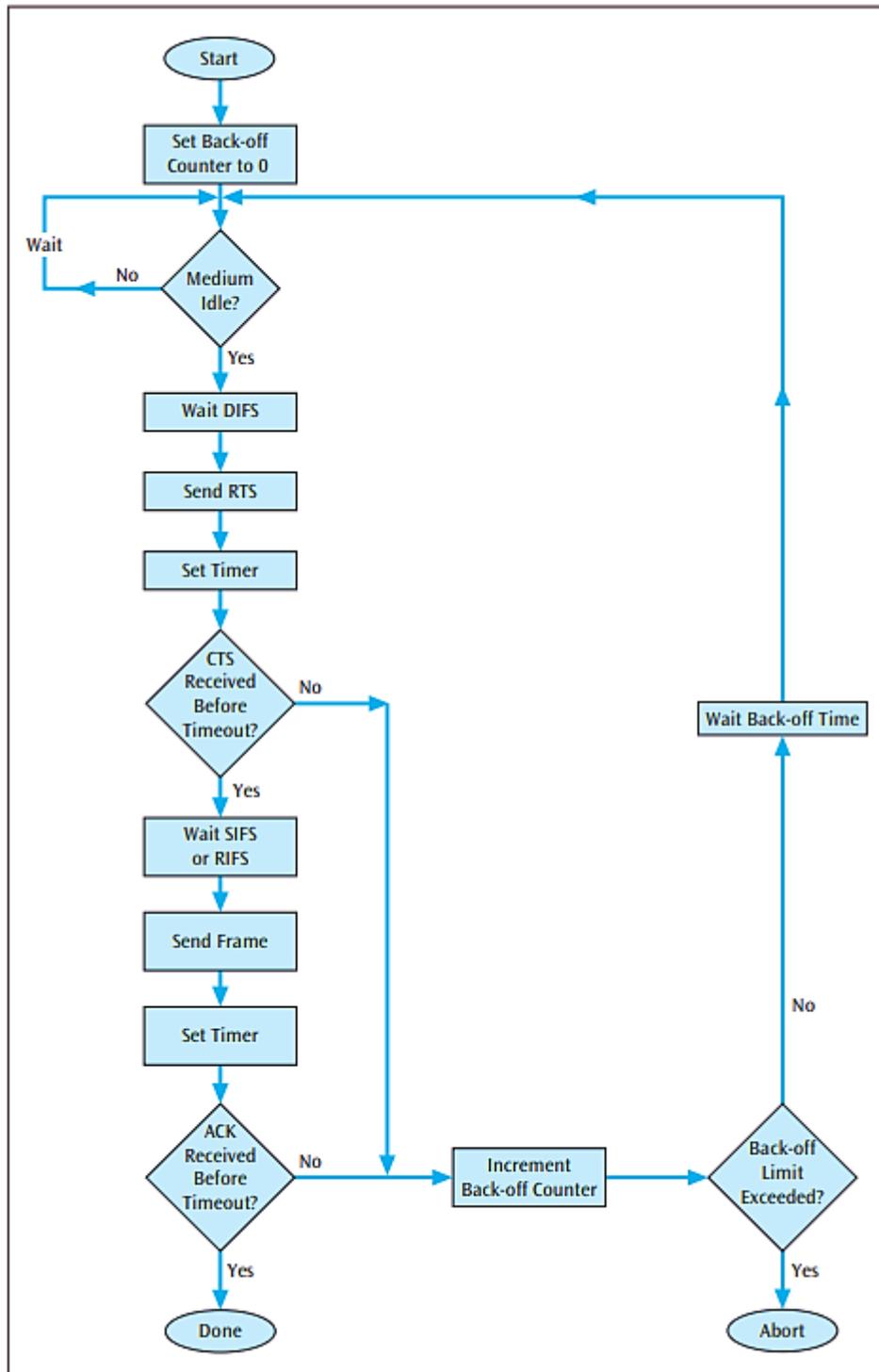
Banyak yang berpendapat bahwa ini adalah strategi yang buruk. Untuk meningkatkan WEP, standar keamanan sementara yang dijuluki Wi-Fi Protected Access (WPA) diciptakan. Di antara penawaran WPA adalah Temporal Key Integrity Program (TKIP). TKIP menggunakan kunci 128-bit pada setiap paket dan kunci tersebut berubah pada setiap paket yang dikirimkan, sehingga hampir mustahil bagi pengguna yang tidak berwenang dengan perangkat nirkabel untuk terhubung ke sinyal yang dilindungi WPA dan akhirnya mengetahui skema transmisi. Wi-Fi Protected Access II (WPA2) adalah standar enkripsi terbaru yang mendukung LAN nirkabel dan telah menggantikan TKIP dengan teknik enkripsi yang semakin kuat yang disebut CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

Sekarang setelah kita memperkenalkan berbagai standar LAN nirkabel, mari kita alihkan perhatian kita ke teknik kontrol akses media yang mendasarinya yang memungkinkan perangkat nirkabel untuk berkomunikasi dengan titik akses nirkabel.

8.3 CSMA/CA NIRKABEL

Protokol kontrol akses media berbasis pertentangan yang mendukung jaringan area lokal nirkabel memiliki dua perbedaan menarik dari protokol CSMA/CD lama yang ditemukan pada LAN kabel berbasis hub. Pertama, tidak ada deteksi tabrakan. Dengan kata lain, pemancar tidak mendengarkan selama transmisinya untuk mengetahui apakah ada tabrakan dengan sinyal lain di suatu tempat di jaringan. Tiga alasan untuk ini adalah biaya produksi pemancar nirkabel yang dapat mentransmisikan dan mendengarkan pada saat yang sama, fakta bahwa tidak ada kabel untuk mendengarkan peningkatan tegangan (tabrakan dua sinyal), dan fakta bahwa jika sangat sering dua stasiun kerja begitu jauh sehingga mereka tidak dapat mendengar sinyal transmisi satu sama lain, maka mereka tidak akan mendengar tabrakan (skenario stasiun kerja tersembunyi). Sebaliknya, algoritme protokol yang mendukung LAN nirkabel membatasi kapan stasiun kerja dapat mentransmisikan, dalam upaya untuk mengurangi jumlah tabrakan. Jenis algoritme yang mencoba menghindari tabrakan disebut akses berganda penginderaan pembawa dengan penghindaran tabrakan (CSMA/CA). Bagaimana algoritme membatasi kapan stasiun kerja dapat mentransmisikan? Bagian dari jawaban itu terkait dengan perbedaan menarik kedua: tingkat prioritas. Dalam upaya untuk menyediakan tingkat prioritas tertentu pada urutan transmisi, algoritma CSMA/CA telah dimodifikasi agar berfungsi sesuai dengan aturan berikut: Jika perangkat pengguna ingin mentransmisikan dan media dalam keadaan diam, perangkat tidak diizinkan untuk segera mentransmisikan. Sebaliknya, perangkat dibuat menunggu selama periode waktu singkat yang disebut ruang antar-bingkai (IFS). Jika media masih diam setelah ruang antar-bingkai ini, perangkat kemudian diizinkan untuk mentransmisikan. Bagaimana ruang antar-bingkai menyediakan sistem prioritas? Ada sejumlah waktu ruang antar-bingkai yang

berbeda yang dapat digunakan. Lihat diagram alir pada Gambar 8-3 untuk mengikuti diskusi ini.



Gambar 8-3 Diagram alir yang menunjukkan algoritma untuk CSMA/CA

Suatu perangkat ingin mengirim ke titik akses. Seperti yang akan kita lihat sebentar lagi, jika suatu perangkat tidak dapat mengirim, perangkat tersebut harus mundur dan menunggu. Ada batasan berapa kali perangkat akan mundur. Untuk menentukan apakah

batasan ini telah terpenuhi, perangkat akan menggunakan Penghitung Mundur. Jadi, untuk memulai, perangkat menyetel Penghitung Mundur ke 0 lalu mendengarkan media untuk melihat apakah ada orang lain yang mengirim. Jika media awalnya sibuk, perangkat akan terus mendengarkan media tersebut. (Beberapa perangkat lunak akan meminta perangkat untuk mencoba lagi nanti setelah jangka waktu acak.) Ketika media menjadi tidak aktif, perangkat pengguna tidak segera mengirim tetapi menunda untuk Differential Interframe Space (DIFS).

Prosedur ini membantu mencegah sejumlah pengguna mendengar media yang tidak aktif, mengirim pada saat yang sama, dan menyebabkan tabrakan. Jika media masih tidak aktif setelah DIFS, perangkat pengguna mengirimkan Request to Send (RTS) ke titik akses dan menyetel pengatur waktu. Mudah-mudahan, Clear to Send (CTS) akan diterima dari titik akses sebelum pengatur waktu habis. Jika CTS diterima tepat waktu, perangkat akan menunggu lagi di ruang antar-bingkai, tetapi kali ini ruang antar-bingkainya lebih pendek (seperti Ruang Antar-bingkai Pendek [SIFS] atau Ruang Antar-bingkai yang Diperkecil [RIFS]). Setelah SIFS (atau RIFS), perangkat akhirnya mentransmisikan bingkai. Seperti yang dapat Anda lihat dari diagram alur pada Gambar 8-3, perangkat menunggu pengakuan (ACK) bahwa bingkai telah diterima dengan benar. Jika terjadi kesalahan, perangkat akan menambah Penghitung Mundurnya sebesar 1, memeriksa untuk memastikan bahwa ia tidak mundur terlalu sering, dan jika tidak, mencoba seluruh prosedur itu lagi.

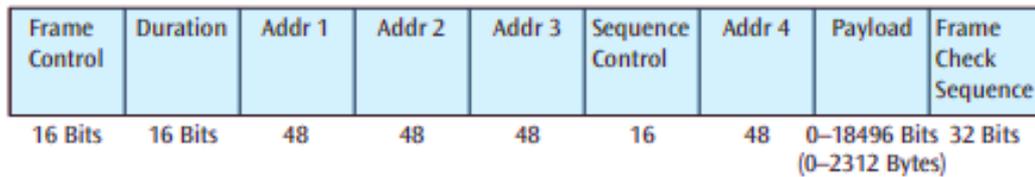
Ada satu teknik tambahan lagi yang digunakan untuk menghindari tabrakan selama seluruh prosedur ini. Jika beberapa perangkat ingin mentransmisikan bingkai, tetapi baru saja mendengar CTS datang dari titik akses, maka ia tahu perangkat lain telah mendahuluinya. Bila perangkat melihat CTS ini, perangkat akan mundur dan menunggu perkiraan waktu yang diperlukan (periode NAV) agar perangkat yang mendahuluinya menyelesaikan transmisinya. Hal ini sekali lagi mengurangi kemungkinan dua perangkat atau lebih mencoba melakukan transmisi pada saat yang bersamaan.

Format bingkai CSMA/CA

Untuk memeriksa informasi terakhir kita mengenai jaringan area lokal nirkabel, mari kita lihat format bingkai yang dikirim antar perangkat dalam jaringan. Saya rasa Anda akan setuju bahwa ada beberapa hal menarik yang perlu diteliti lebih lanjut.

Format dasar untuk bingkai CSMA/CA ditunjukkan pada Gambar 8-4. Salah satu bidang pertama yang perlu diperhatikan adalah bidang Durasi. Bidang ini berisi nilai yang digunakan untuk menyetel nilai NAV yang baru saja disebutkan di atas. Kedua, perhatikan bahwa ada empat bidang alamat (ingat Ethernet standar hanya memiliki dua). Mengapa Ethernet nirkabel memerlukan empat? Selain alamat sumber dan tujuan yang biasa, ada juga dua kemungkinan alamat titik akses. Misalnya, jika perangkat (alamat sumber) mengirim ke titik akses (alamat kedua) dan kemudian dari sana ke titik akses kedua (alamat ketiga) dan akhirnya ke perangkat tujuan (alamat keempat), maka diperlukan empat alamat. Ini akan menjadi contoh jaringan dengan beberapa Set Layanan Dasar. Jika hanya satu BSS yang terlibat, maka hanya tiga alamat dari keempatnya yang digunakan: sumber, tujuan, dan titik akses. Terakhir, perlu dicatat bahwa payload dapat memiliki panjang antara 0 dan 2312 byte. (Tiga kolom yang tersisa adalah Frame Control, yang berisi berbagai kolom untuk mengendalikan transmisi; Sequence

Control, yang menentukan nomor urut frame saat ini; dan Frame Check Sequence, yang merupakan checksum redundansi siklik 32-bit.)



Gambar 8-4 Berbagai bidang bingkai CSMA/CA

Sekarang kita akan mengalihkan perhatian kita ke beberapa perangkat lunak yang berjalan di jaringan area lokal. Kita akan mulai dengan perangkat lunak yang paling besar dan paling penting: sistem operasi jaringan.

8.4 SISTEM OPERASI JARINGAN

Apa itu sistem operasi jaringan (NOS)? Apa saja fungsi yang dijalankannya? Apa perbedaan sistem operasi jaringan dengan sistem operasi (OS) pada PC? Cara terbaik untuk mulai memahami sistem operasi jaringan adalah dengan mempelajari fungsi dasar OS. Setelah memahami fungsi dasar sistem operasi, Anda dapat mulai memahami fungsi tambahan sistem operasi jaringan.

Sistem operasi adalah program yang awalnya dimuat ke dalam memori komputer saat komputer dinyalakan; sistem ini mengelola semua program (aplikasi) dan sumber daya lainnya (seperti disk drive, memori, dan perangkat periferal) di komputer. Bahkan setelah aplikasi dimulai dan dijalankan, aplikasi tersebut menggunakan sistem operasi dengan membuat permintaan layanan melalui antarmuka pemrograman aplikasi (API) yang ditentukan. Selain itu, pengguna dapat berinteraksi langsung dengan sistem operasi melalui antarmuka seperti antarmuka pengguna grafis, bahasa perintah, atau shell.

Sistem operasi dapat menjalankan sejumlah layanan, yang sebagian besar sangat penting untuk pengoperasian sistem komputer modern yang tepat. Salah satu layanan terpenting adalah menentukan aplikasi mana yang berjalan dalam urutan apa, dan berapa banyak waktu yang harus diberikan untuk setiap aplikasi sebelum menjalankan aplikasi lain. Dalam sistem operasi multitugas, beberapa program dapat berjalan pada saat yang sama. Dalam kasus ini, sistem operasi menjadwalkan setiap tugas dan mengalokasikan sedikit waktu untuk pelaksanaan tugas tersebut. Pada kenyataannya, sistem operasi multitugas hanya menjalankan satu program pada satu waktu, tetapi berpindah dari satu program ke program berikutnya dengan sangat cepat sehingga tampak seolah-olah beberapa program sedang dijalankan pada saat yang sama. Tugas yang sama penting dan sulitnya bagi sistem operasi adalah menangani operasi input dan output yang sangat rumit ke dan dari perangkat keras yang terpasang, seperti hard disk, printer, dan modem. Hard disk drive sangat rumit dan rumit sehingga akan menjadi hukuman yang kejam dan tidak biasa untuk meminta pengguna menentukan lokasi yang tepat dari setiap rekaman data saat ditulis atau dibaca dari hard disk. Sama rumitnya dengan mengendalikan ruang penyimpanan pada hard disk drive adalah

mengendalikan ruang penyimpanan di memori utama komputer. Karena pengguna cenderung menjalankan beberapa aplikasi secara bersamaan, sistem operasi harus mampu mengalokasikan jumlah memori utama yang terbatas dengan cara yang menyediakan setiap aplikasi dengan jumlah memori yang cukup untuk beroperasi.

Sistem operasi modern juga harus menyediakan berbagai tingkat keamanan sistem operasi, termasuk keamanan direktori dan berkas, keamanan memori, dan keamanan sumber daya. Seiring dengan semakin canggihnya aplikasi dan penggunaannya, kemampuan sistem operasi untuk memberikan perlindungan dari pengguna yang tidak bertanggung jawab menjadi semakin penting.

Terakhir, fungsi yang mungkin tidak sepenting multitasking, manajemen memori dan penyimpanan, atau keamanan—tetapi sebenarnya sama pentingnya—adalah mengomunikasikan status operasi. Sistem operasi mengirimkan pesan ke aplikasi, pengguna interaktif, atau operator sistem tentang status operasi saat ini. Sistem operasi juga mengirimkan pesan tentang kesalahan yang mungkin terjadi.

Sejumlah sistem operasi populer terdapat pada berbagai jenis sistem komputer. Misalnya, sistem operasi populer untuk komputer mikro meliputi Mac OS X, UNIX, Linux, dan berbagai bentuk Windows XP/Vista/7. Sistem operasi yang lebih baru yang mengoperasikan telepon pintar (seluler) adalah sistem Android. Sistem operasi populer untuk komputer yang lebih besar (komputer mini dan mainframe) meliputi OS/390 dan AS/400 milik IBM, VMS (OpenVMS) milik DEC, dan lagi-lagi UNIX dan Linux.

Sistem operasi jaringan (NOS) adalah program besar dan kompleks yang dapat mengelola sumber daya umum di sebagian besar jaringan area lokal, selain menjalankan layanan sistem operasi standar yang disebutkan sebelumnya. Tabel 8-1 merangkum fungsi sistem operasi jaringan. Sumber daya yang harus dikelola oleh sistem operasi jaringan biasanya meliputi satu atau beberapa server, beberapa printer jaringan, satu atau beberapa jaringan fisik, dan sejumlah besar pengguna yang secara langsung, dan terkadang dari jarak jauh, terhubung ke jaringan. Di antara sumber daya ini, server adalah yang terpenting. Server, seperti yang akan Anda pelajari sebentar lagi, biasanya adalah stasiun kerja berdaya tinggi yang mengelola sistem berkas besar berisi kumpulan data, profil pengguna, dan informasi akses tentang semua periferal jaringan.

Tabel 8-1 Ringkasan fungsi sistem operasi jaringan

Fungsi Sistem Operasi Jaringan
Kelola satu atau lebih server jaringan
Memelihara sistem file kumpulan data, aplikasi, profil pengguna, periferal jaringan
Mengkoordinasikan semua sumber daya dan layanan yang tersedia
Memproses permintaan dari pengguna
Meminta pengguna untuk login jaringan, memvalidasi akun, menerapkan pembatasan, menjalankan fungsi akuntansi
Kelola satu atau lebih printer jaringan
Kelola interkoneksi antar jaringan area lokal
Kelola pengguna yang terhubung secara lokal
Kelola pengguna yang terhubung dari jarak jauh

Keamanan sistem pendukung
 Mendukung fungsi klien/server
 Mendukung pengembangan halaman Web dan operasi server Web

Sistem operasi jaringan juga menjalankan berbagai fungsi pendukung jaringan, termasuk koordinasi semua sumber daya dan layanan di jaringan dan pemrosesan permintaan dari stasiun kerja "klien" atau pengguna. Sistem operasi jaringan juga mendukung interaksi pengguna dengan meminta pengguna untuk masuk ke jaringan, memvalidasi akun pengguna, membatasi pengguna untuk mengakses sumber daya yang tidak diberikan aksesnya, dan menjalankan fungsi akuntansi pengguna.

Fungsi sistem operasi jaringan penting lainnya adalah kemampuan sistem operasi untuk berinteraksi dengan Internet. Semakin banyak pengguna yang bekerja di jaringan area lokal berharap menemukan koneksi yang lancar antara stasiun kerja mereka dan Internet. Jika pengguna ini harus membuat halaman Web Internet, mereka ingin memiliki alat yang tersedia untuk membuat dan memelihara halaman tersebut. Sistem operasi jaringan kemudian harus menyediakan interkoneksi yang lancar ke perangkat lunak berbasis Web yang menyimpan halaman Web dan membuatnya dapat diakses oleh pengguna korporat internal dan pengguna Internet eksternal. Dengan demikian, sistem operasi jaringan harus mampu mendukung aplikasi dan alat yang diperlukan untuk mendukung operasi Internet. Menariknya, banyak sistem operasi desktop saat ini yang menggabungkan banyak fitur yang dijelaskan sebelumnya, sehingga memungkinkan pengguna perorangan untuk membuat sistem operasi jaringan untuk rumah dan usaha kecil mereka. Dengan demikian, batasan antara sistem operasi desktop (seperti Windows 7) dan sistem operasi jaringan (seperti Windows 2008) telah kabur dalam beberapa tahun terakhir. Meskipun demikian, masih ada, seperti yang akan segera kita lihat, perbedaan yang signifikan antara kedua jenis sistem tersebut.

8.5 SISTEM OPERASI JARINGAN MASA LALU DAN SEKARANG

Seperti yang baru saja Anda pelajari, sistem operasi jaringan mendukung banyak fungsi yang biasanya kita, sebagai pengguna, anggap remeh. Memahami fungsi-fungsi dasar ini akan memungkinkan Anda untuk memeriksa sistem operasi jaringan yang sebenarnya dengan lebih saksama. Setelah memeriksa fungsi-fungsi dasar, mari kita alihkan perhatian kita ke beberapa sistem operasi jaringan yang paling populer di pasaran dan melihat bagaimana masing-masing mendukung fungsi-fungsi dasar ini. Namun sebelum kita membahasnya, mari kita mulai dengan pelopor sistem operasi jaringan penting yang sudah tidak ada lagi di pasaran: NetWare.

Novell NetWare

Novell didirikan pada tahun 1983 dan merupakan salah satu pengembang pertama sistem operasi jaringan. Selama bertahun-tahun, perusahaan tersebut menghasilkan sejumlah produk yang berpengaruh, termasuk NetWare Directory Services (NDS), yang merupakan sistem cerdas yang mengautentikasi pengguna dan mencakup basis data informasi terdistribusi tentang setiap aplikasi, pengguna, server, dan sumber daya di jaringan. NetWare 6 adalah versi terakhir dari sistem operasi jaringan Novell sebelum produk tersebut berganti

nama menjadi Open Enterprise Server (lebih lanjut tentang itu akan segera dibahas). Pada suatu saat, lebih dari 70 persen pasar LAN menggunakan sistem operasi jaringan Novell. Meskipun NetWare telah hengkang, produk tersebut memperkenalkan banyak fitur dan konsep yang telah dimasukkan ke dalam sistem operasi jaringan lainnya. Jadi, ada baiknya meluangkan waktu sejenak untuk menelaah warisan NetWare.

Fitur menarik yang dimiliki oleh semua versi NetWare adalah bahwa antarmuka pengguna hampir tidak terlihat oleh pengguna. Bila stasiun kerja merupakan bagian dari sistem operasi jaringan Novell, stasiun kerja tersebut tetap harus menjalankan sistem operasi berbasis stasiun kerja seperti Windows XP/Vista/7 atau Mac OS X. Pengguna melakukan operasi tipe Windows seperti membuka folder dan mengklik dua kali ikon aplikasi tanpa menyadari bahwa aplikasi yang sedang digunakan atau berkas yang diminta secara fisik berada di tempat lain di jaringan—mungkin di server, bukan di stasiun kerja milik pengguna. Administrator jaringan memerintahkan Novell untuk menyembunyikan detail tersebut dari pengguna dan menjalankan semua fungsi jaringan, seperti permintaan klien/server dan operasi pencetakan jaringan, dengan sedikit atau tanpa sepengetahuan pengguna.

Misalnya, anggaplah Anda menggunakan pengolah kata dan ingin mencetak dokumen. Untuk melakukannya, Anda mengklik ikon printer di program pengolah kata. Jika Anda (atau administrator jaringan) memerintahkan stasiun kerja Anda untuk mengalihkan semua keluaran printer ke printer jaringan, pekerjaan cetak Anda tidak akan dicetak pada printer di kantor Anda (dengan asumsi Anda memilikinya), tetapi akan dialihkan ke printer lain. Setelah pengalihan ini ditetapkan, semua permintaan cetak di masa mendatang akan secara otomatis diteruskan ke pencetak jaringan dalam operasi yang transparan bagi Anda dan aplikasi pengolah kata. Sistem operasi jaringan Novell adalah yang pertama kali melakukan pengalihan ini pada jaringan area lokal, dan sekarang semua sistem operasi jaringan lainnya menggabungkan fitur ini.

Versi pertama NetWare yang memperoleh popularitas luas adalah Versi 3, yang dirilis pada tahun 1989. Salah satu fitur utama Versi 3 adalah bindery. Bindery adalah struktur (mirip dengan basis data) yang berisi nama pengguna dan kata sandi pengguna jaringan dan grup pengguna yang diberi wewenang untuk masuk ke server tersebut; bindery terdiri dari tiga file yang ditautkan dan tidak identik yang dienkripsi demi alasan keamanan. Bindery berisi data yang hanya berkaitan dengan server tempatnya berada. Bindery juga menyimpan informasi tentang layanan lain yang disediakan oleh server kepada klien, seperti informasi akses printer, modem, dan bridge/router. Setiap server pada jaringan multiserver memerlukan dan memelihara bindery-nya sendiri, dan pengguna diharuskan untuk masuk ke server tertentu. Pengguna yang memerlukan akses ke dua server akan memerlukan akun di setiap server dan harus masuk ke setiap server secara terpisah.

NetWare Versi 4 merupakan perubahan signifikan dari NetWare 3. Versi 4 memperkenalkan NetWare Directory Services (disebut Novell Directory Services di versi selanjutnya), yang menggantikan bindery. NDS adalah basis data yang menyimpan informasi dan akses ke setiap sumber daya di jaringan, termasuk pengguna, kelompok pengguna, printer, set data, dan server. NDS didasarkan pada standar yang terkenal untuk layanan

direktori yang disebut X.500. Di NDS, semua sumber daya jaringan dianggap sebagai objek, terlepas dari lokasi fisiknya yang sebenarnya. NDS bersifat global terhadap jaringan dan direplikasi pada beberapa server untuk melindunginya dari kegagalan di satu titik. Karena NDS bersifat global, pengguna dapat masuk dari lokasi mana pun di jaringan dan mengakses sumber daya apa pun yang telah diberikan izin kepada mereka. Setiap pengguna yang diizinkan masuk ke jaringan dimasukkan ke dalam NDS oleh administrator jaringan. Demikian pula, semua perangkat pendukung jaringan seperti printer juga dimasukkan ke dalam NDS. Misalnya, jika pengguna X ingin menggunakan printer Y, administrator jaringan harus menetapkan izin yang sesuai untuk mengizinkan pengguna X mengakses printer Y. Izin ini juga dimasukkan ke dalam NDS. Setiap kali pengguna X masuk dan mencoba mengirim pekerjaan cetak ke printer Y, NDS akan dirujuk untuk mendapatkan izin yang diperlukan.

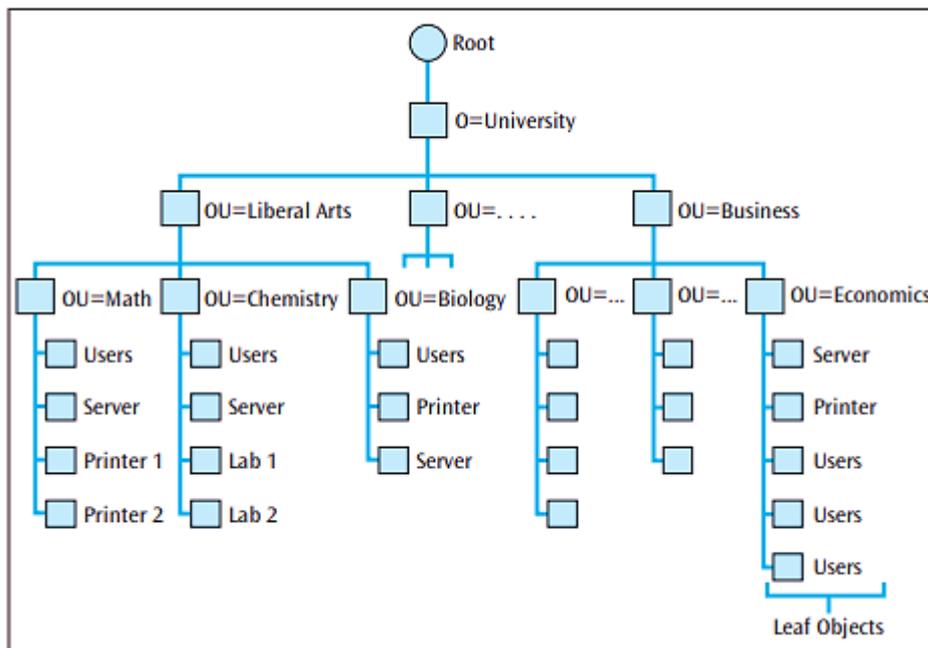
Ide dasar yang mendasari NDS (dan semua direktori berbasis pohon lainnya, seperti Direktori Aktif Microsoft) adalah bahwa administrator jaringan harus membuat pohon hierarki yang mewakili tata letak organisasi. Struktur hierarki ini sebenarnya menyerupai pohon terbalik, dengan akar di bagian atas dan pengguna serta sumber daya jaringan—daun—di bagian bawah. Pohon ini dapat sesuai dengan tata letak fisik organisasi. Misalnya, stasiun kerja 1 hingga 20 akan berada di lantai tiga gedung perkantoran, stasiun kerja 21 hingga 40 di lantai dua, dan stasiun kerja 41 hingga 60 di lantai pertama. Pohon hierarki yang lebih kuat dan fleksibel dapat dibuat berdasarkan tata letak logis. Misalnya, tata letak logis dapat menggambarkan organisasi dalam hal struktur departemennya: departemen teknik (yang dapat tersebar di lantai 1 hingga 3), departemen penjualan (yang dapat terletak di lantai 2, 6, dan 7), dan departemen pemasaran (yang mungkin secara fisik berlokasi di dua gedung berbeda). Membuat desain pohon yang baik dan tepat bukanlah tugas yang mudah; namun, empat langkah dasar berikut akan memberikan awal yang baik bagi administrator jaringan. Pertama, kumpulkan dokumen perusahaan yang sesuai sehingga Anda mengetahui tentang perangkat keras dan perangkat lunak yang tersedia, serta departemen dan divisi karyawan. Sebagai bagian dari langkah pertama ini, Anda harus memperoleh bagan organisasi.

Kedua, rancang bagian atas pohon sebelum Anda mendesain bagian bawah. Untuk mendesain bagian atas pohon, Anda memberi nama objek organisasi pada tingkat atas pohon (dalam kebanyakan kasus, nama perusahaan) lalu buat lapisan pertama unit organisasi, atau objek kontainer. Unit organisasi (OU) adalah objek yang selanjutnya terdiri dari objek tambahan (contohnya termasuk server, printer, pengguna, atau grup pengguna). Misalnya, divisi di perusahaan yang terdiri dari beberapa departemen akan dianggap sebagai unit organisasi. Departemen juga merupakan unit organisasi karena juga terdiri dari objek, seperti karyawan. Jika jaringan Anda sangat kecil, mungkin tidak diperlukan unit organisasi apa pun. Ketiga, Anda mendesain bagian bawah pohon, yang mencakup hierarki unit organisasi dan objek leaf yang tersisa. Objek leaf tidak terdiri dari objek apa pun dan biasanya berupa entitas seperti pengguna, periferal, server, printer, antrean, dan sumber daya jaringan lainnya.

Langkah keempat dan terakhir dalam membuat pohon adalah mendesain hak akses keamanan—menentukan siapa yang memiliki hak atas objek yang sesuai. Misalnya, jika Anda membuat pengguna baru dan menempatkan pengguna tersebut di lokasi tertentu di pohon,

hak apa yang akan dimiliki pengguna tersebut? Printer dan direktori apa yang dapat diakses pengguna tersebut?

Di seluruh proses pembuatan pohon, penting untuk meninjau rancangan rancangan Anda untuk akurasi, fleksibilitas, dan kelengkapan. Karena pohon NDS akan digunakan oleh setiap server di jaringan dan mungkin akan ada selama beberapa tahun, pembuatan pohon yang dirancang dengan baik sangatlah penting. Pohon yang dirancang dengan tidak tepat akan menimbulkan kesulitan di masa mendatang saat Anda mencoba menambahkan pengguna, grup pengguna, dan sumber daya baru ke jaringan. Pohon yang dirancang buruk juga dapat menciptakan sistem yang lambat dengan waktu respons yang buruk.



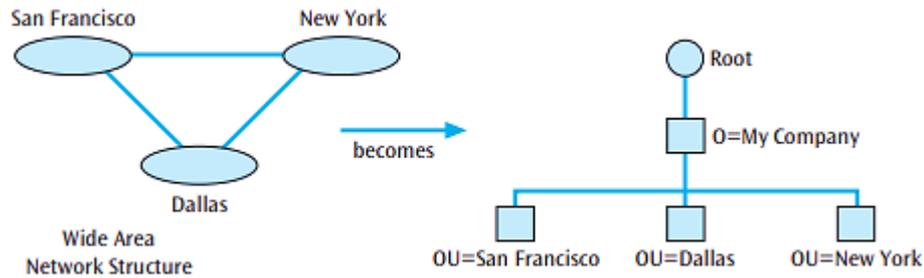
Gambar 8-5 Desain yang mungkin untuk pohon sistem operasi jaringan

Gambar 8-5 menunjukkan contoh desain pohon yang sesuai. Perhatikan bahwa desain pohon idealnya mirip dengan piramida. Objek kontainer harus lebih sedikit di bagian atas pohon daripada di bagian bawah. Pohon yang lebar dan datar biasanya bukan desain yang baik, karena tata letak ini menyebabkan terlalu banyak komunikasi di dalam kontainer, dan pengguna mungkin kesulitan menemukan sumber daya yang sesuai. Demikian pula, pohon yang terlalu sempit dan tinggi mungkin juga dirancang dengan buruk karena terlalu sedikit kontainer yang disertakan, yang dapat menyebabkan masalah di masa mendatang saat administrator jaringan ingin menambahkan pengguna atau sumber daya baru.

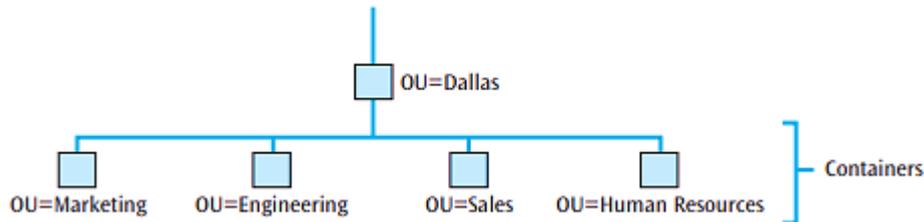
Saran Tambahan untuk Mendesain Pohon Jaringan

Saat merancang struktur direktori pohon seperti Direktori Aktif Microsoft atau NDS NetWare, beberapa perancang jaringan merasa bahwa bagian atas pohon harus didasarkan pada struktur jaringan area luas perusahaan. Misalnya, jika sebuah perusahaan memiliki kantor di San Francisco, Dallas, dan New York, maka tiga OU teratas harus berupa kontainer yang mewakili ketiga kota tersebut (lihat Gambar 8-6). Atau, jika perusahaan tersebut lebih

kecil dan berlokasi hanya di satu kota tetapi menempati beberapa gedung, setiap gedung harus menjadi satu objek kontainer. Namun, jika perusahaan tersebut lebih kecil lagi dan hanya menempati satu gedung, maka tidak perlu menentukan pohon berdasarkan jaringan area luas perusahaan. Sebaliknya, Anda dapat merancang bagian atas pohon berdasarkan desain divisi/departemen/kelompok kerja.



Gambar 8-6 Desain tingkat atas berdasarkan struktur jaringan area luas perusahaan



Gambar 8-7 Wadah pohon tingkat bawah di bawah wadah Dallas tingkat atas

Jika Anda mendesain lapisan atas pohon menggunakan struktur jaringan area luas perusahaan, Anda kemudian akan mendesain bagian pohon berikutnya sesuai dengan struktur jaringan area lokal perusahaan di setiap lokasi jaringan area luas. Desainer sering kali merujuk pada bagan organisasi perusahaan dan peta LAN untuk membuat bagian pohon yang lebih rendah ini. Misalnya, objek kontainer Dallas dari Gambar 8-6 diperluas untuk menyertakan Pemasaran, Teknik, Penjualan, dan Sumber Daya Manusia (lihat Gambar 8-7).

Versi NetWare berikutnya (5, 6, dan 6.5) menambahkan fungsi administratif tambahan termasuk kemampuan untuk mencetak di mana saja dan fitur hebat untuk menjalankan NetWare dari mesin mana pun dengan mengunduh perangkat lunak klien dari Internet. Akhirnya, NetWare berubah menjadi produk yang disebut Open Enterprise Server (OES) pada tahun 2003. OES pada dasarnya adalah sekumpulan aplikasi yang lebih populer dari NetWare: struktur NDS, yang sekarang disebut eDirectory, perangkat lunak cetak populernya yang disebut iPrint, dan sekumpulan layanan sistem operasi inti yang disebut NetWare Core Protocol. OES ditawarkan pada platform Linux dan NetWare. Meskipun perusahaan tersebut berpikir untuk menghentikan platform NetWare, pengguna NetWare yang berdedikasi terus meminta perusahaan untuk mempertahankan status quo.

Meskipun menjadi pelopor dalam desain sistem operasi jaringan, NetWare, dalam beberapa tahun terakhir, telah menghilang dari pasar sistem operasi jaringan. Sebagai gantinya, ada sejumlah sistem operasi jaringan lainnya, salah satunya adalah milik Microsoft.

Microsoft Windows NT dan Windows Server 2000, 2003, dan 2008

Untuk bersaing di pasar sistem operasi jaringan area lokal, Microsoft mengumumkan sistem operasi baru pada pertemuan Comdex Oktober 1991. Nama sistem operasi baru itu adalah Windows NT Versi 3. Microsoft telah mengerjakan sistem operasi ini selama sekitar tiga tahun, dan produk baru itu, meskipun memiliki nama yang mirip dengan sistem operasi desktop Windows, merupakan perubahan yang signifikan. Sejak diperkenalkan, Windows NT telah melalui sejumlah versi dan secara efektif telah menggantikan sistem operasi NetWare milik Novell.

Seperti NetWare, Windows NT dan inkarnasinya selanjutnya, Windows Server 2000/2003/2008 (selanjutnya disebut Windows Server), adalah sistem operasi jaringan yang dirancang untuk berjalan melalui jaringan stasiun kerja mikrokomputer dan menyediakan berbagi berkas dan berbagi periferal. Seperti versi NetWare terbaru, Windows Server dirancang untuk menawarkan alat administratif yang diperlukan untuk mendukung banyak pengguna, banyak server, dan berbagai perangkat periferal jaringan. Selain itu, Windows Server mendukung banyak aplikasi yang memungkinkan pengguna untuk membuat, mengakses, dan menampilkan halaman Web, serta perangkat lunak yang memungkinkan server bertindak sebagai server Web. Salah satu fitur yang membedakan sistem operasi Microsoft dari NetWare adalah bahwa sistem operasi Windows bekerja dengan lancar dengan alat aplikasi Microsoft yang sangat populer.

Windows NT Versi 4

Pertama kali dirilis pada bulan Agustus 1996, Windows NT Versi 4 memuat sejumlah fitur penting yang dengan cepat menjadikan Windows NT sebagai pesaing serius di pasar sistem operasi jaringan. Salah satu fitur NT Versi 4 yang paling mencolok adalah pilihan antarmuka pengguna. Tepatnya, antarmuka pengguna sistem operasi Microsoft Windows 95 untuk komputer pribadi pengguna tunggal dimasukkan ke dalam Windows NT, sehingga antarmuka server lebih mudah digunakan dan konsisten dengan produk Microsoft lainnya.

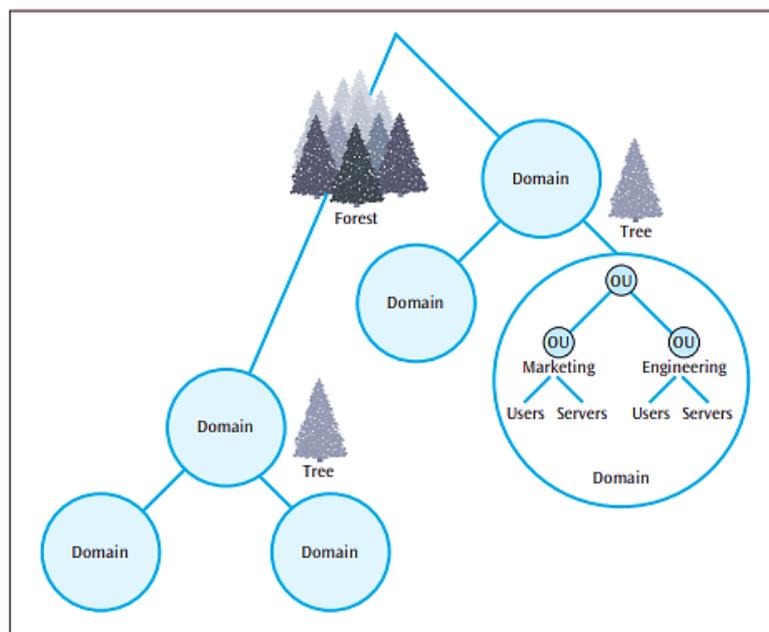
Satu perbedaan mencolok antara Windows NT Versi 4 dan NetWare adalah struktur direktori NT. Sementara NetWare menggunakan objek kontainer dan objek leaf secara ekstensif, NT hanya memiliki domain. Domain NT adalah objek kontainer yang memuat pengguna, server, printer, dan sumber daya jaringan lainnya. Tidak ada cara untuk membawa pengguna dalam satu domain dan membuat serangkaian subdomain atau subkontainer. Jaringan dengan beberapa domain dapat dibuat, tetapi domain-domain ini tidak hierarkis, dan dalam banyak kasus, domain-domain ini meningkatkan tingkat administrasi. Selain model domain yang relatif tidak fleksibel, ketidakstabilan sistem operasi merupakan area lain yang menurut banyak profesional jaringan merupakan kelemahan Windows NT Versi 4. Ketidakstabilan ini sebagian disebabkan oleh banyaknya bug dalam perangkat lunak NT Versi 4. Namun, banyak dari bug ini merupakan jenis yang umum dalam perangkat lunak baru, dan sejujurnya, versi awal NetWare tidak stabil seperti NetWare Versi 3. Karena tersedia dalam jangka waktu yang lebih lama, NetWare memiliki lebih banyak peluang untuk mengatasi masalah. Mengingat masalah ini, Microsoft bekerja keras untuk menghilangkan sebagian

besar masalah ketidakstabilan sistemnya, serta masalah lain yang melekat pada perangkat lunak yang begitu besar.

Windows Server 2000

Windows Server 2000, yang dirilis pada tahun 2000, merupakan generasi berikutnya dari sistem operasi Windows NT dan merupakan peningkatan yang signifikan dibandingkan versi NT sebelumnya. Windows Server 2000 menggabungkan jawaban Microsoft untuk sistem direktori NetWare NDS yang sangat populer: Direktori Aktif. Direktori Aktif menyimpan informasi tentang semua objek dan sumber daya dalam jaringan dan menyediakan informasi ini bagi pengguna, administrator jaringan, dan program aplikasi. Seperti NDS NetWare, Direktori Aktif membuat struktur hierarki sumber daya. Microsoft merasa bahwa yang terbaik adalah membuat layanan direktori berdasarkan standar yang ada daripada membuat layanan direktori milik sendiri yang baru. Jadi, Anda mungkin mendengar spesialis jaringan berbicara tentang bagaimana Direktori Aktif dibangun di sekitar Sistem Nama Domain (DNS) Internet, yang diperkenalkan di Bab Sepuluh, dan standar kedua: Protokol Akses Direktori Ringan (LDAP).

Untuk membangun hierarki Direktori Aktif, Anda membuat desain pohon yang mirip dengan desain pohon NDS. Objek, seperti pengguna, grup pengguna, komputer, aplikasi, dan perangkat jaringan, adalah item daun di dalam pohon. Item daun dikelompokkan dalam unit organisasi yang mirip dengan objek kontainer di NDS NetWare. Satu atau beberapa unit organisasi dapat dikelompokkan bersama menjadi domain.



Gambar 8-8 Contoh desain pohon Direktori Aktif Windows

Seperti di Windows NT, objek utama di Windows Server 2000 adalah domain. Tidak seperti domain NT, domain Windows Server 2000 dapat disusun secara hierarkis sebagai pohon, dan kumpulan pohon tersebut kemudian menjadi hutan. Misalnya, dua departemen dalam suatu organisasi mungkin adalah pemasaran dan teknik (Gambar 8-8). Kedua

departemen ini adalah objek organisasi. Dalam pemasaran dan teknik terdapat pengguna dan server jaringan. Pengelompokan objek dalam pohon direktori memungkinkan administrator untuk mengelola objek dan sumber daya pada tingkat makro, bukan satu per satu. Dengan beberapa klik mouse, administrator jaringan dapat mengizinkan semua pengguna dalam teknik untuk mengakses aplikasi perangkat lunak terkait teknik baru.

Banyak administrator jaringan Windows NT yang senang dengan kemajuan Windows Server 2000, dan dengan demikian memindahkan sistem mereka ke sistem operasi yang lebih baru. Sejumlah administrator NetWare juga pindah ke Windows Server 2000 karena sekarang sudah menyertakan struktur direktori berbasis pohon.

Windows Server 2003

Versi berikutnya dari sistem operasi jaringan Windows adalah Windows Server 2003. Meskipun bukan merupakan reorganisasi besar dari sistem operasi tersebut—seperti Windows Server 2000, jika dibandingkan dengan Windows NT—Windows Server 2003 menawarkan banyak fitur baru yang menurut administrator jaringan bermanfaat. Beberapa fitur tersebut adalah:

- Pembaruan pada Direktori Aktif, termasuk alat manajemen baru yang menyatukan semua tugas yang terkait dengan kebijakan grup
- Kemampuan untuk menghubungkan (mengelompokkan) hingga delapan server Windows 2003 untuk dukungan pengguna dan aplikasi yang lebih baik
- Layanan dukungan berkas dan cetak yang baru dan lebih baik, termasuk keandalan yang lebih tinggi, jangkauan printer yang lebih luas, dan berbagi dokumen jarak jauh
- Dukungan untuk Protokol Internet versi 6 (IPv6)
- Fitur keamanan yang lebih baik untuk berkas, jaringan, server, sistem operasi, dan transaksi berbasis Web

Windows Server 2003 juga akan menjadi sistem operasi inti untuk produk Microsoft generasi mendatang. Jadi, jika sebuah perusahaan memutuskan untuk menginstal Windows Server 2003, perusahaan tersebut akan dapat menggabungkan versi produk Microsoft mendatang (seperti rangkaian aplikasi Office, server berbasis Web, dan sistem komunikasi real-time, untuk menyebutkan beberapa di antaranya) dengan lebih mudah.

Windows Server 2008

Penambahan terbaru pada keluarga Windows Server adalah Windows Server 2008. Meskipun mempertahankan banyak fitur dan karakteristik yang sama dengan server 2003, Windows Server 2008 memiliki sejumlah fitur baru. Beberapa fitur ini mencakup Direktori Aktif yang diperluas (yang mencakup layanan manajemen sertifikat, identitas, dan hak), inti server baru (yang memungkinkan Windows Server 2008 bertindak sebagai sejumlah jenis server yang berbeda, termasuk server virtual Windows), server berkas pemulihan otomatis yang dapat memperbaiki berkas dan/atau folder yang rusak, peningkatan kecepatan pemrosesan, dan kemajuan dalam keamanan jaringan. Jelas, Microsoft tetap kompetitif di pasar sistem operasi jaringan dan kemungkinan besar akan terus menawarkan produk yang menarik bagi administrator jaringan.

UNIX

UNIX adalah sistem operasi populer yang dapat ditemukan pada workstation pengguna tunggal serta pada komputer mainframe dan server. Hal ini paling sering ditemukan dengan antarmuka berbasis teks, meskipun antarmuka pengguna grafis juga tersedia. UNIX awalnya dirancang di Bell Labs dan pertama kali diimplementasikan pada komputer mini PDP-7 pada tahun 1970. Ini adalah sistem yang relatif efisien, yang menjelaskan mengapa ia beroperasi dengan cepat. Tak lama setelah diperkenalkan, perangkat lunak UNIX ditulis ulang dalam bahasa pemrograman C yang populer. Karena karakteristik bahasa pemrograman C dan desain UNIX, kode internal UNIX relatif mudah untuk dimodifikasi. Karena alasan ini, dan karena versi awal sistem operasi diberikan secara gratis, UNIX menjadi sangat populer di institusi akademis. Salah satu varian sistem UNIX yang lebih populer adalah versi BSD yang awalnya dirilis dari University of California, Berkeley.

Karena UNIX adalah salah satu sistem operasi yang lebih tua dan telah berkembang dalam kekuatan pemrosesan selama bertahun-tahun, maka UNIX cukup stabil. Konsekuensi lain dari usianya adalah UNIX berjalan pada variasi perangkat keras terluas dibandingkan sistem operasi jaringan mana pun. Ia menangani operasi jaringan dengan baik, dan berbagai aplikasi telah ditulis untuk dijalankan di UNIX. Saat ini, banyak ahli menganggap UNIX sebagai salah satu sistem operasi terbaik untuk mendukung aplikasi besar seperti sistem database multipengguna dan server berbasis Web.

Sebagai sistem operasi jaringan, UNIX memiliki banyak kelebihan dan mendukung seluruh fitur sistem operasi jaringan yang dirangkum dalam Tabel 8-1. Selain itu, UNIX memiliki sistem keamanan yang stabil yang juga didasarkan pada pengalaman bertahun-tahun. Banyak aplikasi telah dibuat selama bertahun-tahun untuk UNIX yang mendukung fungsi klien/server serta pengembangan halaman Web dan operasi server Web. Karena mempunyai pengikut setia yang akan memastikan evolusinya dalam menghadapi persaingan dari pendatang baru, UNIX mungkin akan tersedia selama bertahun-tahun.

Linux

Sejak awal, UNIX telah berkembang menjadi banyak versi dan dijalankan pada sejumlah platform komputer. Salah satu versi yang menarik banyak minat pada tahun 1990an adalah Linux. Linux, meskipun didasarkan pada konsep UNIX, merupakan penulisan ulang lengkap dari kernel UNIX dan meminjam fungsi tambahan dari kernel UNIX yang sudah ada.

Perangkat GNU dari Free Software Foundation dan dari komunitas perangkat lunak bebas yang lebih besar. Menariknya, beberapa sistem komputer terbesar dan tercepat di dunia dijalankan di Linux. Linux mempunyai banyak kelebihan dan kekurangan yang sama dengan UNIX, dan mempunyai kinerja yang mirip dengan UNIX sebagai sistem operasi jaringan. Namun, sejumlah fitur membedakan Linux dari UNIX dan juga dari semua sistem operasi jaringan lainnya. Yang pertama dan terpenting adalah biaya Linux: Jika diunduh dari Internet, perangkat lunak ini dan selalu gratis.

Namun saat ini, banyak perusahaan memilih untuk membeli Linux dari vendor yang mengkhususkan diri dalam menyediakan versi terbaru Linux beserta semua aplikasi dan utilitas pendukungnya, seperti alat pendukung halaman Web, antarmuka pengguna grafis, dan

versi terbaru dari Linux. driver perifer. Bahkan ketika Linux dibeli dari vendor, biayanya tidak signifikan dibandingkan dengan biaya pembelian UNIX atau Windows Server 2008. Sedangkan UNIX dan Windows Server 2008 bisa berharga ribuan hingga puluhan ribu dolar, tergantung pada jumlah pengguna. workstation, versi komersial Linux harganya hanya beberapa ratus dolar.

Keuntungan kedua Linux dibandingkan sistem operasi jaringan lainnya adalah ketika Anda membeli atau mengunduh Linux, Anda dapat menerima kode sumber asli beserta kode yang dikompilasi secara gratis. Memiliki kode sumber asli memberi organisasi kendali yang besar terhadap perangkat lunak. Di tangan seorang pemrogram berpengalaman, kode sumber Linux dapat dimodifikasi dengan cara yang hampir tak terbatas untuk menyediakan sistem operasi yang disesuaikan. Namun, kemampuan untuk menyesuaikan perangkat lunak adalah pedang bermata dua. Di tangan yang tidak berpengalaman, kode sumber yang disesuaikan dapat menjadi sumber masalah yang terus-menerus.

Keuntungan terakhir Linux adalah ukuran kodenya. Sejak debutnya, Linux telah mampu beroperasi pada sistem sekecil prosesor Intel 386 dengan memori utama hanya sebesar 4 MB. Meskipun Linux pasti akan berjalan pada sistem yang lebih besar, banyak administrator menggunakan sistem Linux pada komputer pribadi lama untuk mendukung fungsi jaringan yang lebih sederhana seperti memberikan keamanan jaringan (firewall). Sistem ini tampaknya dapat berjalan tanpa pengawasan dengan sedikit atau tanpa dukungan. Linux bahkan berjalan pada perangkat sekecil ponsel.

Linux memiliki banyak keunggulan lain yang sama dengan UNIX, seperti eksekusi yang cepat (karena ukurannya yang relatif kecil dan kode yang efisien), fungsi dukungan jaringan, dan opsi yang memberikan perangkat lunak nuansa produk dengan antarmuka pengguna grafis.

Meskipun para pendukung sistem operasi jaringan lain di masa lalu mengklaim bahwa Linux belum siap untuk "prime time", hal ini jelas tidak lagi terjadi. Mungkin aman untuk mengatakan bahwa sebagian besar perusahaan menjalankan Linux pada setidaknya satu server untuk mendukung aplikasi tertentu. Saat ini, perangkat lunak Linux umumnya digunakan untuk mendukung server email, server Web, server FTP, server file/cetak, firewall, server proxy, dan server DNS. Mengenai antarmuka, sistem operasi Linux dapat mendukung USB, SCSI, RAID, dan berbagai bentuk antarmuka video; mereka juga mampu beroperasi dalam mode plug-and-play (di mana driver perangkat dimuat secara otomatis saat perangkat terpasang).

Keunggulan kompetitif lain yang dimiliki Linux dibandingkan sistem operasi jaringan lainnya adalah bahwa Linux merupakan bagian dari rangkaian perangkat lunak sumber terbuka yang semakin berkembang dan sangat dihargai dalam industri bisnis dan pendidikan. Linux dapat digabungkan dengan aplikasi perangkat lunak populer seperti server Web Apache, server database MySQL, AXIS, JBoss, Jetty, Saxon, dan Tomcat untuk menciptakan sistem jaringan yang relatif lengkap yang dapat melayani kebutuhan berbagai jenis bisnis. . Sebagian besar distribusi Linux juga dilengkapi dengan Samba, paket perangkat lunak layanan file dan

pencetakan. Linux jelas merupakan pemain utama dalam arena sistem operasi jaringan dan tidak boleh diabaikan.

Server Mac OS X

Pada saat produk Microsoft mendominasi pasar sistem bisnis, Apple Inc. terus menciptakan ruang unik untuk dirinya sendiri di pasar pendidikan K–12. Untuk mendukung jajaran komputer Macintosh (dan juga komputer non-Macintosh), Apple telah menciptakan Mac OS X Server (yang pada dasarnya merupakan versi kesepuluh). Server ini mampu mendukung kelompok kerja Macintosh dan Windows, dan didasarkan pada perangkat lunak yang dibuat oleh komunitas sumber terbuka. Dengan kata lain, Server Mac OS X didasarkan pada konsep UNIX, dan dengan demikian memiliki beberapa karakteristik yang sama dengan sistem operasi UNIX dan Linux, seperti kode yang cepat, efisien, dan stabil. Sistem operasi ini juga menggabungkan sejumlah aplikasi perangkat lunak sumber terbuka yang terkenal, seperti server Web Apache, keamanan Kerberos, SpamAssassin, layanan direktori OpenLDAP, serta file Samba dan server cetak.

Karena banyak orang dulu dan terus percaya bahwa produk Apple hanya dapat berinteraksi dengan produk Apple lainnya, para perancang Mac OS X Server telah berusaha keras untuk memastikan sistem operasi jaringan mereka kompatibel dengan berbagai macam perangkat. . Misalnya, perangkat lunak berbagi file dan printer Mac OS X menyediakan akses aman ke stasiun kerja klien Macintosh, Windows, dan Linux. Selain itu, perangkat lunak layanan direktori, yang disebut Open Directory, dapat berinteraksi dengan Direktori Aktif Microsoft. Terlepas dari upaya-upaya ini, Mac OS X Server memiliki perjuangan yang panjang jika ingin mengejar ketertinggalan dari keluarga Microsoft Windows Server yang sudah mengakar serta UNIX dan Linux.

8.6 SERVER

Sistem operasi jaringan memerlukan mesin host untuk beroperasi. Meskipun bagian dari sistem operasi jaringan berada di setiap komputer klien, sebagian besar sistem operasi beroperasi di server jaringan, atau sederhananya, server. Lebih tepatnya, server adalah komputer yang menyimpan sumber daya perangkat lunak seperti sistem operasi jaringan, aplikasi komputer, program, kumpulan data, dan database, dan melakukan satu atau lebih layanan tipe jaringan untuk klien yang terhubung. Ada banyak jenis server yang berbeda. Seperti yang baru saja disebutkan, server yang mendukung sistem operasi jaringan disebut server jaringan. Ada juga server file untuk menyimpan file, server email, server cetak untuk penyimpanan sementara pekerjaan pencetakan, server database, server Web (untuk menyimpan halaman Web), server FTP untuk mendukung situs FTP (File Transfer Protocol), dan Server DNS untuk mengonversi URL menjadi alamat IP. Daftarnya terus bertambah. Mari kita periksa berbagai bentuk server, beserta beberapa fitur perangkat keras dan perangkat lunak yang digunakannya.

Ukuran server berkisar dari mikrokomputer kecil hingga komputer mainframe. Biasanya, server adalah stasiun kerja komputer mikro yang kuat yang menjalankan sistem operasi seperti Linux atau UNIX dengan komponen redundan. Redundan adalah kata kuncinya

di sini: Server memiliki disk drive yang berlebihan, pasokan daya yang berlebihan, dan bahkan kipas pendingin yang berlebihan. Stasiun kerja server biasanya menampung gigabyte memori akses acak, satu atau lebih hard disk drive penyimpanan besar (setiap drive menyediakan penyimpanan ratusan hingga ribuan gigabyte), dan setidaknya satu mikroprosesor berkecepatan tinggi. Hard disk drive biasanya bersifat hot swappable dan memiliki antarmuka berkecepatan tinggi, seperti Small Computer System Interface (SCSI). Seperti yang mungkin Anda ingat sebelumnya, perangkat yang dapat ditukar dalam kondisi panas (hot swappable) dapat dilepas dari komputer saat daya masih menyala, sehingga memudahkan pemeliharaan dan perbaikan. Selain disk drive, catu daya dan kipas pendingin di sebagian besar server modern juga dapat ditukar secara hot swap.

Untuk melindungi server dari kegagalan disk yang parah, disk drive di sebagian besar server mendukung salah satu teknik Redundant Array of Independent Disks. Redundant Array of Independent Disks (RAID) adalah kumpulan teknik untuk menghubungkan beberapa hard disk drive ke komputer. Dengan pengecualian teknik RAID pertama, RAID-0, RAID digunakan terutama untuk menyimpan data secara berlebihan pada beberapa hard disk drive. Beberapa teknik RAID yang lebih umum meliputi:

- RAID-0, di mana data dipecah menjadi beberapa bagian, dan masing-masing bagian disimpan pada disk drive yang berbeda. Teknik ini dikenal dengan sebutan striping. Tidak ada redundansi data dalam teknik ini; jadi jika salah satu disk drive gagal, beberapa data akan hilang. Namun, keuntungan dari teknik ini adalah kecepatan membaca atau menulis data di beberapa disk secara bersamaan.
- RAID-1, dimana data disimpan pada setidaknya dua disk drive, dalam rangkap dua, untuk memberikan tingkat redundansi (atau toleransi kesalahan), jika satu disk rusak. Teknik ini juga dikenal sebagai pencerminan disk.
- RAID-3, dimana data disimpan secara berlebihan di beberapa disk drive (striping), dan informasi pengecekan kesalahan mengenai data yang disimpan disimpan di disk terpisah. Informasi pengecekan kesalahan ini dapat digunakan untuk mendeteksi kesalahan dan mungkin merekonstruksi data jika sebagian data rusak.
- RAID-5, di mana data dipecah menjadi beberapa bagian (garis) dan disimpan di tiga disk atau lebih. Informasi paritas (kode pengecekan kesalahan) disimpan bersama dengan data bergaris, bukan pada disk terpisah. RAID-5 adalah teknik RAID yang paling populer.

Ada beberapa teknik RAID lainnya, namun pada dasarnya teknik tersebut merupakan variasi dari empat teknik di atas.

Seiring dengan teknik RAID, sebagian besar server juga dilengkapi seperangkat perangkat lunak manajemen yang kuat. Perangkat lunak ini memungkinkan administrator jaringan untuk memantau status server, menyebarkan aplikasi jaringan dari jarak jauh, memperbarui driver yang diperlukan, menginstal dan menyempurnakan sistem operasi jaringan, dan mengkonfigurasi sistem penyimpanan RAID.

Sehubungan dengan sisi perangkat keras server, banyak server berdaya tinggi mendukung banyak prosesor dan/atau prosesor multi-inti. Karena prosesor adalah mesin penggerak di dalam komputer, server atau stasiun kerja dengan banyak prosesor atau banyak

inti dapat secara bersamaan menjalankan beberapa permintaan dari stasiun kerja lain. Sebuah server yang menawarkan multiprosesor simetris dapat mendistribusikan permintaan yang diterima secara merata ke beberapa prosesor, sehingga secara efektif memanfaatkan potensi penuh dari sistem multiprosesor.

Kemajuan teknologi terkini untuk server adalah virtualisasi server. Dengan virtualisasi server, dimungkinkan untuk membuat satu komputer (atau server) bertindak seolah-olah itu adalah beberapa komputer (atau server). Keuntungannya adalah setiap server mengira itu adalah satu-satunya server yang berjalan di komputer tersebut. Ia memiliki akses ke semua sumber daya yang diperlukan, dan kesulitan apa pun yang dialami perangkat lunak tidak akan mempengaruhi server virtual lain yang berjalan pada mesin itu. Kerugian dari virtualisasi server mencakup kompleksitas perangkat lunak tambahan dan tingkat tambahan manajemen manusia.

Anggota lain dari keluarga server (yang mengalami penurunan popularitas karena virtualisasi server) adalah peralatan server. Peralatan server adalah unit atau kotak tunggal yang mendukung banyak fungsi jaringan seperti berbagi Internet, layanan Web intranet, keamanan firewall, layanan FTP, layanan file dan cetak, layanan email, dan konfigurasi jaringan pribadi virtual. Perusahaan kecil dengan hingga 50 pengguna mungkin menganggap server jenis ini sebagai alat yang sempurna. Karena begitu banyak fungsi yang ditempatkan dalam satu unit, masing-masing komponen tidak dirancang untuk penggunaan berat, seperti yang mungkin terjadi di perusahaan dengan lebih dari 50 pengguna. Selain itu, Anda harus menyadari bahwa sejumlah perangkat dengan nama serupa biasanya dirancang untuk aplikasi tunggal. Misalnya, peralatan server cache dirancang untuk menyediakan layanan mirror atau cadangan untuk server lain. Peralatan server Web dirancang terutama untuk berfungsi sebagai server Web. Peralatan server penyimpanan dirancang hanya untuk menyediakan penyimpanan disk untuk jaringan.

Jenis server lain yang muncul pada pergantian abad adalah server blade. Blade server adalah server yang tidak memiliki kabinet atau kotak, namun berada pada satu kartu sirkuit tercetak. Perusahaan yang ingin memasang banyak server di lokasi yang relatif kecil dapat memasang beberapa bilah server dalam satu bingkai kartu. Meskipun bilah server individual mungkin tidak sekuat server yang berdiri sendiri, bilah tersebut cukup kompak; dan jika digabungkan menjadi puluhan atau ratusan unit, mereka dapat menghasilkan server yang sangat kuat. Selain itu, jika satu server blade gagal, mencabut server blade dan menggantinya dengan unit kerja cukup sederhana.

Sejumlah perangkat pendukung lain-lain dikaitkan dengan server. Server jaringan memerlukan setidaknya satu koneksi ke jaringan dalam bentuk kartu antarmuka jaringan. Untuk menjaga isi disk drive, sistem tape backup biasanya digunakan untuk membuat cadangan isi hard disk secara teratur dan otomatis. Selain itu, beberapa bentuk sistem cadangan baterai (catu daya tak terputus) digunakan untuk menjaga daya ke komputer selama beberapa periode waktu jika daya listrik hilang. Semua perangkat pendukung ini akan diperiksa secara lebih rinci nanti di bab ini.

Jaringan klien/server vs. jaringan peer-to-peer

Kebanyakan jaringan area lokal terdiri dari stasiun kerja pengguna yang berkomunikasi dan bergantung pada satu atau lebih server. Jenis LAN ini disebut jaringan klien/server. Klien, atau stasiun kerja pengguna, meminta sesuatu seperti catatan database dari server. Server menerima permintaan, mengambil data, dan mengembalikan respons. Meskipun mayoritas LAN adalah klien/server, bentuk lain dari LAN semakin populer: jaringan area lokal peer-to-peer. Jaringan peer-to-peer mungkin tidak memiliki server apa pun tetapi memungkinkan komunikasi antar workstation, seolah-olah semua workstation itu setara. Namun sering kali, jaringan peer-to-peer memiliki server, meskipun server mungkin berfungsi dalam peran yang berbeda dari server di jaringan klien/server.

Ketika jaringan peer-to-peer pertama kali muncul sekitar 30 tahun yang lalu, jaringan tersebut merupakan jaringan tanpa server. Semua stasiun kerja berkomunikasi satu sama lain. Karena tidak ada server khusus, setiap stasiun kerja pada dasarnya bertindak sebagai server. Jenis pengaturan peer-to-peer ini hanya dapat mendukung jaringan dengan beberapa workstation saja. Ditambah lagi, tanpa keamanan sistem file bersama, bisnis tidak akan mempercayai pendekatan peer-to-peer. Dengan demikian, bentuk jaringan ini praktis menghilang. Jaringan peer-to-peer saat ini mencoba menghilangkan kelemahan lama ini. Daripada mendefinisikan jenis arsitektur atau topologi tertentu, mereka berfokus pada aplikasi dan penggunaannya.

Jenis aplikasi yang beroperasi pada jaringan peer-to-peer modern mencakup alat kolaborasi, produk manajemen konten, berbagi file terdistribusi, dan pemrosesan terdistribusi (di mana waktu siklus yang tidak terpakai “dipinjam” dari pemroses rekan). Untuk memahami cara kerja jaringan peer-to-peer, pertimbangkan, misalnya, sebuah perusahaan dengan banyak kantor di seluruh negara atau dunia.

Setiap kantor memiliki koleksi file atau database yang unik. Perusahaan ingin memberikan karyawan di kantor mana pun akses ke kumpulan file apa pun. Daripada membuat satu repositori pusat untuk informasi di semua kantor (seperti yang berlaku untuk pengaturan klien/server), perusahaan dapat mengembangkan jaringan peer-to-peer dan memberikan setiap kantor akses ke sistem file semua kantor lainnya. Perhatikan bahwa dalam skenario ini, setiap kantor masih memelihara file atau server databasenya sendiri. Salah satu contoh aplikasi peer-to-peer yang paling terkenal adalah Napster asli, di mana pengguna dapat mengunduh musik dari pengguna Napster lain di Web.

Namun jaringan peer-to-peer masih menghadapi beberapa kendala. Keamanan, seperti disebutkan sebelumnya, mungkin merupakan salah satu tantangan terbesar. Hambatan lainnya mencakup kinerja, manajemen, interoperabilitas, dan kurangnya standarisasi. Tanpa pengembangan seperangkat standar yang diterima untuk mendukung sistem peer-to-peer, akan sangat sulit bagi perusahaan untuk menggabungkan aplikasi perangkat lunak dari beberapa vendor.

Sekarang kita telah membahas berbagai sistem operasi jaringan dan server yang menjalankan sistem tersebut, mari kita alihkan perhatian kita ke banyak perangkat lunak

jaringan lainnya yang mendukung jaringan area lokal. Secara khusus, kami akan memeriksa utilitas perangkat lunak dan perangkat lunak untuk mengakses Internet.

8.7 PERANGKAT LUNAK DUKUNGAN JARINGAN

Meskipun sistem operasi jaringan jelas merupakan perangkat lunak terpenting pada jaringan area lokal, sistem operasi tidak dapat bekerja sendiri. Dua jenis perangkat lunak jaringan area lokal yang bekerja dengan dan mendukung sistem operasi jaringan adalah utilitas dan perangkat lunak Internet. Mari kita periksa keduanya secara bergantian.

Keperluan

Utilitas adalah program perangkat lunak yang beroperasi di latar belakang dan mendukung satu atau lebih fungsi untuk menjaga jaringan tetap berjalan pada kinerja optimal. Untuk mendukung jaringan area lokal dan sistem operasinya, tersedia beragam program utilitas. Terkadang program utilitas ini dibundel dengan sistem operasi, namun sering kali program tersebut terpisah dan harus dibeli satu per satu. Seperti halnya sistem operasi jaringan, penting ketika membeli perangkat lunak utilitas (serta produk perangkat lunak apa pun) untuk memperhatikan perjanjian lisensi. Banyak program utilitas dilisensikan untuk satu mesin. Jika 200 stasiun kerja berada di jaringan area lokal Anda, Anda mungkin harus membeli 200 lisensi sebelum penggunaan Anda sesuai dengan hukum yang berlaku.

Beberapa kelompok perangkat lunak utilitas jaringan yang lebih umum adalah:

- Perangkat lunak antivirus
- Perangkat lunak anti-spam
- Perangkat lunak anti-spyware
- Perangkat lunak cadangan
- Perangkat lunak perlindungan kerusakan
- Perangkat lunak pemantauan jaringan
- Perangkat lunak akses jarak jauh
- Perangkat lunak penilaian keamanan
- Hapus instalasi perangkat lunak

Perangkat lunak antivirus dirancang untuk mendeteksi dan menghapus virus yang telah menginfeksi memori komputer, disk, atau sistem operasi. Karena virus baru selalu muncul, maka penting untuk terus mengupdate software antivirus dengan versi terbaru. Sering kali, pemilik perangkat lunak antivirus yang dibeli dapat mengunduh pembaruan ini dari situs web perusahaan perangkat lunak tersebut tanpa biaya tambahan. Satu-satunya saat diperlukan untuk membeli perangkat lunak antivirus versi baru adalah ketika perangkat lunak tersebut telah mengalami revisi besar-besaran. Beberapa produsen antivirus menawarkan kesepakatan korporat yang membayar biaya tahunan tetap, dan perusahaan dapat menyebarkan dan memperbarui salinan perangkat lunak sebanyak yang diinginkan.

Spam, atau email massal komersial yang tidak diminta, telah menjadi gangguan besar bagi pengguna korporat maupun individu. Beberapa ahli memperkirakan bahwa puluhan miliar pesan spam dikirim setiap hari. Spam dalam jumlah besar ini menyia-nyiakan waktu para pekerja yang harus menghapus pesan-pesan ini, menghabiskan miliaran byte

penyimpanan di server email, dan membuat jaringan yang mentransfer data menjadi padat. Perangkat lunak anti-spam digunakan untuk memblokir email yang tidak diinginkan ini dan tersedia dalam berbagai tingkatan:

- Perangkat lunak desktop, yang memblokir spam di stasiun kerja atau komputer di rumah pengguna
- Perangkat lunak korporat, yang memblokir spam di server email korporat atau di tingkat penyedia layanan Internet
- Layanan yang memblokir spam bahkan sebelum spam tersebut sampai ke server perusahaan atau penyedia layanan Internet

Pengguna komputer bisnis dan rumahan telah menjadi korban jenis gangguan lain dari pihak luar yang tidak bermoral: spyware. Spyware adalah perangkat lunak yang tanpa disadari diunduh oleh pengguna dari Internet, dan ketika perangkat lunak ini dijalankan di mesin pengguna, perangkat lunak tersebut mulai memata-matai pengguna. Perangkat lunak spyware dapat berbentuk program kendali jarak jauh yang dioperasikan oleh peretas, atau dapat berupa program yang diluncurkan oleh pengecer dengan harapan dapat mengumpulkan kebiasaan belanja Anda untuk dirinya sendiri atau untuk dibagikan kepada pengecer lain. Dalam kasus terakhir, program tersebut mungkin hanya merupakan jenis alat riset pasar yang tidak berbahaya. Meski begitu, sebagian besar pengguna merasa bahwa spyware mengganggu dan harus diblokir atau dihilangkan. Perangkat lunak anti-spyware dapat menemukan dan membersihkan program spyware yang ditemukan di memori komputer dan drive hard disk. Pengguna komputer rumahan, serta administrator jaringan, harus menginstal perangkat lunak anti-spyware dan menjalankannya secara teratur atau memprogram sistem operasi untuk menjalankannya pada jadwal yang ditentukan waktunya. Namun Anda harus berhati-hati ketika mencari program spyware gratis di Internet karena banyak di antaranya (tetapi tidak semua) merupakan program spyware itu sendiri.

Perangkat lunak pencadangan memungkinkan administrator jaringan untuk membuat cadangan file data yang saat ini disimpan di hard disk drive server. Biasanya, pencadangan ini ditulis ke sistem tape, namun ada kemungkinan lain, seperti melakukan pencadangan ke situs jarak jauh melalui Internet. Sebagian besar sistem pencadangan dapat sepenuhnya diotomatisasi sehingga perangkat lunak dijalankan pada saat hanya sedikit, jika ada, pengguna yang menggunakan sistem— misalnya, pada dini hari. Beberapa perangkat lunak pencadangan juga mencakup kemampuan pemulihan jika terjadi kegagalan sistem.

Tujuan utama dari perangkat lunak perlindungan kerusakan adalah untuk melakukan penghentian kerusakan, atau mencoba untuk menjaga sistem operasi tetap berjalan cukup lama untuk keluar dengan lancar. Perangkat lunak perlindungan kerusakan juga dikenal sebagai perangkat lunak rollback. Untuk memanfaatkan utilitas ini, perusahaan harus menginstal perangkat lunak tersebut di stasiun kerja pengguna dan server jaringan. Saat aplikasi berjalan.

Ketika stasiun kerja pengguna akan mogok, aplikasi tersebut mengirimkan sinyal ke sistem operasi yang menyatakan bahwa ia mengalami masalah dan perlu dimatikan. Pelindung kerusakan mencegah pesan ini dan mencoba memperbaiki masalah sambil tetap menjaga

aplikasi tetap berjalan. Meskipun tingkat keparahan masalahnya tidak dapat diperbaiki lagi, pelindung kerusakan sering kali membuat jeda yang memungkinkan pengguna menyimpan data penting dan keluar dari program dengan aman. Karena pelindung kerusakan terus berjalan di latar belakang, hal ini menyebabkan penurunan kinerja. Saat ini, sebagian besar pelindung tabrakan menurunkan kinerja sistem secara keseluruhan antara 2 hingga 8 persen. Meskipun hilangnya 8 persen waktu pemrosesan mungkin tidak terlihat terlalu banyak, jika Anda adalah pengguna komputer yang serius (jenis komputer yang dirancang untuk perangkat lunak ini), Anda mungkin akan merasakan hilangnya kecepatan komputasi.

Perangkat lunak pemantauan jaringan menggabungkan sejumlah besar alat pendukung jaringan. Misalnya, ada perangkat lunak yang dapat memantau server dan melaporkan penggunaan CPU, aktivitas jaringan, dan permintaan server. Perangkat yang disebut sniffer dapat digunakan pada jaringan kabel dan jaringan nirkabel. Sniffer dapat “mendengarkan” lalu lintas di jaringan dan menentukan apakah pesan yang dikirimkan tidak valid, melaporkan masalah jaringan seperti NIC yang tidak berfungsi, dan mendeteksi masalah kemacetan lalu lintas. Sniffer nirkabel dapat melakukan operasi serupa dan juga dapat mendeteksi seberapa jauh jangkauan sinyal nirkabel. Jadi, jika Anda mengalami masalah komunikasi nirkabel, sniffer nirkabel dapat memberi tahu Anda jika sinyal terlalu lemah di lokasi tertentu. Sebaliknya, sniffer nirkabel juga dapat memberi tahu Anda jika sinyal nirkabel Anda terlalu jauh, seperti di luar gedung atau di jalan, di mana sinyal tersebut mungkin dieksploitasi oleh pengguna yang tidak berwenang.

Perangkat lunak akses jarak jauh memungkinkan pengguna untuk mengakses semua kemungkinan fungsi stasiun kerja komputer pribadi dari lokasi seluler atau jarak jauh. Dua pengguna perangkat lunak akses jarak jauh yang paling umum adalah pengguna nomaden, yang harus mengakses perangkat lunak dan data di komputer kerja mereka saat bepergian atau bekerja di rumah, dan personel pendukung, yang perlu memasuki sistem komputer pengguna untuk memecahkan masalah dan menyarankan atau melakukan perbaikan. Banyak jenis perangkat lunak akses jarak jauh juga membuat jaringan pribadi virtual (VPN) antara pengguna jarak jauh dan komputer kerja. Di Bab Sepuluh, Anda akan mempelajari bagaimana VPN menggunakan protokol terowongan dan perangkat lunak enkripsi untuk membuat koneksi aman antara komputer jarak jauh dan komputer kerja.

Perangkat lunak penilaian keamanan dirancang untuk memindai alamat IP atau rentang alamat IP untuk mencari segala jenis kelemahan keamanan. Kelemahan mungkin termasuk port yang terbuka, desain share dan trust yang tidak tepat, proses mencurigakan yang berjalan di latar belakang, dan kerentanan yang diketahui dalam sistem operasi yang belum diperbaiki. Anda akan mempelajari lebih lanjut tentang keamanan jaringan di Bab Dua Belas.

Aplikasi perangkat lunak terus bertambah dalam ukuran dan jumlah file pendukung yang diperlukan untuk menjalankan program. Jika seseorang memutuskan untuk menghapus suatu aplikasi, hampir tidak mungkin menemukan semua file yang terkait dengan aplikasi tersebut. Uninstall software bekerja dengan pengguna untuk mencari dan menghapus aplikasi yang tidak diinginkan lagi. Saat perangkat lunak uninstall menemukan setiap file terkait,

pengguna akan diminta untuk memutuskan apakah file tersebut harus dihapus. Karena beberapa file mungkin dibagikan oleh beberapa aplikasi, pengguna mungkin tidak ingin melakukan operasi penghapusan. Kebanyakan program uninstall menyimpan cadangan file yang dihapus untuk memperbaiki masalah jika terjadi kesalahan dan file yang salah dihapus. Program uninstall juga dapat menemukan file yatim piatu yang bukan lagi milik aplikasi apa pun dan meminta pengguna untuk menghapusnya. Terakhir, banyak program uninstall yang dapat menemukan file duplikat dan menghapus duplikatnya.

Fungsi kebalikan dari uninstall perangkat lunak pada dasarnya adalah distribusi perangkat lunak secara otomatis. Beberapa tahun yang lalu, jika administrator jaringan ingin memuat salinan program perangkat lunak ke setiap mesin di jaringan, administrator harus mengunjungi setiap mesin secara fisik dan menginstal perangkat lunak tersebut. Sekarang, terdapat perangkat lunak yang memungkinkan administrator jaringan untuk memuat perangkat lunak dari jarak jauh ke semua mesin di jaringan.

Perangkat Lunak Internet

Salah satu segmen penting dari pasar perangkat lunak adalah perangkat lunak Internet, perangkat untuk mendukung layanan terkait Internet. Layanan dan aplikasi ini mencakup browser Web, perangkat lunak server Web, dan perangkat lunak penerbitan halaman Web, serta aplikasi lainnya.

Browser memungkinkan pengguna mengunduh dan melihat halaman World Wide Web. Browser juga memungkinkan pengguna mengakses halaman intranet internal dan halaman ekstranet perusahaan. Sebagian besar pengguna akrab dengan Internet Explorer Microsoft. Pada musim panas 2011, Firefox unggul tipis atas pesaing terdekat berikutnya, Firefox. Chrome, Safari, browser seluler, dan Opera melengkapi fitur lainnya.

Sejumlah alat tersedia untuk mendukung browser, seperti pemeriksa ejaan, pemblokir pop-up, dan pengelola unduhan yang dapat menangani pengunduhan halaman Web dengan lancar dan efisien, berapa pun kecepatan koneksinya.

Perangkat lunak server web adalah aplikasi atau serangkaian program yang menyimpan halaman Web dan memungkinkan browser dari mana saja di dunia untuk mengakses halaman Web tersebut. Ketika pengguna yang menjalankan browser memasukkan atau mengklik alamat halaman Web (Uniform Resource Locator, atau URL), browser mengirimkan permintaan halaman ke server Web di alamat yang dikutip. Server Web menerima permintaan, mengambil halaman Web yang sesuai, dan mengirimkan halaman Web yang diminta kembali melalui Internet ke browser. Perangkat lunak server web mampu mendukung koneksi aman. Koneksi yang aman memungkinkan sistem untuk mentransfer data sensitif, seperti informasi kartu kredit, dengan keyakinan bahwa integritas data tidak akan dilanggar.

Ketika pengguna ingin membuat satu atau lebih halaman Web yang akan disimpan di server Web, perangkat lunak penerbitan halaman Web membantu mereka menyiapkan file yang diperlukan. Sebagian besar program penerbitan halaman web memungkinkan pengguna untuk memasukkan gambar statis, gambar animasi, berbagai bentuk skrip, dan kode berbasis Java ke dalam file HTML.

Sekarang kita sudah familiar dengan berbagai jenis perangkat lunak jaringan area lokal, kita perlu mengkaji masalah hukum penting yang melibatkan perangkat lunak.

8.8 PERJANJIAN LISENSI PERANGKAT LUNAK

Perjanjian lisensi yang menyertai produk perangkat lunak adalah kontrak hukum dan menjelaskan sejumlah kondisi yang harus ditegakkan agar paket perangkat lunak dapat digunakan dengan benar. Kebanyakan perjanjian lisensi menetapkan ketentuan-ketentuan dalam bidang-bidang berikut:

- *Instalasi dan penggunaan perangkat lunak*—Menentukan jumlah komputer di mana pengguna boleh menginstal dan menggunakan perangkat lunak secara legal
- *Instalasi jaringan*—Menunjukkan apakah paket dapat diinstal pada jaringan komputer; dan jika demikian, apakah diperlukan lisensi tambahan untuk setiap mesin di jaringan
- *Salinan cadangan*—Memberi tahu pengguna apakah pembuatan salinan cadangan dapat diterima
- *Dekompilasi*—Menetapkan bahwa pengguna tidak boleh mendekompilasi, membongkar, atau merekayasa balik kode perangkat lunak dalam upaya mengambil bahasa tingkat tinggi untuk membuat modifikasi pada kode
- *Pernyataan sewa*—Menyatakan bahwa pengguna tidak diperbolehkan menyewakan atau menyewakan perangkat lunak kepada pihak ketiga
- *Peningkatan*—Jika program perangkat lunak merupakan peningkatan dari versi sebelumnya, informasikan kepada pengguna bahwa versi sebelumnya perlu dibeli sebelum peningkatan tersebut dapat diinstal
- *Hak Cipta*—Memberi tahu pengguna bahwa semua dokumentasi, gambar, dan materi lain yang disertakan dalam paket adalah hak cipta dan berada di bawah perlindungan undang-undang hak cipta
- *Pemeliharaan*—Memberi tahu pengguna apakah dukungan produk disertakan dalam pembelian paket perangkat lunak

Salah satu masalah terpenting yang mempengaruhi sebagian besar pengguna adalah instalasi dan penggunaan perangkat lunak. Ketika paket perangkat lunak dijual, biasanya paket tersebut ditujukan untuk jenis instalasi tertentu, yang disebut sebagai lisensi pengguna. Perusahaan perangkat lunak menetapkan lisensi pengguna sehingga seseorang di perusahaan tidak membeli satu salinan program dan menginstalnya pada, misalnya, 200 mesin, sehingga menipu perusahaan perangkat lunak tersebut sebesar 199 biaya pembelian, atau royalti. Royalti ini membayar biaya pembuatan perangkat lunak dan membantu mendukung biaya penyediaan peningkatan dan pemeliharaan di masa depan.

Ada beberapa bentuk lisensi pengguna: lisensi pengguna tunggal, lisensi pengguna interaktif, lisensi berbasis sistem, lisensi situs, lisensi perusahaan, dan Lisensi Publik Umum. Berdasarkan ketentuan salah satu lisensi pengguna yang paling umum, lisensi pengguna tunggal-stasiun tunggal, paket perangkat lunak dapat diinstal pada satu mesin, dan kemudian hanya satu pengguna pada satu waktu yang dapat menggunakan mesin tersebut. Beberapa paket perangkat lunak sebenarnya menghitung berapa kali perangkat lunak telah diinstal dan

hanya mengizinkan satu instalasi. Untuk memindahkan perangkat lunak ke komputer lain memerlukan menjalankan utilitas `uninstall` perangkat lunak. Lisensi satu pengguna-beberapa stasiun dirancang untuk pengguna yang mungkin memiliki mesin desktop di kantor dan mesin laptop untuk situs jarak jauh, atau mesin desktop lain di rumah. Pengguna berhak untuk mengizinkan hanya satu salinan perangkat lunak untuk digunakan pada satu waktu. Misalnya, jika pengguna sedang bekerja dan mengoperasikan program pengolah kata tertentu dengan lisensi `single-user-multiple-station`, tidak seorang pun boleh menjalankan program yang sama di laptop pengguna pada waktu yang bersamaan.

Lisensi pengguna interaktif, lisensi pengguna sistem operasi, dan lisensi pengguna bersamaan dalam jumlah terkontrol semuanya mengacu pada situasi yang pada dasarnya sama. Ketika paket perangkat lunak diinstal pada sistem multipengguna, seperti server pada jaringan area lokal, banyak pengguna dapat mengeksekusi banyak salinan dari satu program. Banyak paket perangkat lunak multipengguna yang memelihara penghitung untuk setiap orang yang sedang menjalankan program. Ketika jumlah maksimum pengguna secara bersamaan tercapai, tidak ada lagi pengguna yang dapat mengakses program. Ketika penghitung perangkat lunak tidak digunakan, administrator jaringan harus memperkirakan berapa banyak pengguna bersamaan dari paket perangkat lunak ini yang mungkin pada satu saat dan mengambil langkah-langkah yang diperlukan untuk membeli jumlah lisensi pengguna bersamaan yang sesuai.

Lisensi berbasis sistem, lisensi `cluster-wide`, dan lisensi server serupa dengan lisensi pengguna interaktif. Namun, dengan lisensi berbasis sistem atau server, jarang ada penghitung perangkat lunak yang mengontrol jumlah pengguna saat ini.

Lisensi situs memungkinkan paket perangkat lunak diinstal pada setiap dan semua stasiun kerja dan server di situs tertentu. Tidak ada penghitung instalasi perangkat lunak yang digunakan. Namun administrator jaringan harus menjamin bahwa salinan perangkat lunak tidak akan meninggalkan situs.

Lisensi perusahaan memungkinkan paket perangkat lunak diinstal di mana saja dalam suatu perusahaan, meskipun instalasi melibatkan banyak situs. Sekali lagi, administrator jaringan harus memastikan bahwa salinan perangkat lunak tidak meninggalkan instalasi perusahaan dan, misalnya, dibawa pulang bersama pengguna.

Lisensi Publik Umum (GPL) dikaitkan dengan perangkat lunak yang bebas untuk dibagikan dan diubah. Lisensi dengan jelas menetapkan bahwa “gratis” menyiratkan kebebasan untuk berbagi dan berubah, namun pembuat perangkat lunak tetap dapat mengenakan biaya. Pengguna yang tertarik untuk membuat atau menggunakan perangkat lunak GPL dianjurkan untuk mengunjungi situs Web Lisensi Publik Umum GNU (www.gnu.org/copyleft/gpl.html) untuk rincian lebih lanjut.

Setiap perusahaan perangkat lunak dapat membuat merek lisensi penggunanya sendiri dan menamainya dengan sesuatu yang unik. Orang yang menginstal perangkat lunak tersebut bertanggung jawab—baik pengguna, administrator sistem, atau administrator jaringan—untuk mengetahui rincian lisensi pengguna dan mengikutinya dengan cermat.

Apa yang terjadi jika seseorang tidak berperilaku sesuai dengan lisensi pengguna dan menginstal paket perangkat lunak di lingkungan yang tidak dimaksudkan? Dalam situasi ini, beberapa paket tidak akan berfungsi. Paket lain tidak akan berfungsi dengan benar jika instalasi tidak mengikuti perjanjian lisensi. Misalnya, beberapa paket perangkat lunak memiliki penghitung dan tidak mengizinkan salinan lebih banyak dari yang disepakati saat pembelian. Beberapa paket perangkat lunak, seperti sistem basis data, mungkin dapat diinstal pada beberapa mesin atau mungkin memberikan kesan mengizinkan akses banyak pengguna, namun jika paket tersebut tidak dirancang untuk akses banyak pengguna, paket tersebut mungkin tidak berfungsi dengan benar. Faktanya, penting selama akses database multipengguna bahwa sistem database mengunci pengguna lain saat satu pengguna sedang mengakses catatan data. Jika sistem sengaja tidak dirancang untuk akses multipengguna secara bersamaan, pelanggaran terhadap perjanjian lisensi dapat mengakibatkan hasil yang tidak diketahui.

Menginstal perangkat lunak pada lebih banyak mesin daripada yang disetujui dalam lisensi pengguna adalah tindakan ilegal. Jika Anda menginstal lebih banyak salinan daripada jumlah lisensi yang Anda miliki dan produsen perangkat lunak menemukan fakta ini, Anda dan perusahaan Anda mungkin menghadapi konsekuensi hukum. Oleh karena itu, ini adalah risiko yang jelas tidak layak untuk diambil. Pastikan perangkat lunak apa pun yang Anda pertimbangkan untuk dipasang memiliki lisensi pengguna yang sesuai sebelum Anda menginstalnya.

Hingga saat ini, bab ini telah memperkenalkan perangkat lunak jaringan area lokal—sistem operasi jaringan, utilitas, dan alat lainnya—dan lisensi perangkat lunak. Sisi perangkat keras jaringan area lokal berisi berbagai jenis perangkat yang juga memerlukan penyelidikan lebih lanjut.

8.9 PERANGKAT DUKUNGAN LAN

Jaringan area lokal terdiri dari banyak elemen, baik komponen perangkat lunak maupun perangkat keras. Dalam Bab Tujuh, hub, switch, dan router—perangkat keras yang menghubungkan perangkat-perangkat di jaringan—dibahas secara rinci. Mari kita lihat sejumlah perangkat pendukung LAN lainnya—termasuk catu daya yang tidak pernah terputus, tape drive, penyimpanan yang terhubung ke jaringan, printer, konverter media, dan stasiun kerja—yang mungkin Anda temui di jaringan area lokal pada umumnya.

Catu daya yang tidak pernah terputus (UPS) adalah perangkat yang berharga jika terjadi kegagalan daya. UPS adalah perangkat cadangan baterai yang dapat mempertahankan daya ke satu atau lebih peralatan untuk jangka waktu singkat (biasanya kurang dari satu jam). Dalam lingkungan perusahaan, perangkat UPS sering digunakan untuk membuat cadangan server area lokal dan komputer mainframe. Sebagian besar perusahaan menggunakan sistem UPS untuk mempertahankan daya cukup lama agar server atau mainframe dapat dimatikan dengan benar. Beberapa orang bahkan menggunakan perangkat UPS di rumah mereka untuk melindungi diri mereka dari kehilangan data jika aliran listrik terputus saat mereka sedang mengerjakan dokumen. Namun secara umum, sebagian besar pengguna rumahan tidak

menggunakan perangkat UPS. Sebaliknya, banyak yang melindungi komputer mereka dengan menggunakan pelindung lonjakan listrik sederhana yang mengisolasi peralatan komputer mereka dari lonjakan listrik.

Tape drive masih merupakan perangkat cadangan yang sangat baik, namun suatu saat mungkin akan digantikan dengan perangkat seperti hard disk drive atau solid-state drive. Alternatifnya, banyak perusahaan (dan pengguna rumahan) kini mencadangkan data mereka ke “cloud.” Sejumlah perusahaan berbasis Internet menawarkan layanan di mana pengguna dapat menyimpan data mereka (seperti data perusahaan, gambar, musik) di Internet dengan biaya bulanan atau tahunan. Meskipun demikian, masih umum untuk memasang tape drive ke server sehingga file yang dimodifikasi dapat dicadangkan satu kali atau lebih dalam sehari. Banyak perusahaan mencadangkan file mereka setiap malam, saat semua karyawan berada di rumah dan penggunaan jaringan minimal.

Penyimpanan terpasang jaringan (NAS) adalah perangkat berbasis komputer yang menyediakan penyimpanan dalam jumlah besar kepada pengguna di jaringan. Sistem operasi sederhana yang berjalan di NAS dirancang hanya untuk tujuan mengambil data bagi pengguna. Biasanya, perangkat NAS tidak memiliki keyboard atau monitor. Akses ke operasi kontrolnya biasanya diperoleh melalui alamat Web yang ditetapkan.

NAS tidak sama dengan SAN (jaringan area penyimpanan). SAN adalah perangkat penyimpanan yang lebih sederhana dan menggunakan protokol jaringan seperti iSCSI dan Fibre Channel untuk menyimpan dan mengambil data. Cara lain untuk melihat perbedaan antara NAS dan SAN adalah bahwa NAS cukup kuat untuk menggunakan protokol sistem filenya sendiri, sedangkan SAN lebih sederhana (hanya perangkat penyimpanan) dan bergantung pada protokol tingkat jaringan untuk membuat file sistem.

Printer cenderung berkembang lebih cepat dibandingkan perangkat jaringan lainnya. Beberapa tahun yang lalu, beragam pilihan printer dot-matrix, printer daisy-wheel, printer rantai, printer ink-jet, printer garis, dan printer laser telah tersedia. Saat ini, pasar printer pada dasarnya menyusut menjadi hanya dua format dasar: ink jet dan laser. Kedua format tersebut mampu mencetak hitam putih dan berwarna dengan resolusi sangat tinggi.

Konverter media adalah perangkat yang berguna jika diperlukan untuk menghubungkan satu jenis media dengan jenis media lainnya. Misalnya, jika bagian yang berbeda dari satu jaringan diinstal pada waktu yang berbeda dengan menggunakan media yang berbeda, mungkin lebih masuk akal untuk menggunakan konverter media untuk menghubungkan kedua jenis media tersebut daripada menghapus semua media lama dan menggantinya dengan yang lebih baru. Ada banyak tipe konverter media yang berbeda, sama halnya dengan kombinasi media yang berbeda-beda. Misalnya, ada media konverter yang khusus untuk menghubungkan kabel koaksial ke kabel twisted pair, dan kabel twisted pair ke kabel serat optik.

Seperti periferal komputer, stasiun kerja komputer itu sendiri telah berkembang selama bertahun-tahun. Workstation sekarang mendukung ratusan megabyte (bahkan gigabyte) memori akses acak dan memiliki penyimpanan hard disk ratusan gigabyte. Namun, beberapa aplikasi tidak memerlukan workstation dengan disk drive. Stasiun kerja klien tipis

adalah komputer tanpa disk drive apa pun. Perangkat lunak apa pun yang beroperasi pada klien tipis diunduh dari server ke klien tipis. Ide di balik klien tipis adalah untuk meminimalkan pemeliharaan stasiun kerja dan mengurangi biaya perangkat keras. Keamanan juga ditingkatkan dalam sistem klien tipis karena tidak mungkin memasukkan CD-ROM atau DVD untuk mengunggah atau mengunduh perangkat lunak atau data. Namun, gagasan untuk menghemat biaya perangkat keras dengan menggunakan klien tipis dibandingkan stasiun kerja yang dikonfigurasi sepenuhnya kehilangan momentum ketika produsen stasiun kerja yang dikonfigurasi sepenuhnya menurunkan harga mereka menjadi kurang dari Rp. 10.000.000 untuk mesin tingkat pemula. Meskipun demikian, klien tipis masih memperhatikan pertimbangan keamanan yang penting, dan biaya pemeliharaannya lebih rendah karena kurangnya disk drive. Setelah memeriksa komponen perangkat lunak dan perangkat keras yang penting dari jaringan area lokal, sekarang kita siap untuk melihat contoh bisnis.

8.10 PENGGUNAAN LAN DALAM PERUSAHAAN

Seperti yang kita lihat di bab sebelumnya, Hannah adalah administrator jaringan untuk sebuah perusahaan kecil. Tanggung jawabnya adalah menciptakan jaringan area lokal yang cukup sederhana yang menyediakan email antar kantor, akses ke database lokal, dan layanan pencetakan. Dia selanjutnya memperbarui jaringan untuk memasukkan akses ke Internet. Selain menentukan tata letak dan penempatan stasiun kerja, kabel, dan perangkat interkoneksi, Hannah kini harus memutuskan sistem operasi jaringan mana yang akan diinstal di semua stasiun kerja dan server perusahaannya. Seperti yang dipahami Hannah, dari membaca bab ini dia memiliki lima pilihan berikut:

1. Linux
2. UNIX
3. Server Windows
4. Server Mac OS X
5. NetWare OES dengan Linux atau Windows

Untuk membantu mengambil keputusan, Hannah bertanya pada dirinya sendiri pertanyaan-pertanyaan berikut:

- Apa kegunaan (aplikasi) utama dari sistem yang ada saat ini? Apakah kegunaan utama sistem akan berubah jika NOS tertentu dipasang?
- Bagaimana pengaruh pilihan NOS tertentu terhadap pemeliharaan dan dukungan?
- Apakah keuangan merupakan masalah dalam pemilihan NOS?
- Apakah sistem perusahaannya saat ini mempunyai perangkat keras atau perangkat lunak yang tidak biasa yang mungkin mempengaruhi pilihan NOS?
- Apakah jaringan akan berlokasi di satu lokasi atau di beberapa lokasi?
- Apakah ada tekanan politik dari manajemen untuk memilih NOS tertentu?

Mari kita periksa masing-masing pertanyaan ini untuk melihat bagaimana pengaruhnya terhadap keputusan yang harus diambil Hannah sehubungan dengan pemilihan sistem operasi jaringan untuk perusahaannya.

Kegunaan utama dari sistem saat ini

Seperti yang kita lihat sebelumnya, perusahaan tempat Hannah bekerja menggunakan stasiun kerja dan jaringannya untuk spreadsheet, pengolah kata, email lokal dan jarak jauh, serta akses halaman Web. Semua aplikasi ini cukup umum dan tidak menimbulkan persyaratan jaringan yang tidak biasa. Selain itu, perusahaan ini tidak memiliki aplikasi lama atau aplikasi buatan sendiri yang dapat bekerja dengan baik pada satu jenis sistem operasi namun tidak pada sistem operasi lainnya.

Satu-satunya aplikasi yang saat ini digunakan oleh karyawan yang mungkin menjadi perhatian adalah sistem database. Paket perangkat lunak basis data dapat menyebabkan kesulitan, tergantung di mana penyimpanan data sebenarnya disimpan. Jika perusahaan ingin mempertahankan penyimpanan data lokal pada masing-masing workstation, maka pilihan paket tidak menimbulkan persyaratan khusus dalam hal sistem operasi jaringan karena sejumlah paket database akan mendukung pengaturan ini. Namun, jika perusahaan ingin mempertahankan penyimpanan data terpusat, pilihan paket database yang tersedia lebih sedikit. Perhatian harus diberikan untuk memastikan paket database penyimpanan pusat yang dipilih berfungsi dengan sistem operasi tertentu. Misalnya, server penyimpanan database Microsoft, SQL Server, paling baik beroperasi di jaringan Microsoft dan mungkin tidak berinteroperasi dengan jaringan lain.

Pemeliharaan dan dukungan jaringan

Hannah prihatin dengan tingkat pemeliharaan yang diperlukan untuk mendukung jaringan area lokal perusahaan. Karena perusahaannya kecil, dengan kurang dari 40 stasiun kerja, Hannah mungkin akan melakukan sebagian besar administrasi jaringannya sendiri. Oleh karena itu, dia ingin (secara alami) memilih sistem operasi jaringan yang membutuhkan pekerjaan paling sedikit.

Hannah mungkin ingin menerima pelatihan untuk mendukung pilihan NOS-nya. Seseorang dapat menjadi administrator jaringan bersertifikat di Windows dan OES/NetWare. Sertifikasi yang paling umum untuk Windows adalah MCSE (Microsoft Certified Systems Engineer); dan untuk Linux adalah LPI (Linux Professional Institute). Alternatifnya, akan lebih mudah untuk mempekerjakan seseorang yang memiliki salah satu atau kedua sertifikasi tersebut.

Salah satu skenario yang coba dihindari Hannah adalah memiliki banyak sistem operasi. Mungkin saja, dan cukup umum, jaringan mendukung lebih dari satu jenis sistem operasi jaringan. Misalnya, seseorang dapat membuat server database Microsoft dan menginstalnya pada Microsoft NOS, dan juga menginstal Server Mac OS X untuk menangani file jaringan dan permintaan pencetakan. Namun, solusi ini mengharuskan Hannah untuk mempelajari dua sistem operasi jaringan dan melakukan dua rangkaian administrasi—bukan posisi yang dia inginkan.

Biaya NOS

Ketika mempertimbangkan biaya sistem operasi jaringan, Hannah perlu mempertimbangkan biaya administrasi menjalankan sistem selain pengeluaran dana awal yang diperlukan untuk membeli perangkat lunak. Selain itu, ia perlu memperhitungkan biaya

downtime yang signifikan jika NOS yang ia pilih ternyata tidak stabil seperti yang diharapkan. Ketika sistem baru dipasang, biaya pelatihan yang signifikan juga dikeluarkan.

Ketika Hannah memeriksa biaya awal sistem operasi jaringan, Linux adalah pemenangnya (mulai dari nol dolar hingga beberapa ratus dolar). Mac OS X Server juga cukup menarik dengan formula harga saat ini. OES/NetWare, Windows, dan UNIX lebih mahal dan kira-kira setara satu sama lain dalam biaya pembelian keseluruhan. Namun dari penelitiannya, Hannah mengetahui bahwa ada biaya lain yang tidak selalu terlihat jelas dan harus dia waspadai. Misalnya, meskipun lisensi satu pengguna-stasiun tunggal untuk Windows lebih murah dibandingkan lisensi satu pengguna-stasiun tunggal untuk OES/NetWare, penggunaan Windows NOS juga memerlukan pembelian lisensi server Windows. Tidak ada biaya yang terkait dengan server NetWare. Demikian pula Linux, UNIX, dan Mac OS X Server tidak memiliki lisensi klien dan server terpisah.

Pilihan perangkat keras unik apa pun yang memengaruhi keputusan NOS

Tak satu pun dari sistem operasi jaringan yang dipertimbangkan Hannah memerlukan perangkat keras unik. Sebaliknya, perangkat keras yang dipilih Hannah untuk mendukung jaringan tidak akan memberikan batasan apa pun pada pilihan NOS. Salah satu fitur menarik dari Linux adalah, bergantung pada operasi yang dijalankannya, ia dapat dijalankan dalam ruang memori yang relatif kecil dan pada teknologi mikroprosesor yang cukup lama (seperti mikroprosesor Intel 386). Sistem operasi jaringan lainnya memerlukan lebih banyak memori dan ruang hard disk, serta teknologi prosesor modern.

Lokasi tunggal atau beberapa lokasi

Saat ini, semua sumber daya perusahaan Hannah berada di satu lokasi. Namun jika perusahaan ingin menambah pengguna jarak jauh atau seluler, OES/NetWare, dengan persyaratan perangkat lunak klien yang lebih sederhana, merupakan pilihan yang sangat menarik. Fungsi administratif OES/NetWare dan Mac OS X Server memudahkan penanganan pengguna lokal dan jarak jauh. Meskipun sistem operasi lain juga dapat menangani kedua jenis pengguna tersebut, fungsi administrasinya mungkin lebih menantang.

Tekanan politik mempengaruhi keputusan

Tidak ada tekanan politik yang memaksa Hannah untuk memilih satu NOS tertentu dibandingkan NOS lainnya. Administrasi perusahaan tidak memiliki kesetiaan terhadap sistem tertentu dan memiliki sedikit atau tidak memiliki pengalaman sebelumnya dengan NOS tertentu. Demikian pula, sebagian besar pengguna tidak terlalu menyukai satu sistem dibandingkan sistem lainnya. Masalah potensial yang pernah ada adalah ketika pengguna terbiasa dengan lingkungan seperti Windows, dan tidak semua sistem operasi jaringan menawarkan lingkungan seperti Windows. Namun, hal tersebut tidak lagi terjadi. Selain itu, banyak orang (secara keliru) berpikir bahwa Server Mac OS X hanya berfungsi dengan perangkat Apple lainnya dan, oleh karena itu, mungkin menolak gagasan menggunakannya untuk aplikasi jenis bisnis.

Keputusan akhir

Saat Anda mempertimbangkan satu sistem operasi jaringan dibandingkan sistem operasi lainnya, keputusan yang paling penting adalah dipikirkan dengan matang. Semua

faktor harus dipertimbangkan, dan hype serta iklan tidak boleh menjadi bagian dari pertimbangan. Untungnya, semua sistem operasi jaringan yang Hannah pertimbangkan adalah produk berkualitas tinggi. Selain itu, kelima sistem tersebut populer dan kuat, dan masing-masing memiliki pengikut yang kuat. Salah satu kekhawatiran yang terkait dengan NetWare/OES adalah berapa lama sistem ini akan bertahan. Namun mengingat kekuatan lapangannya, kecil kemungkinannya Hannah akan membuat pilihan yang buruk, asalkan dia mempertimbangkan faktor-faktor yang dijelaskan sebelumnya dan kebutuhan perusahaannya.

8.11 JARINGAN NIRKABEL UNTUK RUMAH

Sam memiliki tiga komputer, printer multifungsi yang bagus (cetak/faks/scan/copy), dan koneksi Internet berkecepatan tinggi di rumah. Dia ingin menghubungkan ketiga komputer tersebut ke Internet dan printer, namun dia tidak ingin memasang kabel apa pun karena komputer tersebut terletak di lantai yang berbeda di rumahnya. Jadi Sam memutuskan untuk memasang jaringan area lokal nirkabel. Mari kita ikuti Sam saat dia membuat banyak keputusan yang diperlukan untuk memasang jaringan nirkabel.

Sam terlebih dahulu perlu menentukan teknologi LAN nirkabel mana yang didukung perangkatnya. Ingatlah bahwa ada empat teknologi yang disetujui untuk LAN nirkabel: IEEE 802.11b, 802.11a, 802.11g, dan 802.11n. IEEE 802.11b adalah standar pertama yang disetujui (pada tahun 1999) untuk digunakan dengan LAN nirkabel. Ini mentransmisikan sinyal pada 2,4 GHz sekitar 50 meter (150 kaki) antara titik akses dan perangkat nirkabel. IEEE 802.11b secara teoritis mentransfer data pada 11 Mbps. Namun, kecepatan transfer data sebenarnya adalah sekitar 5 Mbps. IEEE 802.11a adalah standar kedua yang disetujui pada tahun 2002. Standar ini mentransfer data dengan kecepatan teoretis 54 Mbps (dengan kecepatan sebenarnya kira-kira setengahnya) menggunakan frekuensi 5 GHz. Karena frekuensi yang lebih tinggi, 802.11a hanya dapat mentransmisikan sekitar setengah jarak 802.11b. Yang lebih rumit lagi, 802.11a dan 802.11b tidak kompatibel. Standar ketiga yang disetujui adalah IEEE 802.11g, pada tahun 2003. Standar ini mentransmisikan pada frekuensi yang sama dengan 802.11b (2,4 GHz) tetapi memiliki kecepatan transfer teoretis sebesar 54 Mbps (dengan kecepatan sebenarnya kira-kira setengahnya). Ini kompatibel dengan 802.11b dan memiliki jarak transmisi yang sama, kira-kira 50 meter. Terakhir, 802.11n disetujui pada tahun 2009 dan dapat mentransfer data dalam jumlah ratusan Mbps. Banyak, jika tidak sebagian besar, laptop dan desktop yang dijual saat ini mendukung keempat teknologi nirkabel. Peralatan lama mungkin hanya mendukung 802.11b/a/g. Jika salah satu komputer Sam tidak memiliki NIC nirkabel terpasang, ia harus membeli kartu NIC nirkabel untuk dipasang di desktop, atau perangkat NIC nirkabel yang dapat dicolokkan ke konektor USB di laptop.

Sekarang Sam perlu memiliki titik akses nirkabel, tapi dia telah membaca bahwa ada juga perangkat yang disebut router nirkabel dan gateway. Apa bedanya? Jika Anda sudah memiliki jaringan kabel di rumah (modem untuk menyambung ke Internet berkecepatan tinggi dan router untuk menghubungkan berbagai stasiun kerja), maka yang Anda perlukan hanyalah titik akses nirkabel. Hubungkan titik akses, sambungkan ke router yang ada, instal perangkat

lunak keamanan, dan Anda akan siap. Jika Anda memiliki koneksi Internet berkecepatan tinggi tetapi tidak memiliki koneksi lain, Anda dapat membeli router nirkabel. Router nirkabel bertindak sebagai router dan titik akses nirkabel. Jika Anda belum memiliki koneksi Internet berkecepatan tinggi, Anda mungkin mempertimbangkan untuk memasang gateway. Gateway sering kali merupakan kombinasi modem berkecepatan tinggi, router, dan titik akses nirkabel—ketiga perangkat tersebut digabung menjadi satu. Banyak perusahaan yang menyediakan layanan Internet ke rumah akan memberi Anda perangkat gateway nirkabel dengan biaya bulanan atau tanpa biaya sama sekali. Potensi masalah saat membeli modem berkecepatan tinggi Anda sendiri (seperti bagian dari gateway) adalah kompatibilitas dengan layanan Internet kecepatan tinggi. Pastikan Anda menghubungi penyedia layanan Internet Anda sebelum membeli modem Anda sendiri.

Sam sudah memiliki layanan Internet berkecepatan tinggi, namun tidak memiliki router nirkabel, sehingga ia memutuskan untuk membeli router nirkabel, memastikan router tersebut memiliki opsi keamanan seperti WPA atau WPA II. Saat memasang router, dia segera mengubah nama jaringan default dan kata sandi administrator untuk meminimalkan kemungkinan seseorang meretas jaringan nirkabelnya. Salah satu opsi keamanan tambahan yang dicari Sam adalah Stateful Packet Inspection (SPI). Sebuah router yang menjalankan SPI memastikan bahwa setiap paket masuk sesuai dengan permintaan keluar yang dibuat Sam, dan bukan seseorang di sebelahnya yang “mencuri” transmisi radio gratis Sam.

Bagaimana dengan sistem operasi di workstation-nya? Apakah Sam memerlukan sistem operasi jaringan seperti Linux atau Windows Server? Tidak, Sam tidak memerlukan sesuatu yang sekuat sistem operasi jaringan, meskipun ia membuat jaringan perangkat nirkabel. Banyak sistem operasi desktop terkini seperti Windows 7 atau Mac OS X mempunyai ketentuan untuk mendukung workstation nirkabel. Sam mungkin harus menggunakan Panel Kontrol di sistem operasi untuk memilih Protokol Internet TCP/IP untuk sambungan, dan memberi tahu sistem operasi bagaimana alamat IP untuk perangkat ini akan diperoleh. Petunjuk seperti ini biasanya disertakan bersama router nirkabel dan kartu antarmuka jaringan, dan tidak sulit untuk diikuti.

Apakah Sam memerlukan perangkat lunak pendukung jaringan tambahan? Dia pasti memerlukan beberapa bentuk perangkat lunak antivirus untuk melindungi mesinnya dari virus, dan mungkin bukan ide yang buruk untuk menginstal perangkat lunak anti-spam dan anti-spyware secara bersamaan. Perangkat lunak penilaian keamanan selalu berguna, terutama dengan perangkat nirkabel dan akses Internet. Sam juga berencana menggunakan perangkat lunak firewall yang disertakan dengan router dan mengatur opsi keamanan untuk melindungi komputer dan datanya.

Sam harus siap menggunakan jaringan nirkabel barunya. Semua perangkat telah dikonfigurasi untuk komunikasi LAN nirkabel (termasuk printer), serta router nirkabel dan perangkat lunak keamanan. Kini Sam bisa berselancar di Internet dari ruangan mana pun di rumahnya, bahkan mungkin dari halaman belakang, di samping kolam renang.

RINGKASAN

- Topologi nirkabel memungkinkan penempatan stasiun kerja yang sangat fleksibel dan tidak memerlukan kabel untuk mengirim dan menerima data.
- CSMA/CA adalah perangkat lunak kontrol akses medium yang memungkinkan perangkat nirkabel terhubung ke titik akses.
- Sistem operasi jaringan mempunyai beberapa fungsi tambahan yang biasanya tidak ditemukan dalam sistem operasi. Misalnya, dapat:
 - Kelola satu atau lebih server
 - Memelihara sistem file kumpulan data, aplikasi, profil pengguna, dan periferal jaringan
 - Mengkoordinasikan semua sumber daya dan layanan yang tersedia
 - Memproses permintaan dari pengguna
 - Meminta pengguna untuk login jaringan, memvalidasi akun, menerapkan pembatasan, dan menjalankan fungsi akuntansi
 - Kelola satu atau lebih printer jaringan
 - Kelola interkoneksi antar jaringan area lokal
 - Kelola pengguna yang terhubung secara lokal dan pengguna yang terhubung dari jarak jauh
 - Mendukung keamanan sistem dan fungsi klien/server
 - Mendukung pengembangan halaman Web dan pengoperasian server Web
- Novell NetWare (sekarang disebut Open Enterprise Server) adalah sistem operasi jaringan populer pertama dengan layanan direktori yang kuat (NDS), dan sangat baik dalam melakukan penyajian file dan pencetakan.
- Windows NT adalah sistem operasi jaringan populer pertama milik Microsoft, sangat baik dalam mendukung aplikasi klien/server, dan berbasis domain. Windows Server 2000/2003/2008 mewakili kemajuan yang signifikan dibandingkan NT dan mencakup layanan direktori yang kuat, Active Directory.
- UNIX adalah sistem operasi lama yang stabil, cepat, dan mampu berjalan di berbagai platform.
- Linux adalah turunan UNIX yang memiliki fitur stabilitas dan kecepatan yang sama dengan UNIX serta biaya rendah dan kemampuan untuk berjalan di berbagai platform.
- Mac OS X Server adalah turunan lain dari UNIX dan, seperti Linux, memiliki fitur stabilitas dan kecepatan yang sama dengan UNIX. Ini mendukung kelompok kerja Macintosh dan PC.
- Server adalah komputer yang menyimpan sumber daya perangkat lunak seperti sistem operasi jaringan, aplikasi komputer, program, kumpulan data, dan basis data, dan menyediakan satu atau lebih layanan kepada pengguna yang terhubung.
- Banyak server yang dapat menjalankan satu atau lebih level RAID. RAID dirancang untuk menyediakan cadangan data berlebihan ke beberapa hard disk drive.
- Banyak jenis program perangkat lunak yang mendukung jaringan area lokal. Ini termasuk program utilitas dan perangkat lunak Internet.

- Perjanjian lisensi perangkat lunak merupakan bagian penting dari instalasi perangkat lunak jaringan area lokal. Bentuk yang paling umum adalah pengguna tunggal-stasiun tunggal, pengguna tunggal-banyak stasiun, pengguna interaktif, berbasis sistem, situs, lisensi perusahaan, dan Lisensi Publik Umum.
- Banyak jenis perangkat keras yang diperlukan untuk mendukung jaringan area lokal, termasuk hub, switch, dan router; pasokan listrik yang tidak pernah terputus dan pelindung lonjakan arus; tape drive; penyimpanan terlampir jaringan; printer dan server cetak; konverter media; stasiun kerja; dan server.

PERTANYAAN

1. Apa keuntungan utama dari LAN nirkabel?
2. Apa yang dimaksud dengan Perangkat Layanan Dasar?
3. Buat daftar versi teknologi LAN nirkabel terkini.
4. Apa perbedaan antara CSMA/CA dan CSMA/CD?
5. Sebutkan enam fungsi dasar sistem operasi.
6. Apa yang membedakan sistem operasi multitasking dengan sistem operasi non-multitasking?
7. Sebutkan perbedaan utama antara sistem operasi jaringan dan sistem operasi.
8. Apa yang dimaksud dengan antarmuka pemrograman aplikasi?
9. Apa fungsi dasar sistem operasi jaringan?
10. Apa yang dimaksud dengan pencerminan disk?
11. Apa yang dimaksud dengan unit organisasi?
12. Apa fungsi NDS OES/NetWare?
13. Apa kelebihan utama Windows Server 2000 dibandingkan NT Versi 4?
14. Apa perbedaan antara Windows Server 2008 dan Windows Server 2000?
15. Apa fungsi Direktori Aktif Window?
16. Apa kelebihan UNIX?
17. Sebutkan alasan popularitas Linux.
18. Apa kelebihan Mac OS X Server?
19. Apa fungsi server?
20. Jenis server apa saja yang tersedia?
21. Apa saja tingkatan RAID yang berbeda, dan apa fungsinya?
22. Permasalahan apa saja yang sering disebutkan dalam perjanjian lisensi perangkat lunak?
23. Sebutkan jenis-jenis perjanjian lisensi perangkat lunak.
24. Apa sembilan kelompok perangkat lunak utilitas jaringan yang paling umum?
25. Apa fungsi utama server halaman Web Internet?
26. Apa saja jenis perangkat pendukung perangkat keras untuk jaringan area lokal?
27. Apa perbedaan antara NAS dan SAN?

LATIHAN

1. Buat daftar standar IEEE 802.11b/a/g/n dalam urutan kecepatan transmisi terendah hingga kecepatan transmisi tertinggi.
2. Pada rentang frekuensi berapa standar IEEE 802.11b/a/g/n mentransmisikan? Apa yang penting tentang frekuensi yang berbeda ini?
3. Perangkat LAN nirkabel Anda baru saja mengirimkan permintaan untuk mengirim (RTS). Apa yang terjadi selanjutnya?
4. Perangkat LAN nirkabel Anda baru saja menentukan bahwa medianya menganggur. Apa yang terjadi selanjutnya?
5. Perusahaan Anda ingin membuat jaringan nirkabel untuk seluruh gedung kantor. Gedungnya setinggi 10 lantai, dan perusahaan ingin menggabungkan IEEE 802.11a dengan menempatkan satu titik akses di lantai sepuluh. Apakah tata letak ini akan berhasil? Menjelaskan.
6. Dalam CSMA/CA nirkabel, apa tujuan dari periode NAV?
7. Dalam sistem klien/server, klien mengirimkan permintaan ke server, server melakukan operasi pemrosesan, dan server mengembalikan hasilnya. Buat daftar semua kemungkinan masalah yang dapat terjadi pada transmisi dalam skenario ini.
8. Apa keunggulan utama NDS NetWare dibandingkan pengikatan sebelumnya?
9. Anda ingin membuat jaringan area lokal yang melindungi isi hard disk server dari kerusakan disk. Sebutkan semua teknik berbeda untuk memberikan perlindungan yang telah disajikan sejauh ini.
10. Apa struktur utama (wadah) yang digunakan saat merancang jaringan Windows NT?
11. Windows Server 2000/2003/2008 menggunakan Active Directory untuk layanan direktorinya, dan NetWare/OES menggunakan NDS. Apa persamaan kedua layanan direktori? Bagaimana mereka berbeda?
12. Anda bekerja di perusahaan yang memiliki tiga divisi: pemasaran, riset, dan penjualan. Setiap divisi memiliki banyak karyawan, masing-masing dengan tempat kerjanya sendiri. Setiap divisi juga memiliki server jaringannya sendiri dan sejumlah printer berkualitas tinggi. Gambarlah diagram Windows Active Directory dan diagram OES/NetWare NDS yang mendukung struktur jaringan perusahaan ini.
13. Apa persamaan UNIX dan Linux? Dalam hal apa mereka berbeda?
14. Mengapa stabilitas Linux begitu tinggi jika dibandingkan dengan sistem operasi jaringan lainnya?
15. Masalah dengan perangkat lunak antivirus adalah virus baru bermunculan setiap hari. Jika Anda mempunyai perangkat lunak anti-virus yang diinstal pada mesin atau jaringan Anda, bagaimana Anda selalu memperbarui perangkat lunak Anda?
16. Apa perbedaan antara lisensi perangkat lunak satu-pengguna-stasiun-tunggal dengan lisensi-pengguna-tunggal-banyak-stasiun? Apakah yang satu memiliki keunggulan dibandingkan yang lain dalam dunia bisnis? Di dunia komputer rumahan?
17. Jenis aplikasi perangkat lunak apa yang mungkin dipertimbangkan oleh perusahaan sebagai kandidat untuk mendapatkan lisensi situs?

18. Pertimbangkan skenario lisensi perangkat lunak berikut: Office Suite 1 berharga Rp. 2.990.000 per lisensi pengguna tunggal-stasiun tunggal, sedangkan Office Suite 2 berharga Rp. 2.990.000 per lisensi pengguna interaktif. Anda memiliki 200 pengguna di jaringan Anda, dan Anda memperkirakan bahwa pada satu waktu hanya 60 persen pengguna Anda yang akan menggunakan aplikasi suite. Tentukan solusi lisensi terbaik. Pada tingkat penggunaan interaktif berapa biaya lisensi pengguna interaktif akan mencapai titik impas dengan biaya lisensi stasiun tunggal pengguna tunggal?
19. Apakah komputer klien tipis lebih menguntungkan di lingkungan perusahaan atau di rumah pengguna? Menjelaskan.
20. Jika penting untuk tidak kehilangan data apa pun, teknik RAID mana yang Anda sarankan untuk digunakan?

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Sebuah usaha kecil dengan 100 stasiun kerja komputer sedang memasang jaringan area lokal baru. Semua pengguna melakukan operasi biasa email, pengolah kata, browsing Internet, dan beberapa persiapan spreadsheet. Sekitar seperempat karyawan melakukan sejumlah besar permintaan klien/server ke dalam sistem database. Sistem operasi jaringan area lokal manakah yang akan Anda rekomendasikan? Nyatakan alasan Anda.
2. Buat struktur pohon NDS atau Direktori Aktif untuk salah satu lingkungan berikut:
 - a. Segmen perusahaan tempat Anda bekerja
 - b. Seluruh perusahaan tempat Anda bekerja
 - c. Segmen sekolah tempat Anda terdaftar
 - d. Seluruh sekolah tempat Anda terdaftar
 - e. Perusahaan hipotetis yang memiliki banyak departemen, server, periferal, dan pengguna
3. Anda membuat jaringan di rumah yang terdiri dari beberapa komputer, printer berkualitas tinggi, dan router dengan akses ke koneksi Internet berkecepatan tinggi. Tentunya Anda tidak memerlukan Windows Server 2008 atau OES/NetWare, namun adakah sistem operasi desktop tertentu yang dapat diinstal pada setiap komputer yang akan mengoptimalkan operasional jaringan rumah Anda?
4. Anda mempunyai tiga komputer di rumah, dan Anda ingin menghubungkan ketiganya secara bersamaan. Dua komputer berada di lantai utama rumah, tetapi komputer ketiga ada di lantai atas di kamar tidur. Sebutkan sebanyak mungkin cara untuk menghubungkan ketiga komputer sehingga mereka dapat beroperasi pada satu jaringan area lokal.
5. Sebuah kompleks perkantoran setinggi empat lantai. Setiap lantai kira-kira berukuran 75 meter (yard) kali 75 meter. Perusahaan ingin membuat LAN nirkabel untuk seluruh kompleks. Teknologi LAN nirkabel manakah yang Anda rekomendasikan? Di mana Anda akan menempatkan titik akses? Di mana Anda akan menempatkan tulang punggung kabel?

6. Siapa yang membuat mesin thin client? Bagaimana spesifikasi, fitur, dan harganya?
7. Apakah ada sistem operasi jaringan selain yang tercantum dalam bab ini? Apakah mereka bertahan atau malah terlupakan?
8. Sistem operasi jaringan area lokal yang cukup populer selama beberapa tahun adalah OS/2. Bagaimana keadaan sistem ini saat ini? Apakah masih diproduksi? Apakah masih didukung? Bisakah Anda menemukan perkiraan berapa banyak jaringan yang menggunakan OS/2?
9. Apa perbedaan antara hak cipta dan paten bila diterapkan pada perangkat lunak komputer? Berapa lama hak cipta berlaku? Berapa lama masa berlaku paten?
10. Dalam bab ini, Anda mempelajari empat level RAID: RAID-0, RAID-1, RAID-3, dan RAID-5. Teliti dan buat daftar semua level (atau versi) RAID yang ada. Apa fungsi utama setiap level?

Bab 9

Pengantar Jaringan Area Metropolitan dan Jaringan Area Luas

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Membedakan jaringan area lokal, jaringan area metropolitan, dan jaringan area luas satu sama lain
- Identifikasi karakteristik jaringan area metropolitan, dan jelaskan bagaimana mereka membandingkan dan membedakannya dengan jaringan area luas dan jaringan area lokal
- Jelaskan cara kerja jaringan Circuit-Switched, Datagram Packet-Switched, dan Virtual Circuit Packet-Switched dan bagaimana mereka menyusun sebuah jaringan cloud
- Identifikasi perbedaan antara jaringan berorientasi koneksi dan jaringan tanpa koneksi, dan berikan contohnya masing-masing
- Jelaskan perbedaan antara perutean terpusat dan perutean terdistribusi, serta sebutkan kelebihan dan kekurangan masing-masing
- Jelaskan perbedaan antara perutean statis dan perutean adaptif, serta sebutkan kelebihan dan kekurangan masing-masing
- Dokumentasikan karakteristik utama banjir, dan gunakan jumlah lompatan dan batas lompatan dalam contoh sederhana
- Diskusikan konsep dasar kemacetan jaringan, termasuk kualitas layanan

VINTON CERF, CO-CREATOR TCP (protokol utama yang digunakan di Internet), telah mengalihkan perhatiannya pada penciptaan jaringan yang dapat menjangkau wilayah yang sangat luas: tata surya. Cerf bergabung dengan tim dari NASA untuk membuat jaringan nirkabel yang memungkinkan pengguna di Bumi, satelit, pesawat luar angkasa, dan akhirnya astronot untuk berbicara satu sama lain. Jaringan ini disebut Internet Antarplanet (IPN).

Cerf mengatakan: “Saya menyadari bahwa dibutuhkan waktu 20 tahun agar Internet bisa berkembang pesat: dari tahun 1973 hingga 1993. Jadi saya bertanya-tanya apa yang harus saya lakukan untuk mempersiapkan kebutuhan kita di masa depan. Jawabannya adalah tulang punggung antarplanet.”

Saat ini, kedua penjelajah di Mars memiliki alamat IPN masing-masing, nama domain .mars, dan protokol baru yang mirip dengan TCP/IP tetapi disederhanakan untuk mengatasi kekhasan transmisi data melalui luar angkasa. Beberapa keanehan yang harus diatasi oleh IPN adalah tingkat kebisingan yang tinggi, sinyal yang lemah, pasokan daya yang kecil, dan penundaan propagasi yang lama.

Untuk proyek berikutnya, Cerf berharap dapat menempatkan satelit telepon di orbit pada akhir dekade ini yang akan menghubungkan kedua planet tersebut. Akankah NASA mampu melakukan hal ini? Cerf optimis. Ia merasa bahwa ketika perjalanan luar angkasa

menjadi sebuah upaya komersial (seperti Internet pada akhirnya), IPN dan komunikasi antarplanet akan berkembang pesat. Seperti roket.

*Internet dan Internet Antarplanet adalah jaringan area luas. Apa yang dimaksud dengan jaringan area luas, dan apa bedanya dengan jaringan area lokal?
Apakah semua jaringan area luas mempunyai fitur yang sama?*

9.1 PENDAHULUAN

Jaringan area lokal, seperti yang Anda ingat, biasanya terbatas pada satu gedung atau sekumpulan gedung yang berdekatan (seperti di kampus). Apa yang terjadi ketika jaringan diperluas ke wilayah metropolitan, lintas negara bagian, atau seluruh negara? Jaringan yang meluas ke wilayah metropolitan dan menunjukkan kecepatan data yang tinggi, keandalan yang tinggi, dan kehilangan data yang rendah disebut jaringan area metropolitan (MAN). Dalam bab ini, kita akan mengkaji jaringan wilayah metropolitan dan melihat bagaimana jaringan tersebut dibandingkan dan dikontraskan dengan bentuk jaringan lainnya.

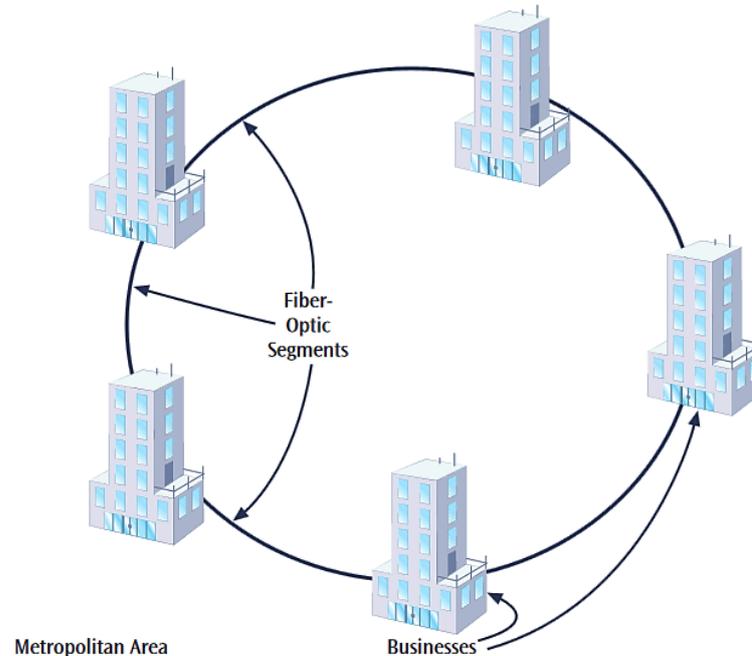
Apa yang terjadi jika jaringan lebih besar dari wilayah metropolitan? Jaringan yang meluas melampaui wilayah metropolitan adalah jaringan area luas. Jaringan area luas mempunyai beberapa karakteristik yang sama dengan jaringan area lokal: Jaringan ini menghubungkan komputer, menggunakan beberapa bentuk media untuk interkoneksi, dan mendukung aplikasi jaringan. Tapi ada perbedaan. Jaringan area lokal tidak melakukan perutean. Sebaliknya, mengalihkan frame ke tujuan lokal yang tepat, sementara router merutekan paket dari satu jaringan area luas ke jaringan area luas lainnya. Jaringan area luas dapat menghubungkan sejumlah besar stasiun kerja (perangkat), sedemikian rupa sehingga stasiun kerja mana pun dapat mentransfer data ke stasiun kerja lainnya.

Sesuai dengan namanya, jaringan area luas dapat mencakup jarak geografis yang luas, termasuk seluruh bumi. Faktanya, seperti yang Anda pelajari pada sketsa pembuka bab ini, terdapat rencana untuk membangun jaringan di planet Mars karena semakin banyak teknologi yang dibuang ke planet ini dan kebutuhan untuk mengembalikan sinyal ke Bumi menjadi lebih besar. Dengan demikian, jaringan area luas suatu hari nanti mungkin mencakup seluruh tata surya!

Karena perbedaan antara jaringan area lokal dan jaringan area metropolitan dan jaringan area luas, dua bentuk jaringan terakhir layak untuk didiskusikan sendiri. Mari kita mulai dengan diskusi tentang jaringan area metropolitan, dan kemudian memperkenalkan terminologi dasar jaringan area luas. Kami kemudian akan memeriksa perbedaan antara jaringan area luas Circuit-Switched dan Packet-Switched. Pengenalan singkat tentang perutean juga diperlukan karena jaringan area luas menggunakan perutean secara ekstensif untuk mentransfer data. Bab selanjutnya dari teks ini akan membahas jenis jaringan area luas yang unik—khususnya, Internet.

9.2 DASAR-DASAR JARINGAN WILAYAH METROPOLITAN

Banyak dari teknologi dan protokol komunikasi yang sama yang ditemukan di jaringan area lokal (dan jaringan area luas) digunakan untuk membuat jaringan area metropolitan. Namun MAN seringkali unik dalam hal topologi dan karakteristik operasi. MAN dapat digunakan untuk mendukung sistem pemulihan bencana berkecepatan tinggi dan sistem cadangan transaksi real-time.



Gambar 9-1 Cincin fisik yang digunakan untuk mendukung jaringan area metropolitan

Mereka juga dapat menyediakan interkoneksi antara pusat data perusahaan dan penyedia layanan Internet, dan mendukung koneksi berkecepatan tinggi antara fasilitas pemerintahan, bisnis, medis, dan pendidikan. MAN hampir secara eksklusif merupakan jaringan serat optik dan, dengan demikian, mampu mendukung kecepatan data hingga puluhan juta dan ratusan juta bit per detik. Untuk alasan yang sama, mereka diiklankan sebagai jaringan dengan tingkat kesalahan yang sangat rendah dan throughput yang sangat tinggi. Meskipun karakteristik ini tidak jauh berbeda dengan jaringan area lokal lainnya, ada beberapa karakteristik yang membedakan MAN dari LAN. Karakteristik pertama adalah bahwa MAN mencakup jarak yang lebih jauh dibandingkan LAN. Sesuai dengan namanya, jaringan area metropolitan cukup mampu mendukung seluruh wilayah metropolitan, seperti New York, Chicago, dan Los Angeles. Jaringan area lokal jarang melampaui tembok suatu bangunan, dan karenanya lebih kecil dari MAN.

Karakteristik kedua yang membedakan MAN dari LAN (tetapi tidak harus dari WAN) adalah bahwa sebagian besar MAN dapat pulih dengan sangat cepat dari kegagalan link atau switch/router. MAN dirancang untuk memiliki sirkuit yang sangat redundant sehingga jika terjadi kegagalan komponen, jaringan dapat dengan cepat mengalihkan lalu lintas dari komponen yang gagal tersebut. Kemampuan untuk mengubah rute jika terjadi kegagalan disebut failover, dan kecepatan terjadinya failover adalah waktu failover. Meskipun tidak

semua MAN memiliki waktu failover yang rendah, mencapainya tentu saja merupakan tujuan dari setiap perusahaan yang menawarkan layanan MAN.

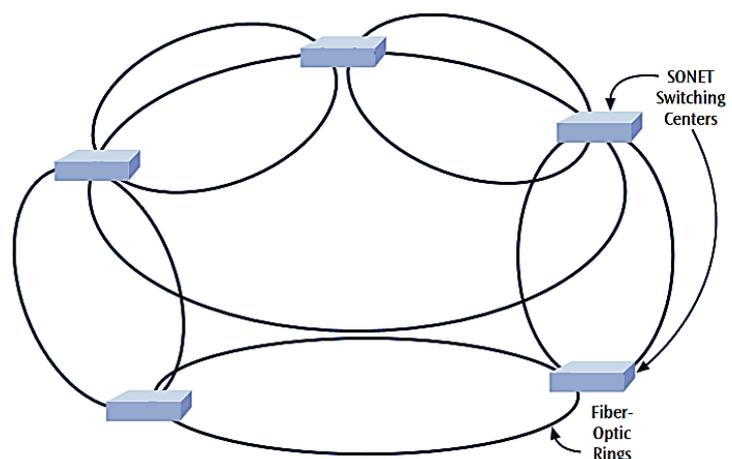
Karakteristik ketiga yang membedakan banyak MAN dari LAN dan WAN adalah bahwa beberapa topologi MAN didasarkan pada sebuah cincin. Cincin MAN unik karena merupakan cincin baik secara logika maupun fisik. Dengan demikian, tidak hanya data yang dilewatkan dalam bentuk cincin, tetapi juga router dan switch jaringan saling berhubungan dalam bentuk cincin (Gambar 9-1).

Terakhir, fitur yang mulai muncul di MAN, namun tidak dimiliki oleh LAN maupun WAN saat ini, adalah kemampuan pengguna untuk secara dinamis mengalokasikan lebih banyak bandwidth sesuai permintaan. Katakanlah Anda bekerja untuk sebuah bisnis dan memiliki koneksi MAN antara kantor perusahaan Anda dan penyedia layanan Internet. Anda mengantisipasi, mungkin karena Anda akan memperkenalkan penawaran layanan pelanggan baru, bahwa permintaan terhadap link MAN akan tumbuh secara substansial dalam beberapa hari ke depan. Jadi, Anda melakukan panggilan telepon—atau, dalam beberapa kasus, mengakses halaman Web—dan meminta agar bandwidth koneksi MAN Anda ditingkatkan dengan jumlah tertentu. Penyedia layanan MAN menerima permintaan Anda, segera meningkatkan bandwidth Anda, dan menagih Anda sesuai kebutuhan. Mungkin suatu saat nanti, semua jaringan—lokal, metropolitan, dan wilayah luas—akan memiliki fitur canggih ini. Untuk saat ini hanya ditawarkan oleh penyedia layanan MAN tertentu.

Sekarang kita telah memeriksa beberapa karakteristik dasar yang membedakan MAN dari LAN dan WAN, mari kita mengalihkan perhatian kita ke teknologi yang mendukung MAN.

SONET vs Ethernet

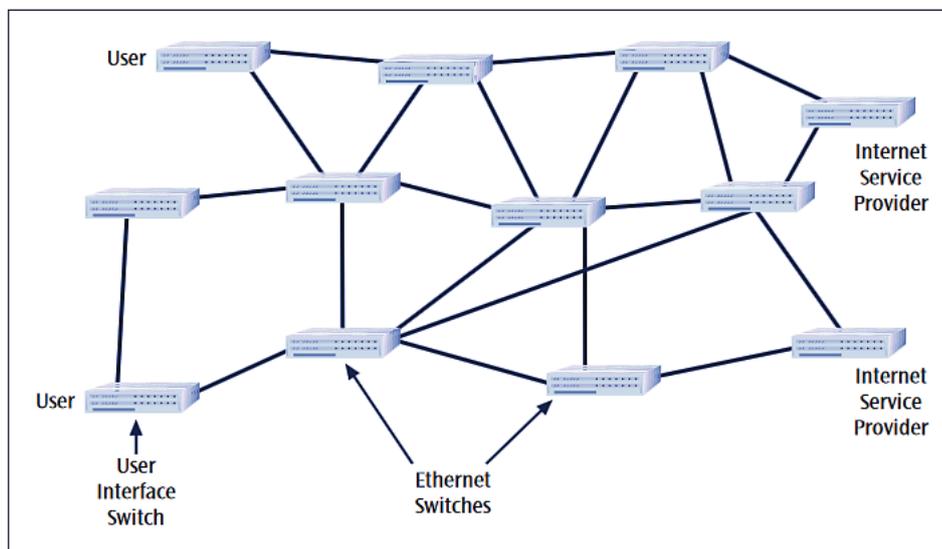
Hampir semua MAN didasarkan pada salah satu dari dua bentuk dasar teknologi pendukung: SONET atau Ethernet. SONET, seperti yang kita lihat di Bab Lima, adalah teknik multiplexing pembagian waktu sinkron yang mampu mengirimkan data dengan kecepatan ratusan juta bit per detik. Topologi jaringan berbentuk cincin, namun cincin ini sebenarnya terdiri dari beberapa cincin yang memungkinkan jaringan menyediakan cadangan jika terjadi kegagalan segmen (Gambar 9-2). Ini adalah salah satu karakteristik cincin SONET yang memungkinkannya memiliki waktu failover yang sangat rendah. Saat ini, banyak MAN yang didukung oleh teknologi cincin SONET.



Gambar 9-2 Sistem SONET terdiri dari beberapa cincin

Sayangnya, SONET memiliki sejumlah kelemahan. Ini adalah teknologi yang kompleks dan cukup mahal yang tidak dapat disediakan secara dinamis. Lebih jauh lagi, SONET dirancang untuk mendukung beberapa aliran saluran suara (seperti beberapa T-1, yang mentransmisikan pada 1,544 Mbps) dan dengan demikian tidak dapat diskalakan dengan baik ke dalam 1-Mbps, 10-Mbps, 100-Mbps, dan 1000. Potongan -Mbps yang biasanya digunakan dengan transmisi data. Menariknya, kekurangan ini menghidupkan kembali minat terhadap teknologi yang lebih tua dari SONET namun merupakan pendatang baru di bidang jaringan area metropolitan: Ethernet.

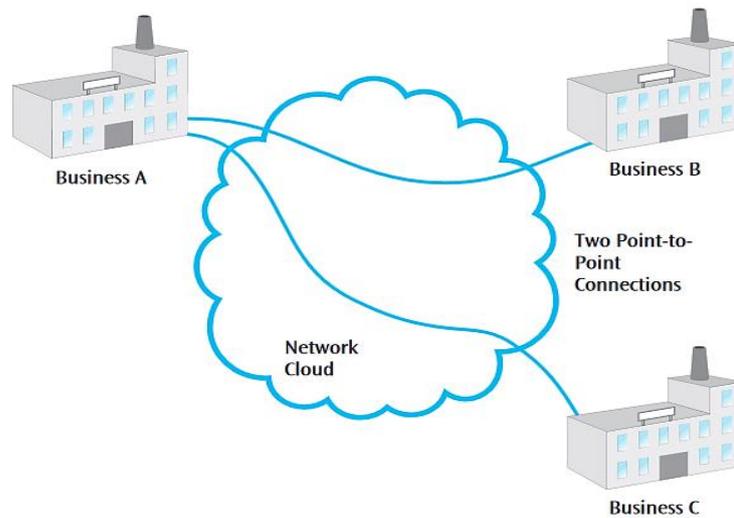
Ethernet MAN lebih murah dibandingkan sistem SONET, dipahami dengan baik, mudah diskalakan dari 10 Mbps hingga 100 Mbps hingga 1000 Mbps hingga 10 Gbps, dan teknologi terbaik untuk membawa lalu lintas IP (jenis lalu lintas yang berjalan melalui Internet). Salah satu kelemahan yang mengganggu beberapa versi Ethernet di MAN adalah waktu failover yang lebih tinggi. Ethernet MAN yang menggunakan Spanning Tree Protocol (dari Bab Tujuh) untuk mengkonfigurasi ulang jaringan yang diubah tidak pulih secepat SONET berdering dan berpotensi meninggalkan pelanggan tanpa layanan selama 10 detik. Cincin SONET biasanya memiliki waktu failover 50 milidetik atau kurang. Untuk meningkatkan waktu failover MAN berbasis Ethernet, banyak jaringan sekarang menggunakan Rapid Spanning Tree Protocol, yang dapat menurunkan waktu failover menjadi 50 milidetik. Terlepas dari itu, Ethernet MAN memiliki sejumlah karakteristik menarik dan semakin populer. Gambar 9-3 menunjukkan tata letak khas topologi Ethernet MAN. Perhatikan bagaimana jaringan merupakan desain mesh dengan jalur redundan antar titik akhir.



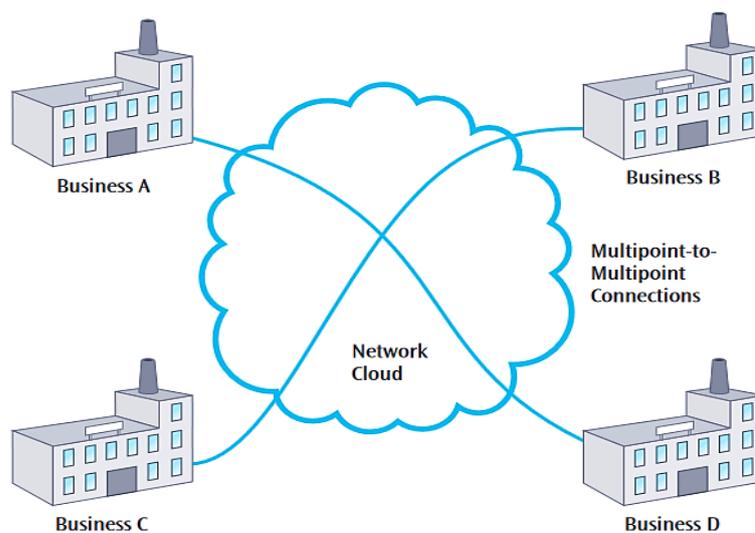
Gambar 9-3 Topologi mesh dari Ethernet MAN

Ethernet MAN telah memunculkan layanan baru yang popularitasnya meningkat dalam beberapa tahun terakhir: Metro Ethernet. Metro Ethernet adalah layanan transfer data yang dapat menghubungkan bisnis Anda ke bisnis (atau bisnis) lain menggunakan koneksi Ethernet standar. Dengan Metro Ethernet, Anda dapat menghubungkan perusahaan Anda secara langsung ke perusahaan lain menggunakan koneksi point-to-point, atau, misalnya, ke

dua perusahaan lain menggunakan dua koneksi point-to-point, seperti yang ditunjukkan pada Gambar 9-4 (A). Alternatifnya, Anda dapat menghubungkan perusahaan Anda ke beberapa perusahaan seolah-olah mereka semua adalah bagian dari jaringan area lokal yang besar, seperti yang ditunjukkan pada Gambar 9-4(b). Koneksi yang pertama sama dengan memiliki koneksi pribadi antara dua titik. Contoh umum dari jenis koneksi Metro Ethernet ini ditemukan ketika sebuah perusahaan terhubung ke penyedia layanan Internet. Semua lalu lintas pada sambungan ini hanya antara dua lokasi. Koneksi yang terakhir adalah contoh koneksi multipoint-to-multipoint. Di sini, perusahaan mana pun dapat berbicara dengan satu atau lebih (atau semua) perusahaan yang terhubung. Oleh karena itu, sebuah perusahaan hanya perlu mengirimkan satu paket untuk memastikan bahwa banyak perusahaan menerima data ini.



Gambar 9-4(a) Dua koneksi point-to-point



Gambar 9-4(b) Koneksi multipoint-to-multipoint

Aspek yang menarik dari Metro Ethernet adalah pengguna layanan ini dapat dengan mudah menghubungkan jaringan area lokal Ethernet perusahaan mereka ke layanan Metro Ethernet. Karena semua jaringan yang terlibat adalah Ethernet, tidak diperlukan konversi yang memakan waktu dan terkadang canggung dari satu format ke format lainnya. Dengan demikian, LAN perusahaan yang berjalan pada 100 Mbps dapat terhubung dengan baik ke layanan Metro Ethernet yang juga berjalan pada 100 Mbps. Hal yang sama tidak dapat dikatakan jika seseorang menghubungkan LAN 100-Mbps ke SONET, dengan kecepatan yang biasanya dimulai pada 51,48 Mbps.

Jika kita melihat apa yang ada di balik Metro Ethernet, kita akan melihat bahwa ada sejumlah variasi. Yang pertama disebut Ethernet murni. Namun karena Ethernet dirancang untuk jaringan area lokal yang lebih kecil, Ethernet murni tidak akan berfungsi dengan baik pada jarak jauh dengan jumlah pengguna yang besar tanpa bantuan protokol tambahan (seperti Rapid Spanning Tree Protocol). Ada juga Metro Ethernet di mana Ethernet sebenarnya berjalan melalui protokol data link kedua, seperti SONET/SDH atau MPLS. Dalam kasus ini, frame Ethernet digabungkan ke dalam frame SONET/SDH atau ke dalam frame MPLS. Metro Ethernet juga disebut Carrier Ethernet.

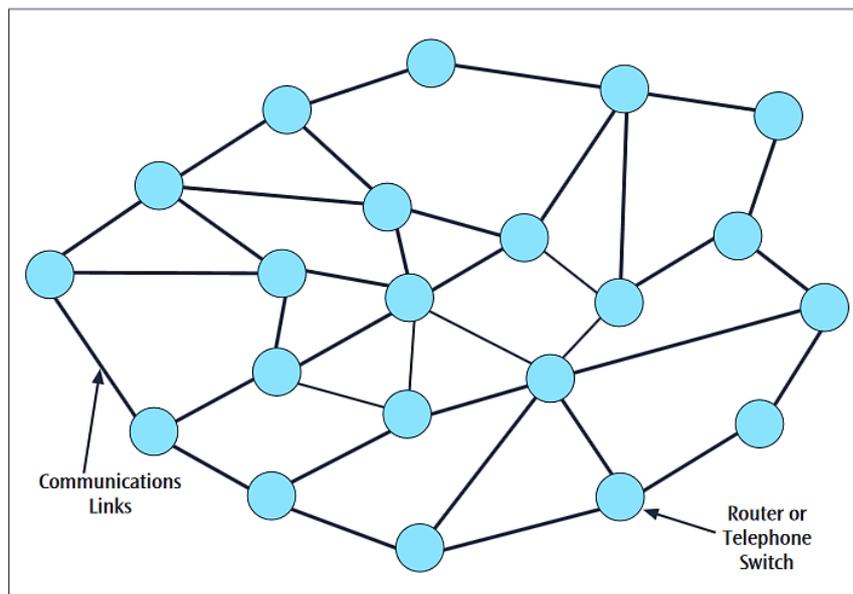
Perusahaan yang memiliki koneksi dengan Metro Ethernet dapat membuat profil bandwidth untuk koneksi tersebut. Profil bandwidth ini menjelaskan berbagai karakteristik koneksi, seperti kecepatan transfer data dasar, kecepatan burst dasar (burst, seperti yang Anda ingat, adalah gelombang besar data yang dikirimkan dalam jangka waktu singkat), kelebihan data, kecepatan transfer, dan tingkat ledakan berlebih. Ethernet jaringan area lokal, seperti yang kita lihat di Bab Tujuh, tidak mengizinkan pengguna untuk mengatur kecepatan transfer data mereka sendiri—mereka hanya harus menerima satu kecepatan yang sesuai dengan merek Ethernet tertentu (seperti Ethernet 100-Mbps) yang mereka miliki. terpilih. Fitur profil Metro Ethernet ini merupakan pilihan yang menarik dan kuat bagi perusahaan yang ingin menyesuaikan koneksi ke aplikasi tertentu. Misalnya, jika sebuah perusahaan meluncurkan aplikasi Web baru dan mengharapkan tingkat respons pengguna yang bervariasi, personel jaringan perusahaan dapat menetapkan kecepatan transfer data dasar untuk respons rata-rata yang diantisipasi, dan kemudian menetapkan kecepatan ledakan berlebih untuk periode puncak. Sekarang kita telah mempelajari dasar-dasar MAN, mari kita lihat dasar-dasar jaringan area luas.

9.3 DASAR-DASAR JARINGAN AREA LUAS (WAN)

Jaringan area luas (WAN) adalah kumpulan komputer dan peralatan terkait komputer yang saling terhubung untuk menjalankan fungsi atau fungsi tertentu, biasanya menggunakan sistem telekomunikasi lokal dan jarak jauh. Jenis komputer yang digunakan dalam jaringan area luas berkisar dari mikrokomputer hingga mainframe. Jalur telekomunikasi dapat sesederhana saluran telepon standar atau secanggih sistem satelit. Jaringan area luas biasanya digunakan untuk mentransfer data massal antara dua titik akhir dan menyediakan layanan surat elektronik, akses ke sistem database, dan akses ke Internet kepada pengguna.

Jaringan area luas juga dapat membantu operasi khusus di banyak bidang, seperti manufaktur, kedokteran, navigasi, pendidikan, hiburan, dan telekomunikasi.

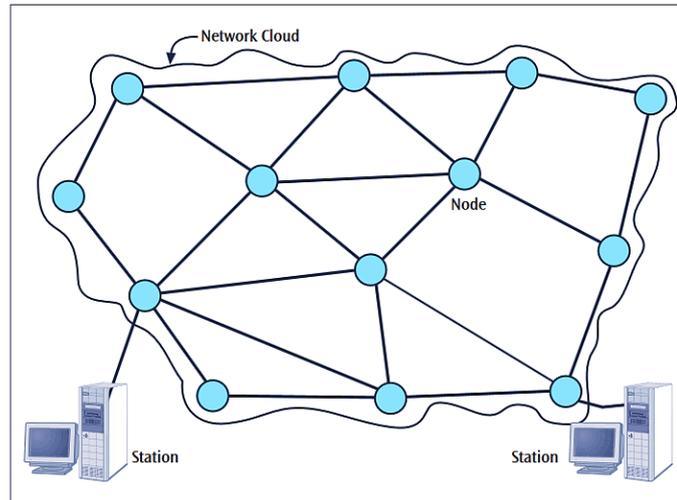
Seperti yang mungkin Anda ingat, jaringan area lokal berfungsi sebagai jaringan berbasis bus di mana cluster stasiun kerja terhubung ke titik pusat (hub atau switch) yang melaluinya stasiun kerja dapat mengirimkan pesan satu sama lain. Karena terdapat begitu banyak workstation dalam jaringan area luas dan tersebar dalam jarak yang jauh (mungkin sangat jauh), penggunaan koneksi tipe LAN tidak memungkinkan. Demikian pula, jaringan di mana setiap stasiun kerja terhubung ke setiap stasiun kerja jaringan lainnya juga tidak praktis, karena akan ada begitu banyak koneksi ke setiap stasiun kerja sehingga teknologinya tidak dapat dikelola sama sekali. Sebaliknya, jaringan area luas menghubungkan stasiun kerjanya melalui penggunaan desain mesh dan memerlukan perutean untuk mentransfer data melalui jaringan. Jaringan yang terhubung dalam mesh adalah jaringan yang tetangganya hanya terhubung ke tetangganya (Gambar 9-5). Jadi, untuk ditransmisikan melalui jaringan mesh, data harus diteruskan sepanjang rute dari stasiun kerja ke stasiun kerja lainnya.



Gambar 9-5 Jaringan mesh sederhana

Semua jaringan area luas merupakan kumpulan dari setidaknya dua tipe dasar peralatan: stasiun dan node. Stasiun adalah perangkat yang berinteraksi dengan pengguna untuk mengakses jaringan, dan berisi aplikasi perangkat lunak yang memungkinkan seseorang menggunakan jaringan untuk tujuan tertentu. Seringkali, stasiun adalah komputer mikro atau stasiun kerja, namun bisa juga berupa terminal, telepon seluler, atau komputer main-frame. Node adalah perangkat yang memungkinkan satu atau lebih stasiun mengakses jaringan fisik, dan merupakan titik transfer untuk meneruskan informasi melalui jaringan. Ketika data atau informasi berjalan melalui jaringan, informasi tersebut ditransfer dari node ke node melalui jaringan. Ketika informasi tiba di tujuan yang tepat, node tujuan mengirimkannya ke stasiun tujuan. Dalam jaringan yang dirancang untuk mentransfer data komputer, seperti Internet,

node biasanya berupa router yang sangat cepat dan kuat dengan banyak port. Data yang masuk tiba di satu port dan, bergantung pada rute yang harus diambil data untuk mencapai tujuannya, ditransmisikan kembali ke port kedua. Dalam jaringan yang dirancang untuk mentransfer sinyal suara, node biasanya merupakan saklar telepon kuat yang menjalankan fungsi serupa dengan router.



Gambar 9-6 Jaringan cloud, node, dan dua stasiun akhir

Struktur pendukung jaringan area luas adalah subjaringan, atau jaringan cloud. Subjaringan, atau jaringan cloud, adalah kumpulan node dan tautan telekomunikasi yang saling berhubungan, seperti yang ditunjukkan pada Gambar 9-6 (perhatikan bagaimana subjaringan digambar menyerupai awan). Jenis dan jumlah interkoneksi antar node dan cara data jaringan dikirimkan dari node ke node adalah tanggung jawab cloud jaringan. Ada baiknya jika kita menganggap jaringan area luas dan jaringan cloud sebagai dua entitas yang berbeda. Jaringan area luas adalah keseluruhan sistem: node, stasiun, jalur komunikasi, perangkat lunak, dan bahkan mungkin pengguna. Jaringan cloud adalah interkoneksi fisik yang mendasari node dan jalur komunikasi yang mentransfer data dari satu lokasi ke lokasi lain. Semua komponen ini bekerja sama untuk menciptakan jaringan. Pengguna yang duduk di stasiun kerja dan menjalankan aplikasi jaringan meneruskan datanya ke jaringan melalui stasiun, yang meneruskan data tersebut ke cloud. Cloud jaringan bertanggung jawab untuk mengirimkan data ke node tujuan yang tepat, yang kemudian mengirimkannya ke stasiun tujuan yang sesuai. Jelasnya, suatu jaringan tidak akan ada tanpa adanya cloud jaringan, namun tidak menjadi masalah bagi jaringan seperti apa bagian dalam dari cloud jaringan itu. Jaringan cloud hanyalah sarana untuk membawa data dari pengirim ke tujuan.

Topik yang diperkenalkan di sisa bab ini—cloud jaringan, perutean, dan kemacetan—ditangani oleh lapisan jaringan model arsitektur jaringan, terlepas dari apakah model tersebut TCP/IP atau model lainnya. Mari kita periksa topik cloud jaringan terlebih dahulu secara mendetail, lalu jelajahi perutean dan kemacetan.

Jenis awan jaringan

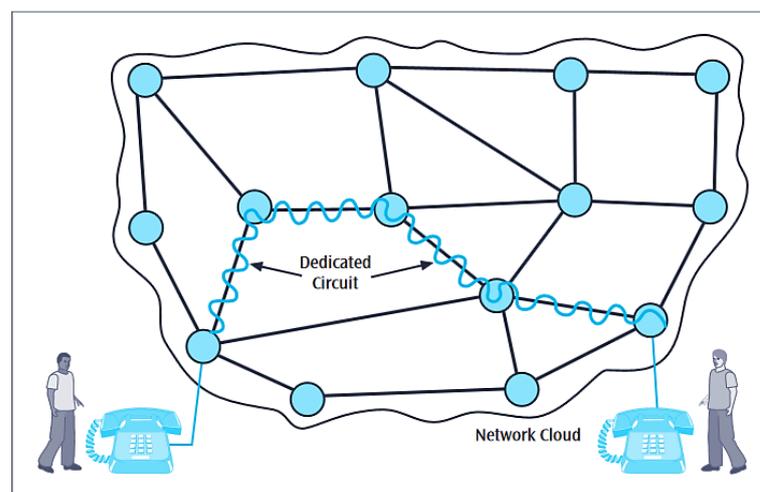
Cloud jaringan area luas dapat dikategorikan berdasarkan cara transfer informasi dari satu ujung cloud ke ujung lainnya. Tiga tipe dasar cloud adalah Circuit-switched, Packet-switched, dan Broadcast. Mari kita periksa satu per satu. Untuk mempermudah, kami akan menyebutnya sebagai jaringan.

Jaringan Circuit-Switched

Jaringan Circuit-switched adalah jaringan cloud di mana sirkuit khusus dibuat antara pengirim dan penerima, dan semua data melewati sirkuit ini. Salah satu contoh terbaik dari jaringan Circuit-switched adalah sistem telepon dial-up Amerika Utara pada abad ke-20. Ketika seseorang melakukan panggilan pada jaringan telepon dial-up, suatu sirkuit, atau jalur, dibuat antara orang yang melakukan panggilan dan penerima panggilan. Sirkuit fisik ini unik, atau didedikasikan, untuk satu panggilan ini dan ada selama panggilan berlangsung. Informasi (percakapan telepon) mengikuti jalur khusus ini dari node ke node dalam jaringan, seperti yang ditunjukkan pada Gambar 9-7.

Ketika panggilan telepon dilakukan melalui jaringan Circuit-Switched, jaringan memerlukan waktu untuk membangun sirkuit dan menghancurkan sirkuit. Namun begitu sirkuit terbentuk, semua data selanjutnya berpindah dengan cepat dari satu node ke node lainnya. Jaringan Circuit-Switched mempunyai dua kelemahan utama. Pertama, setiap sirkuit didedikasikan hanya untuk satu koneksi. Kedua, ketika sirkuit digunakan untuk mentransfer data (dibandingkan dengan suara), sirkuit tersebut mungkin tidak digunakan sepenuhnya karena transfer data komputer sering kali dilakukan secara sporadis.

Meskipun penggunaan jaringan Circuit-switched tersebar luas sepanjang abad kedua puluh, semua jaringan Circuit-Switched di Amerika Utara yang mendukung jaringan telepon umum telah digantikan dengan desain jaringan yang lebih efisien: jaringan packet-switched. Meskipun demikian, jaringan Circuit-Switched masih ada di jaringan swasta tertentu dan di beberapa negara di luar Amerika Utara, oleh karena itu kita perlu terus mempelajari jaringan Circuit-Switched, setidaknya untuk sementara waktu.



Gambar 9-7 Dua orang melakukan percakapan telepon menggunakan jaringan Circuit-Switched

Jaringan Beralih Paket

Jaringan packet-switched awalnya dibuat untuk mentransfer data komputer, bukan panggilan telepon. Saat ini, jaringan packet-switched membawa segala bentuk data, termasuk suara dan video. Dalam jaringan packet-switched, semua pesan data ditransmisikan menggunakan paket berukuran tetap, yang disebut paket, dan tidak ada jalur fisik unik dan khusus yang dibuat untuk mengirimkan paket data melintasi subjaringan. (Untuk membedakan antara sebagian data yang diproses pada lapisan data link dan sebagian data yang diproses pada lapisan jaringan, istilah “frame” digunakan pada lapisan data link, dan istilah “paket” digunakan pada lapisan jaringan). lapisan kerja.) Jika pesan yang akan ditransfer berukuran besar, pesan tersebut dipecah menjadi beberapa paket. Ketika beberapa paket tiba di tujuan, mereka disusun kembali menjadi pesan aslinya.

Dua jenis jaringan packet-switched adalah datagram dan sirkuit virtual. Dalam jaringan packet-switched datagram, setiap paket data dapat mengikuti jalurnya sendiri, yang mungkin unik, melalui cloud. Ketika setiap paket tiba di sebuah node, keputusan dibuat mengenai jalur mana yang akan diikuti paket selanjutnya. Pengambilan keputusan yang dinamis ini memungkinkan adanya fleksibilitas yang besar jika jaringan mengalami kemacetan atau kegagalan. Misalnya, jika sekelompok paket data sedang dirutekan melalui Dallas dalam perjalanan ke Phoenix, dan Dallas mengalami masalah router, jaringan dapat merutekan ulang paket tersebut melalui Denver. Masalah dengan jaringan datagram adalah ketika sekelompok besar paket dialamatkan ke tujuan yang sama, node jaringan harus memeriksa setiap paket satu per satu dan menentukan jalur berikutnya dari setiap paket. Hal ini dapat menyebabkan inefisiensi, atau hanya membuang-buang waktu.

Untuk mengatasi masalah ini, jaringan packet-switched sirkuit virtual telah dibuat. Dalam jaringan packet-switched sirkuit virtual, semua paket yang termasuk dalam koneksi logis dapat mengikuti jalur yang sama melalui jaringan. Misalnya, satu stasiun mungkin ingin mentransfer data dalam jumlah besar, seperti seluruh isi elektronik sebuah buku, melalui jaringan ke stasiun lain. Untuk mencapai hal ini, sirkuit virtual memecah sejumlah besar data menjadi n paket dan menentukan jalur sementara yang optimal melalui jaringan. Setiap router di sepanjang jalur kemudian diberitahu bahwa ia akan berpartisipasi dalam sirkuit virtual tertentu. Ketika data tiba dengan alamat sirkuit virtual tertentu, router hanya mengirimkan data keluar dari koneksi router yang terkait dengan sirkuit virtual tersebut. Ketika transfer data selesai, jalur sementara dibubarkan (yaitu, setiap router membuang informasi sirkuit virtual tersebut). Jenis jaringan packet-switched ini disebut sirkuit virtual karena jalur yang diikuti oleh paket-paket tersebut bertindak seperti sirkuit namun bukan sirkuit fisik aktual seperti sirkuit telepon.

Meskipun jenis jaringan ini terdengar mirip dengan jaringan Circuit-switched, karena semua paket data mengikuti jalur tetap, namun secara substansial berbeda. Jalur dalam jaringan packet-switched sirkuit virtual hanya ada di perangkat lunak dan hanya ketika jaringan membuat tabel perutean yang diperlukan pada node yang sesuai. Tabel routing ini mirip dengan tabel port yang digunakan oleh switch untuk menentukan jalur melalui jaringan area lokal. Perbedaan lain antara sirkuit virtual dan jaringan sirkuit-switched adalah bahwa

jalur dalam jaringan sirkuit virtual dapat digunakan bersama oleh lalu lintas lainnya. Untuk menghargai pentingnya hal ini, ingatlah bahwa ketika Anda melakukan panggilan pada jaringan Circuit-switched, Anda memiliki sirkuit khusus dari satu ujung sambungan ke ujung lainnya. Jadi, jika Anda dapat melihat data saat bergerak melalui kabel di sirkuit Anda, Anda akan melihat bahwa satu-satunya data di sirkuit ini adalah data Anda. Sebaliknya, setiap pengguna dalam jaringan sirkuit virtual berbagi satu atau lebih sirkuit dengan pengguna lain. Jika Anda dapat melihat kabel di sirkuit ini, Anda mungkin melihat data dari beberapa pengguna, atau data dari satu pengguna, lalu pengguna lainnya, berjalan melintasi jaringan. Dengan demikian, berbagai kabel yang membentuk sebuah sirkuit dalam jaringan sirkuit virtual membawa aliran data dari banyak pengguna, dan perangkat lunak yang menjaga setiap aliran data terpisah dari yang lain.

Ringkasnya, jaringan packet-switched memecah catatan data komputer, transmisi suara telepon, dan download video menjadi paket-paket berukuran tetap dan mengirimkan paket-paket ini melalui jaringan yang digunakan bersama oleh banyak pengguna. Dalam jaringan packet-switched datagram, setiap paket merupakan suatu entitas tersendiri. Ketika sebuah pesan besar telah dipecah menjadi n paket, setiap paket dalam jaringan datagram memasuki sebuah node, dimana keputusan routing yang unik dibuat. Karena tidak ada sirkuit tetap yang harus diikuti, jaringan tidak menghabiskan waktu dalam membuat sirkuit. Namun, waktu dihabiskan untuk menentukan rute setiap paket. Meskipun demikian, jaringan datagram cukup fleksibel karena dapat bereaksi dengan cepat terhadap perubahan jaringan. Jenis lain dari jaringan packet-switched, yaitu jaringan packet-switched sirkuit virtual, merupakan gabungan dari jaringan packet-switched dan jaringan Circuit-switched. Ketika sebuah pesan besar di jaringan ini dipecah menjadi beberapa paket, semua paket ini mengikuti jalur yang sama melalui jaringan. Jalur ini ditentukan sebelum paket pertama dikirim—suatu aktivitas yang memerlukan waktu pengaturan sirkuit—dan sirkuit virtual, dengan tabel perutean internalnya, membantu merutekan paket dari sumber ke tujuan.

Perusahaan telepon Sprint pertama kali mengumumkan pada tahun 2003 bahwa mereka mulai mengganti jaringan circuit-switched dengan jaringan packet-switched. Sejak itu, perusahaan telepon lain pun mengikuti jejaknya. Penggunaan jaringan packet-switched dalam transmisi percakapan telepon melibatkan digitalisasi data suara dan mengubahnya menjadi paket-paket. Setelah data suara berbentuk paket, data tersebut dapat ditransfer melalui jaringan packet-switched bersama dengan data dan video. Jenis konversi ini akan menghasilkan komunikasi yang lebih ekonomis karena semua bentuk data yang dikirimkan akan berbagi satu bentuk jaringan. Salah satu kendala terbesar dalam menggunakan jaringan packet-switched untuk mentransfer suara (yaitu, untuk membuat panggilan telepon) adalah bahwa beberapa jaringan packet-switched seperti Internet tidak selalu merupakan yang terbaik untuk mengirimkan paket suara secara real-time pada a secara konsisten dan, oleh karena itu, percakapan suara dapat terputus. Jika Anda adalah perusahaan komunikasi yang berharap menawarkan layanan baru atau alternatif, hal ini dapat mengakibatkan pelanggan tidak puas dan, akibatnya, kerugian bisnis.

Jaringan Broadcast

Seperti halnya sebuah node dalam desain siaran di sebagian besar jaringan area lokal, ketika sebuah node di jaringan siaran jaringan area luas mengirimkan datanya, data tersebut diterima oleh semua node lainnya. Bentuk jaringan area luas ini, pada saat ini, relatif jarang. Namun, beberapa sistem sudah ada. Sistem ini menggunakan frekuensi radio untuk menyiarkan data ke semua stasiun kerja dan biasanya beroperasi sebagai jaringan siaran radio di daerah pedesaan atau di daerah di mana terdapat banyak pulau yang dikelilingi oleh perairan besar. Beberapa layanan akses Internet nirkabel baru seperti Wi-Max (Bab Tiga) juga didasarkan pada jaringan siaran, namun lebih sering dianggap sebagai jaringan area metropolitan daripada jaringan area luas. Karena jaringan penyiaran tidak umum seperti jaringan Circuit-Switched dan Packet-Switched, maka pembahasan selanjutnya dalam bab ini tidak akan mencakup keduanya.

Singkatnya, desain fisik jaringan area luas, atau jaringan cloud-nya, memiliki tiga bentuk dasar: switch sirkuit, paket switch (datagram dan sirkuit virtual), dan siaran. Karakteristik bentuk-bentuk ini dirangkum pada Tabel 9-1. Perhatikan bagaimana jaringan sirkuit-switched dan sirkuit virtual memerlukan waktu pengaturan jalur dan tidak dapat merutekan ulang paket secara dinamis jika terjadi masalah jaringan. Perlu juga dicatat dari Tabel 9-1 bahwa jaringan Circuit-Switched dirancang terutama untuk sinyal suara dan merupakan satu-satunya jaringan yang menawarkan jalur khusus.

Tabel 9-1 Ringkasan karakteristik jaringan cloud

Karakteristik	Circuit Switched	Datagram Paket Switched	Sirkuit Virtual paket Switched	Broadcast
Waktu penyiapan jalur?	Ya	Tidak	Ya	Tidak
Keputusan perutean untuk setiap paket?	Tidak	Ya	Tidak	Biasanya Tidak
Jalur khusus?	Ya	Tidak	Tidak	Tidak
Bisakah perutean ulang secara dinamis jika terjadi masalah?	Tidak	Ya	Tidak	Biasanya Tidak
Koneksi yang didedikasikan untuk transfer Anda saja?	Ya	Tidak	Tidak	Tidak

Setelah memeriksa desain fisik jaringan area luas, sekarang mari kita mengalihkan perhatian kita ke desain logisnya.

Aplikasi jaringan berorientasi koneksi vs. tanpa koneksi

Jaringan cloud dari jaringan area luas adalah infrastruktur fisik dan karenanya terdiri dari node (router atau switch) dan berbagai jenis media interkoneksi. Bagaimana dengan entitas logis yang beroperasi pada infrastruktur fisik ini? Entitas logis ini sering kali berbentuk aplikasi perangkat lunak. Misalnya, jika Anda menggunakan aplikasi email untuk mengirim pesan ke teman di seluruh negeri, aplikasi email tersebut adalah entitas logis yang menggunakan infrastruktur fisik jaringan atau cloud untuk menyampaikan pesan. Banyak jenis

aplikasi berbeda yang ditemukan di jaringan area luas, termasuk email, penelusuran web, dan aplikasi komersial lainnya. Mari kita kategorikan semua aplikasi jaringan, atau entitas logis, ke dalam dua kategori dasar: aplikasi berorientasi koneksi dan aplikasi tanpa koneksi.

Aplikasi jaringan berorientasi koneksi, misalnya aplikasi yang melakukan transfer file menggunakan FTP, memberikan jaminan bahwa informasi yang melewati jaringan tidak akan hilang dan paket informasi akan dikirimkan ke penerima yang dituju dengan urutan yang sama. Mereka ditularkan. Dengan demikian, aplikasi jaringan yang berorientasi koneksi menyediakan apa yang disebut layanan yang dapat diandalkan. Untuk menyediakan layanan yang andal, jaringan memerlukan koneksi logis yang dibuat antara dua titik akhir. Jika perlu, negosiasi koneksi dilakukan untuk membantu menjalin koneksi ini.

Misalnya, pertimbangkan skenario berikut: Sebuah bank ingin mentransfer sejumlah besar uang secara elektronik ke bank kedua. Bank pertama membuat koneksi dengan bank kedua. Sebagai bagian dari membangun hubungan ini, kedua bank setuju untuk mentransfer dana menggunakan enkripsi data. Setelah bank pertama mengirimkan permintaan transfer, bank kedua memeriksa keakuratan permintaan tersebut dan mengembalikan pengakuan ke bank pertama. Bank pertama akan menunggu sampai pengakuan tiba sebelum melakukan hal lain. Semua paket yang ditransfer selama periode ini adalah bagian dari koneksi ini dan diakui keakuratannya. Jika ini adalah satu-satunya transfer elektronik, bank pertama akan mengucapkan selamat tinggal, dan bank kedua akan mengucapkan selamat tinggal. Perhatikan bahwa jenis subjaringan yang digunakan dalam proses transfer ini bukan merupakan masalah yang relevan. Jaringannya bisa saja berupa Circuit Switched atau Packet Switched. Semua aplikasi yang diperlukan hanyalah koneksi yang andal yang dapat digunakan untuk mentransfer dana. Anda dapat melakukan permintaan perbankan online (yaitu, menggunakan aplikasi jaringan berorientasi koneksi) melalui jaringan area lokal (jaringan packet-switched) di kantor atau sekolah, sama seperti Anda dapat melakukannya melalui sambungan telepon dial-up (a jaringan Circuit-switched) dari rumah.

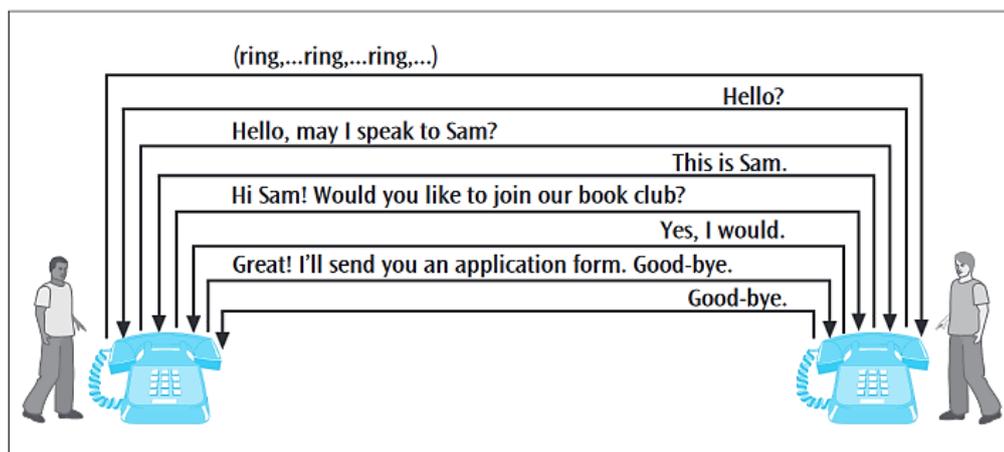
Aplikasi jaringan tanpa koneksi tidak memerlukan koneksi logis yang dibuat sebelum transfer data. Dengan demikian, aplikasi connectionless tidak menjamin terkirimnya informasi atau data apa pun. Data mungkin hilang, tertunda, atau bahkan terduplikasi. Tidak ada prosedur pembuatan atau penghentian koneksi yang diikuti karena tidak perlu membuat koneksi. Setiap paket dikirim sebagai satu kesatuan dan bukan sebagai bagian dari koneksi jaringan.

Contoh umum dari aplikasi jaringan tanpa koneksi adalah DNS, sebuah program yang mengubah URL, seperti www.cdm.depaul.edu menjadi alamat IP. Saat Anda meminta halaman Web menggunakan URL-nya, tidak ada koneksi yang dibuat antara Anda dan sistem DNS. Anda cukup mengklik tombol browser, dan kemudian DNS mengubah URL permintaan menjadi alamat IP dan mengirimkan permintaan tersebut. Aplikasi tanpa koneksi tidak menegosiasikan koneksi, dan transfer data jarang, jika pernah, diakui. Selain itu, jika Anda mengirim permintaan URL kedua, permintaan tersebut tidak ada hubungannya (dari segi jaringan) dengan permintaan URL pertama. Seperti halnya aplikasi jaringan berorientasi koneksi, cloud jaringan yang mendasari aplikasi tanpa koneksi, sekali lagi, tidak terlalu menjadi

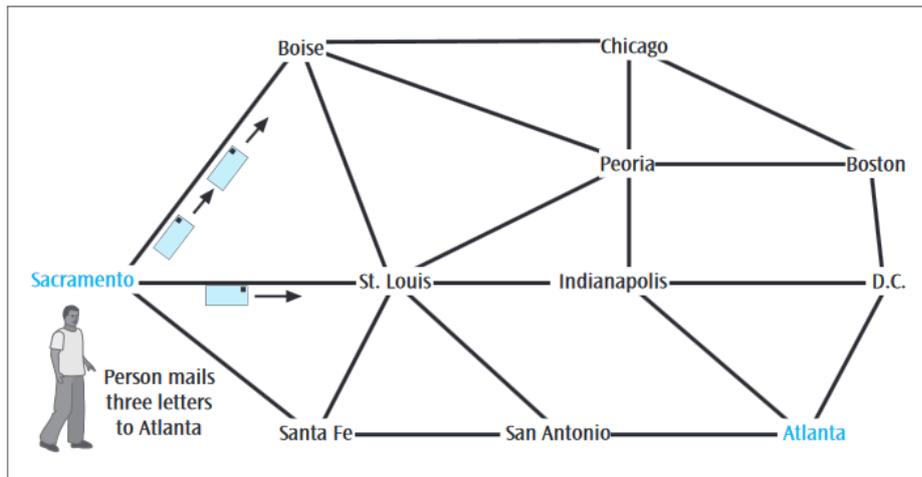
masalah. Ini bisa berupa jaringan Circuit-switched atau jaringan packet-switched. Anda dapat mengirim permintaan URL dari kantor atau sekolah melalui jaringan area lokal (packet-switched network), sama seperti yang Anda dapat dari rumah melalui koneksi dial-up (circular-switched network).

Contoh bagus lainnya yang menggambarkan perbedaan antara jaringan berorientasi koneksi dan jaringan tanpa koneksi adalah hubungan antara sistem telepon dan layanan pos. Saat Anda menelepon seseorang, orang tersebut akan menjawab telepon jika dia ada. Setelah telepon dijawab, sambungan dibuat. Percakapan menyusul, dan ketika salah satu orang telah selesai dengan percakapan tersebut, semacam pernyataan akhir dikeluarkan, kedua belah pihak menutup telepon, dan sambungan diakhiri (Gambar 9-8). Jadi, ketika Anda menggunakan sistem telepon, Anda menggunakan jaringan berorientasi koneksi yang menyediakan layanan yang dapat diandalkan.

Sebaliknya, jika Anda mengirim surat standar kepada seseorang melalui Layanan Pos AS, kemungkinan besar surat tersebut akan terkirim, namun tidak ada jaminan. Juga tidak ada jaminan kapan akan tiba. Jika surat itu hilang, Anda tidak akan mengetahuinya sampai beberapa waktu berlalu dan Anda mulai berpikir, “Saya belum mendengar kabar dari Kathleen; apakah dia menerima suratku?” Oleh karena itu, layanan pos mirip dengan jaringan tanpa koneksi yang menyediakan (tidak bermaksud menyinggung) layanan yang tidak dapat diandalkan. Layanan tidak dapat diandalkan yang ditawarkan oleh “jaringan” pos tanpa koneksi mengharuskan Anda mengambil tindakan tambahan jika Anda ingin memastikan bahwa surat terkirim sebagaimana dimaksud. Selain itu, pelindung pos tidak pernah mengetahui secara pasti rute mana yang akan dilalui surat melalui jaringan pos. Dalam keadaan tertentu, surat ditransfer dengan truk; dalam keadaan lain, itu ditransfer melalui pesawat terbang (Gambar 9-9).



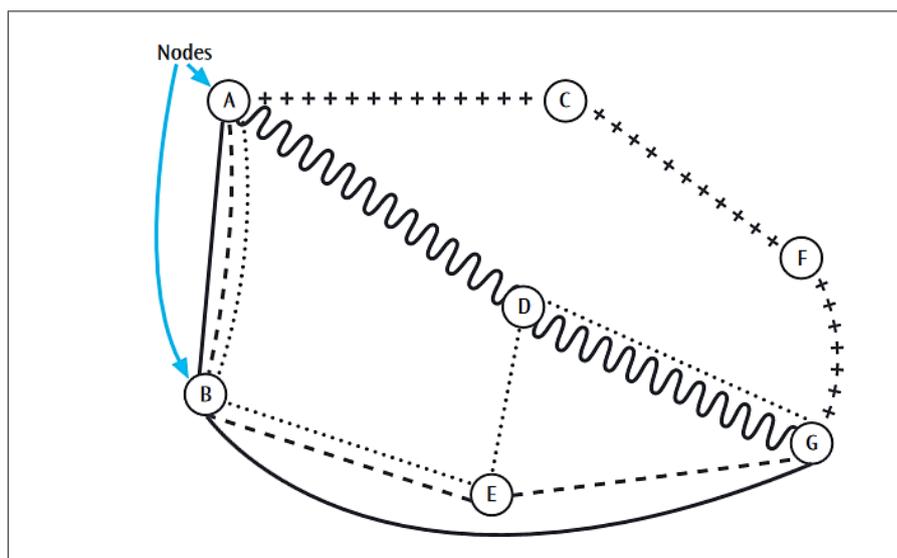
Gambar 9-8 Panggilan telepon berorientasi koneksi



Gambar 9-9 Jaringan pos tanpa koneksi

9.4 RUTE

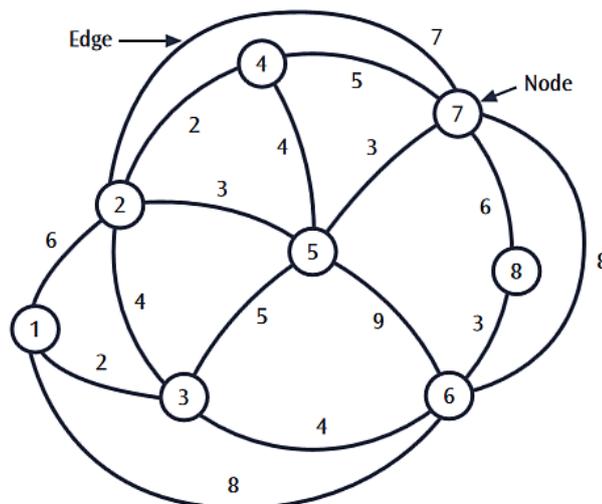
Ingatlah bahwa cloud jaringan yang mendasari jaringan area luas terdiri dari beberapa node, masing-masing dengan beberapa kemungkinan koneksi ke node lain dalam jaringan. Setiap node merupakan router yang menerima paket masukan, memeriksa alamat tujuan paket tersebut, dan meneruskan paket tersebut ke jalur komunikasi tertentu. Dalam kasus node multi-link, mungkin ada satu atau lebih jalur menuju sebuah node dan juga satu atau lebih jalur keluar dari sebuah node. Jika sebagian besar node dalam jaringan memiliki banyak input dan output, mungkin ada banyak rute dari node sumber ke node tujuan. Dengan memperhatikan Gambar 9-10, Anda dapat melihat bahwa sejumlah rute yang mungkin dilakukan antara Node A dan Node G: A-B-G, A-D-G, A-B-E-G, dan A-B-E-D-G, adalah beberapa di antaranya.



Gambar 9-10 Jaringan tujuh node menunjukkan beberapa rute antar node

Bagaimana perutean melalui jaringan area luas dilakukan? Pertimbangkan Internet sebagai contoh: Internet adalah kumpulan besar jaringan, router, dan jalur komunikasi. Ketika sebuah paket data memasuki router, router memeriksa alamat IP yang dikemas dalam lapisan jaringan paket tersebut dan menentukan ke mana paket tersebut harus pergi selanjutnya. Ketika ada beberapa rute melalui jaringan seperti Internet, bagaimana cara memilih satu rute tertentu? Meskipun perutean di Internet cukup rumit, teknik perutean dasar yang digunakan semua jenis jaringan area luas dapat diperiksa. Namun perlu diingat bahwa jaringan area luas tidak hanya menggunakan satu bentuk routing. Algoritma perutean yang digunakan dalam Internet, misalnya, sebenarnya merupakan kombinasi dari beberapa jenis teknik perutean dasar.

Untuk mulai memahami masalah perutean yang seringkali rumit, akan berguna jika kita membayangkan jaringan cloud sebagai grafik yang terdiri dari node (komputer, router, atau switch) dan edge (hubungan komunikasi antar node), seperti yang ditunjukkan pada Gambar 9-11. Dalam grafik jaringan ini, tepi antara masing-masing pasangan node dapat diberi bobot atau biaya terkait, seperti yang telah dilakukan pada Gambar 9-11, untuk membentuk struktur yang disebut grafik jaringan berbobot.



Gambar 9-11 Contoh sederhana grafik jaringan

Anda dapat menetapkan banyak arti pada bobot dalam grafik jaringan berbobot. Misalnya, bobot dapat disesuaikan dengan biaya penggunaan hubungan komunikasi antara dua node. Bobot juga dapat mewakili biaya waktu tunda yang terkait dengan transmisi data pada hubungan antara node sumber dan tujuan. Faktor lain yang umumnya direpresentasikan sebagai bobot adalah ukuran antrian yang telah dicadangkan saat menunggu paket dikirim ke suatu link. Masing-masing bobot ini mungkin berguna untuk menentukan rute melalui jaringan.

Setelah Anda mempertimbangkan cloud jaringan sebagai grafik dan menetapkan bobot pada jalur antar node, Anda dapat mengembangkan algoritme untuk melintasi jaringan. Faktanya, ada banyak algoritma untuk memilih rute melalui jaringan. Seringkali, algoritme

berupaya mendapatkan rute optimal melalui jaringan, namun ada cara berbeda untuk mendefinisikan “optimal”. Misalnya, suatu algoritme mungkin mendefinisikan rute optimal sebagai rute yang menghasilkan biaya paling sedikit. Algoritma lain mungkin menganggap jalur dengan waktu tunda paling sedikit sebagai rute optimal. Algoritma ketiga mungkin mendefinisikan rute optimal sebagai rute yang memiliki panjang antrian terkecil pada node di sepanjang jalur.

Beberapa algoritma menggunakan kriteria selain optimalitas. Misalnya, mereka mungkin mencoba menyeimbangkan beban jaringan melalui sejumlah jalur berbeda. Algoritme jenis lain mungkin lebih menyukai satu jenis lalu lintas dibandingkan jenis lalu lintas lainnya—misalnya, lalu lintas waktu nyata dibandingkan lalu lintas non-waktu nyata. Tipe ketiga mungkin mencoba untuk tetap kuat, menanggapi perubahan tuntutan jaringan ketika node dan jalur komunikasi gagal atau menjadi padat. Namun jenis keempat mungkin mencoba untuk tetap statis dan tidak beralih di antara jalur-jalur yang memungkinkan. Seperti yang Anda lihat, perutean adalah topik yang rumit.

Untuk memahami perutean dalam jaringan area luas, mari kita periksa beberapa algoritme perutean yang paling umum digunakan (algoritme berbiaya paling rendah dan banjir Dijkstra) dan beberapa teknik untuk mengelola informasi perutean (perutean terpusat versus terdistribusi; perutean adaptif versus perutean tetap). Sebagian besar jaringan area luas menggunakan kombinasi teknik perutean ini untuk mencapai algoritma perutean yang adil, efisien, dan kuat, namun pada saat yang sama stabil.

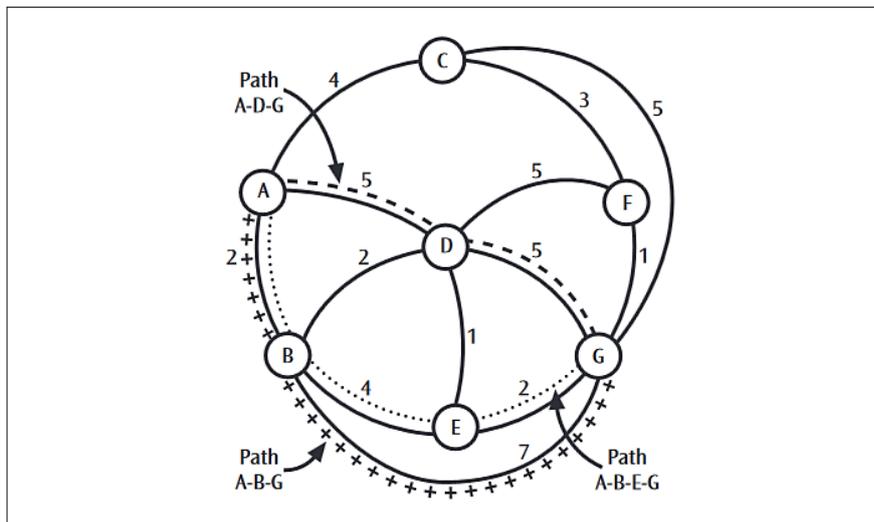
Algoritma Dijkstra yang berbiaya paling rendah

Salah satu metode yang mungkin untuk memilih rute melalui jaringan adalah dengan memilih rute yang meminimalkan jumlah biaya semua jalur komunikasi sepanjang rute tersebut. Algoritma klasik yang menghitung jalur berbiaya paling rendah melalui suatu jaringan adalah algoritma berbiaya paling rendah dari Dijkstra. Algoritme ini dijalankan oleh setiap node, dan hasilnya disimpan di node tersebut dan terkadang dibagikan ke node lain. Karena perhitungan ini memakan waktu, perhitungan ini hanya dilakukan secara periodik atau ketika sesuatu dalam jaringan berubah—misalnya, ketika ada koneksi atau kegagalan node.

Mari kita lihat sebuah contoh. Gambar 9-12 menggambarkan cloud jaringan yang sama seperti yang ditunjukkan pada Gambar 9-10, namun telah dimodifikasi untuk menyertakan serangkaian biaya terkait pada setiap link. Jalur A-B-G memiliki biaya 9 ($2+7$), A-D-G memiliki biaya 10 ($5+5$), dan jalur A-B-E-G memiliki biaya 8 ($2+4+2$). Untuk memastikan bahwa Anda menemukan rute yang paling murah, Anda perlu menggunakan prosedur yang menghitung biaya setiap rute yang mungkin, dimulai dari node tertentu. Meskipun mata manusia dapat dengan cepat memilih jalur melalui grafik jaringan, ada sejumlah kelemahan dalam “mengamati” data untuk menemukan solusi:

- Anda dapat dengan mudah melewati satu atau lebih jalur.
- Anda mungkin tidak menemukan jalur yang paling murah.
- Jaringan area luas tidak pernah sesederhana jaringan pada Gambar 9-12; oleh karena itu, mengamati data tidak akan pernah bisa dipertahankan sebagai prosedur jangka panjang yang andal.

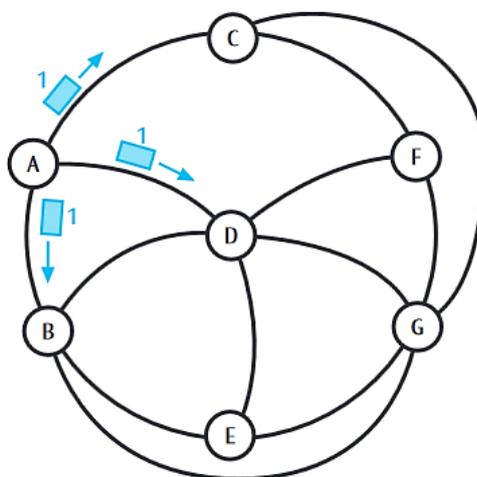
Sebagian besar jaringan area luas menggunakan beberapa bentuk algoritma Dijkstra untuk menentukan rute dengan biaya paling rendah melalui suatu jaringan, baik biaya tersebut merupakan ukuran waktu atau uang.



Gambar 9-12 Jaringan dengan biaya yang terkait dengan setiap link

Flood

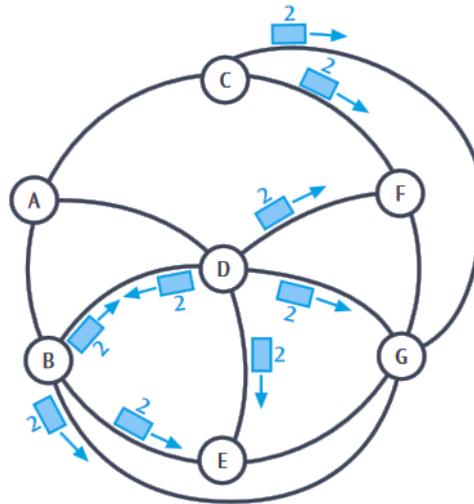
Dibandingkan dengan algoritma routing Dijkstra yang berbiaya paling rendah, teknik banjir tampak sederhana. Flooding menyatakan bahwa setiap node mengambil paket masuk dan mengirimkannya kembali ke setiap link keluar. Misalnya, asumsikan sebuah paket berasal dari Node A, seperti yang ditunjukkan pada Gambar 9-13. Node A hanya mengirimkan salinan paket pada setiap link keluarnya. Jadi, salinan paket (salinan pertama, atau salinan 1) dikirim ke Node B, C, dan D.



Gambar 9-13 Jaringan yang terendam banjir, dimulai dari Node A

Ketika paket tiba di Node B, B cukup mengirimkan salinan paket tersebut ke masing-masing node keluarnya (D, E, dan G). Demikian pula Node C akan mengirimkan salinan paket

ke masing-masing node keluarannya (F dan G). Node D juga akan mengirimkan salinan paket ke masing-masing node keluarannya (B, E, F, dan G). Gambar 9-14 menunjukkan salinan kedua dari paket yang meninggalkan Node B, C, dan D. Tidak perlu waktu lama bagi Anda untuk menyadari bahwa jaringan akan dengan cepat dibanjiri salinan paket data asli.



Gambar 9-14 Banjir terus berlanjut hingga Node B, C, dan D

Untuk mencegah jumlah paket yang disalin menjadi terlalu banyak, dua aturan yang masuk akal dapat dibuat. Pertama, sebuah node tidak perlu mengirim salinan paket kembali ke link asal paket tersebut tiba. Jadi, ketika Node A mengirimkan salinan paket ke Node C, C tidak perlu segera mengirimkannya kembali ke A.

Kedua, batas jaringan, yang disebut batas hop, dapat ditempatkan pada berapa kali suatu paket disalin. Setiap kali sebuah paket disalin, penghitung yang terkait dengan paket tersebut bertambah sebesar 1. Penghitung ini disebut jumlah hop. Ketika jumlah hop sama dengan batas hop jaringan, paket khusus ini tidak akan disalin lagi. Misalnya, jaringan mempunyai batas hop sebesar 3. Ketika Node A pertama kali mengirimkan salinan ke B, C, dan D, masing-masing dari ketiga salinan tersebut memiliki jumlah hop sebesar 1. Ketika paket tiba di Node C, salinan dengan hop hitungan 2 akan dikirim ke F dan G (Gambar 9-14). Ketika salinan tiba di Node F, dua salinan dengan jumlah hop 3 akan dikirim ke D dan G, dan paket yang tiba di D dan G dengan jumlah hop 3 tidak akan dikirim lebih jauh.

Meskipun banjir mungkin tampak seperti cara yang aneh untuk merutekan paket melalui jaringan, prosedur ini memiliki manfaatnya. Jika salinan sebuah paket harus dikirim ke node tertentu, banjir akan membawanya ke sana—tentu saja dengan asumsi, setidaknya ada satu link aktif ke node penerima, dan batas hop jaringan tidak ditetapkan pada nilai yang terlalu kecil. . Flooding juga bermanfaat ketika salinan paket perlu sampai ke semua node—misalnya, ketika informasi darurat atau informasi inisialisasi jaringan dikirim. Kerugian utama dari banjir adalah banyaknya jumlah paket yang disalin yang didistribusikan ke seluruh jaringan.

Perutean terpusat vs. terdistribusi

Perutean terpusat dan terdistribusi bukanlah algoritma untuk merutekan paket data melalui jaringan, melainkan merupakan teknik untuk menyediakan informasi perutean. Perutean terpusat melibatkan penyimpanan semua informasi perutean di satu lokasi pusat (Tabel 9-2). Setiap kali router mana pun dalam jaringan memerlukan informasi perutean, lokasi pusat ini akan ditanyakan dan hasil perutean dikembalikan. Misalnya, jika sebuah paket tiba di Node A dan ditujukan ke Node G, Tabel 9-2 menunjukkan bahwa paket tersebut harus dikirim ke Node B berikutnya. Saat ini, perutean terpusat jarang digunakan di jaringan area luas. Sebaliknya, sebagian besar jaringan area luas sekarang menggunakan perutean terdistribusi. Perutean terdistribusi adalah teknik yang menggunakan algoritme perutean, seperti algoritme berbiaya paling rendah, untuk menghasilkan informasi perutean dan menentukan bahwa informasi ini disimpan (dalam bentuk tabel perutean) di lokasi terdistribusi—biasanya, router—di dalam jaringan. Ketika sebuah paket data memasuki jaringan pada node x , node tersebut berkonsultasi dengan tabel routingsya sendiri untuk menentukan node berikutnya yang harus menerima paket tersebut. Dalam skema ini, setiap node memerlukan informasi routing hanya untuk lokalnya sendiri. Misalnya, Tabel 9-3 berisi tabel routing untuk Node C. Dari tabel ini, Anda dapat melihat bahwa jika sebuah paket data tiba di Node C dan ditujukan ke Node G, maka paket tersebut harus dikirim ke Node F selanjutnya. (Setelah paket tiba di Node F, tabel routing Node F harus diperiksa untuk hop berikutnya di jalur tersebut.)

Tabel 9-2 Tabel perutean disimpan di situs jaringan terpusat

		Node Tujuan						
		A	B	C	D	E	F	G
Node Sumber	A	-	B	C	B	B	C	B
	B	A	-	A	D	D	D	D
	C	A	A	-	A	F	F	F
	D	B	B	F	-	E	E	E
	E	D	D	G	D	-	G	G
	F	C	G	C	G	G	-	G
	G	E	E	F	E	E	F	-

Salah satu keuntungan utama dari routing terdistribusi adalah kenyataan bahwa tidak ada satu node (atau router pusat) yang bertanggung jawab untuk memelihara semua informasi routing. Situasi ini memberikan sejumlah manfaat. Pertama, jika ada node yang mogok, kemungkinan besar tidak akan menonaktifkan seluruh jaringan. Kedua, sebuah node tidak perlu mengirimkan permintaan ke router pusat karena setiap node memiliki tabelnya sendiri. Dengan (1) menghilangkan paket permintaan yang, dalam routing terpusat, dikirimkan ke node yang memegang tabel routing dan (2) menghilangkan paket-paket yang dihasilkan meninggalkan node tabel routing, routing terdistribusi menghilangkan sebagian besar lalu lintas data di jaringan. jaringan yang dapat dihasilkan oleh skema perutean terpusat.

Tabel 9-3 Tabel routing lokal untuk Node C

		Node Tujuan						
		A	B	C	D	E	F	G
Node Sumber	C	A	A	-	A	F	F	F

Salah satu kelemahan dari routing terdistribusi adalah terkait dengan masalah yang muncul jika tabel routing perlu diperbarui. Ketika semua informasi perutean ada di satu tempat (yaitu, dalam satu tabel), pembaruan menjadi mudah. Ketika informasi routing tersebar di seluruh jaringan, mendapatkan informasi routing yang tepat ke setiap node merupakan masalah yang kompleks. Konsekuensi lain dari menyimpan informasi perutean di beberapa lokasi adalah bahwa pada suatu titik waktu tertentu, mungkin ada satu atau lebih tabel perutean yang berisi informasi lama atau salah.

Routing Information Protocol (RIP)

Mari kita perhatikan contoh berikut tentang cara kerja Routing Information Protocol (RIP). Anggaplah Router A mempunyai koneksi ke empat jaringan (123, 234, 345, dan 789) dan mempunyai tabel routing terkini (Tabel 9-4):

Tabel 9-4 Tabel routing saat ini untuk Router A

Jaringan	Hop Cost	Next Router
123	8	B
234	5	C
345	6	C
789	10	D

Sekarang misalkan Router D mengirimkan informasi routing berikut (Tabel 9-5) (perhatikan bahwa Router D tidak mengirimkan informasi Router Berikutnya karena setiap router akan menentukan informasi itu sendiri):

Tabel 9-5 Informasi routing yang dikirim oleh Router D

Jaringan	Hop Cost
123	4
345	5
567	7
789	10

Router A akan melihat setiap entri di tabel Router D dan membuat keputusan berikut:

1. Router D mengatakan Jaringan 123 berjarak 4 hop (dari Router D). Karena Router D berjarak 1 hop dari Router A, Jaringan 123 sebenarnya berjarak 5 hop dari Router A. Itu lebih baik daripada entri 8 hop saat ini di tabel Router A, sehingga Router A akan
1. perbarui entri untuk Jaringan 123.

2. Router D mengatakan Jaringan 345 berjarak 6 hop (5 hop dari Router D ditambah 1 hop antara Router A dan Router D). Saat ini jumlah hop sama seperti yang ditunjukkan pada tabel Router A untuk Jaringan 345, sehingga Router A tidak akan memperbarui tabelnya.
3. Router D mengatakan Jaringan 567 berjarak 8 hop (7 hop dari Router D ditambah 1 hop antara Router A dan Router D). Karena Router A tidak mempunyai informasi tentang Jaringan 567, Router A akan menambahkan entri ini ke tabelnya. Dan karena informasinya berasal dari Router D, entri Router Berikutnya pada Router A untuk jaringan 567 diatur ke D.
4. Router D mengatakan Jaringan 789 berjarak 11 hop (10 hop dari Router D ditambah 1 hop antara Router A dan Router D), yang lebih buruk dari nilai pada tabel Router A. Biasanya kita akan mengabaikan informasi yang lebih buruk; tapi karena info terkini di tabel Router A untuk Jaringan 789 berasal dari Router D, dan Router D lah yang memberi kita informasi baru, kita perlu menggunakan informasi ini dan memperbarui tabel kita sesuai dengan itu.

Tabel routing Router A yang diperbarui akan terlihat seperti berikut (Tabel 9-6):

Tabel 9-6 Tabel routing yang diperbarui untuk Router A

Jaringan	Hop Cost	Next Router
123	5	D
234	5	C
345	6	C
567	8	D
789	10	D

Router A sekarang memiliki tabel routing yang diperbarui (berdasarkan informasi yang dikirim dari Router D). Ia telah menemukan jalur yang lebih pendek ke Jaringan 123 melalui Router D dan telah mengetahui bahwa Jaringan 567 berjarak 8 hop dari dirinya sendiri.

Perutean adaptif vs. tetap

Perutean terpusat dan terdistribusi adalah metode untuk mengirimkan informasi perutean. Mereka biasanya digunakan bersama dengan beberapa bentuk algoritma routing yang paling murah. Terlepas dari apakah informasi routing terpusat atau terdistribusi, ketika jaringan berubah, informasi routing juga perlu berubah.

Ketika tabel perutean beradaptasi dengan perubahan jaringan, sistem perutean disebut adaptif. Perutean adaptif adalah teknik dinamis di mana tabel perutean bereaksi terhadap fluktuasi jaringan, seperti kemacetan dan kegagalan node/link. Ketika masalah terjadi pada jaringan dengan routing adaptif, informasi yang sesuai dikirimkan ke tabel routing, dan rute baru dibuat untuk menghindari area masalah. Perutean adaptif menimbulkan beberapa pertanyaan dan permasalahan: Seberapa sering informasi harus dibagikan, dan seberapa sering tabel perutean harus diperbarui? Berapa banyak lalu lintas tambahan yang dihasilkan oleh pesan yang mengirimkan informasi perutean?

Sayangnya, perutean adaptif dapat menambah kemacetan jaringan. Setiap kali jaringan mengalami perubahan kemacetan, informasi tentang perubahan ini dikirimkan ke satu atau lebih node. Transmisi informasi ini menambah kemacetan, dan mungkin memperburuknya. Selain itu, jika jaringan bereaksi terlalu cepat terhadap masalah kemacetan dan mengalihkan semua lalu lintas ke jalur yang berbeda, hal ini dapat menimbulkan masalah kemacetan di area lain. Jaringan kemudian dapat mendeteksi kemacetan di area berbeda ini dan mungkin mengalihkan semua lalu lintas kembali ke area masalah pertama. Perutean ulang bolak-balik ini menghasilkan efek yo-yo, yang memengaruhi stabilitas jaringan dan menurunkan efisiensi.

Kebalikan dari perutean adaptif adalah perutean tetap. Dengan routing tetap, tabel routing dibuat satu kali, biasanya ketika jaringan diinstal, dan kemudian tidak pernah diperbarui lagi. Meskipun metode ini sederhana dan menghilangkan kebutuhan router untuk berkomunikasi satu sama lain (sehingga menghindari lalu lintas tambahan), metode ini juga dapat menghasilkan jaringan dengan informasi yang ketinggalan jaman sehingga perutean menjadi tidak efisien atau lambat. Masih menjadi perdebatan apakah perutean tetap ada lagi pada jaringan area luas (atau, dalam hal ini, pada jenis jaringan lainnya).

Contoh perutean

Internet dibahas secara rinci dalam Bab Sepuluh, tapi mari kita luangkan waktu beberapa menit untuk memeriksa dua algoritma routing yang telah digunakan dalam Internet selama bertahun-tahun. Dengan memeriksa algoritma ini, Anda akan melihat bagaimana protokol routing sebenarnya terdiri dari banyak algoritma dan teknik yang diperkenalkan pada bagian sebelumnya.

Algoritma perutean pertama yang digunakan di Internet (saat masih disebut ARPANET) disebut algoritma perutean vektor jarak. Algoritma perutean vektor jarak adalah algoritma adaptif di mana setiap node memelihara tabel perutean yang disebut vektor. Karena setiap node memelihara tabel routingnya sendiri, algoritma routing juga merupakan algoritma terdistribusi. Setiap 30 detik, setiap node menukar vektornya dengan tetangganya. Ketika semua vektor tetangganya masuk, sebuah node akan memperbarui vektornya sendiri dengan nilai biaya terendah dari semua tetangganya. Algoritme terdistribusi adaptif ini memiliki nama resmi Routing Information Protocol (RIP). Protokol ini memiliki dua efek samping yang tidak menguntungkan. Yang pertama adalah kabar baik (informasi perutean yang mengindikasikan jalur yang lebih pendek) bergerak relatif lambat melalui jaringan, satu router pada satu waktu. Efek samping kedua adalah berita buruk, seperti kegagalan router atau link, seringkali bergerak lebih lambat melalui jaringan.

Protokol routing berikutnya yang diimplementasikan di Internet (kira-kira pada tahun 1979) disebut algoritma routing link state. Perutean link state pada dasarnya melibatkan empat langkah. Langkah pertama adalah mengukur penundaan atau biaya untuk setiap router tetangga. Misalnya, setiap router dapat mengirimkan paket gema khusus yang akan segera dipantulkan kembali. Jika stempel waktu ditempatkan pada paket saat paket berangkat dan kembali, router akan mengetahui waktu transfer ke dan dari router tetangga. Langkah kedua adalah membuat paket link state yang berisi semua informasi waktu ini. Langkah ketiga adalah

mendistribusikan paket link state melalui banjir. Selain menggunakan banjir, algoritma routing link state merupakan algoritma terdistribusi. Langkah keempat dan terakhir adalah menghitung rute baru berdasarkan informasi terkini. Setelah router mengumpulkan satu set lengkap paket link state dari tetangganya, router tersebut membuat tabel routingnya, biasanya menggunakan algoritma berbiaya paling rendah dari Dijkstra. Protokol Open Shortest Path First (OSPF) adalah algoritma link state dan masih digunakan sampai sekarang oleh banyak router Internet. Untuk mempelajari lebih lanjut tentang algoritma ini, periksa kotak Detail berjudul “OSPF.”

Sekarang kita tahu bagaimana data dirutekan dalam jaringan, kita perlu melihat efek samping umum dari merutekan terlalu banyak data dalam satu waktu: kemacetan.

9.5 KECEPATAN JARINGAN

Ketika jaringan atau bagian dari jaringan menjadi terlalu jenuh dengan paket data sehingga transfer paket menjadi terhambat, kemacetan jaringan terjadi. Kemacetan mungkin disebabkan oleh masalah jangka pendek, seperti kegagalan link atau node sementara, atau mungkin karena masalah jangka panjang, seperti perencanaan yang tidak memadai untuk kebutuhan lalu lintas di masa depan atau tabel perutean dan pembuatan tabel perutean yang buruk. algoritma perutean. Seperti banyak hal dalam hidup, jaringan hanya akan sekuat tautan terlemahnya. Jika perancang jaringan dapat merencanakan masa depan dengan baik, kemacetan jaringan mungkin hanya terjadi dalam kasus yang jarang terjadi. Namun industri komputer, seperti kebanyakan industri lainnya, dipenuhi dengan contoh kegagalan dalam merencanakan masa depan dengan baik. Jaringan komputer akan mengalami kemacetan, dan tidak ada perencanaan yang dapat menghindari situasi ini. Oleh karena itu, penting untuk mempertimbangkan teknik penghindaran kemacetan dan penanganan kemacetan yang efektif.

Masalah yang terkait dengan kemacetan jaringan

Jaringan mengalami kemacetan karena berbagai alasan. Kegagalan jaringan—baik kegagalan pada tautan komunikasi antar node atau kegagalan node itu sendiri—dapat menyebabkan kemacetan jaringan. Jika jaringan tidak dapat dengan cepat mendeteksi titik kegagalan dan secara dinamis melakukan rute di sekitar titik ini, jaringan mungkin mengalami berbagai masalah kemacetan, mulai dari pelambatan kecil pada masing-masing link hingga jaringan kolaps total. Bahkan jika jaringan memulai proses perutean ulang, jaringan mungkin masih mengalami kemacetan karena tersedia satu jalur jaringan yang lebih sedikit. Namun kegagalan jalur komunikasi dan node bukan satu-satunya penyebab kemacetan.

Ruang buffer yang tidak mencukupi pada sebuah node dalam jaringan juga dapat menyebabkan kemacetan jaringan. Bukan hal yang aneh jika ratusan atau bahkan jutaan paket tiba di sebuah node jaringan setiap detiknya. Jika node tidak dapat memproses paket dengan cukup cepat, paket masuk akan mulai terakumulasi di ruang buffer. Ketika paket berada di buffer untuk jangka waktu yang cukup lama, throughput jaringan mulai terganggu. Jika routing adaptif digunakan, kemacetan ini dapat dikenali, dan tabel routing yang diperbarui dapat dikirim ke node yang sesuai (atau ke fasilitas routing pusat). Namun mengubah tabel routing

untuk membelokkan kemacetan mungkin hanya memberikan perbaikan sementara, jika memang ada perbaikan. Yang dibutuhkan adalah solusi yang lebih permanen. Dua kemungkinan solusi yang lebih permanen adalah meningkatkan kecepatan prosesor node yang bertanggung jawab memproses paket data yang masuk, dan meningkatkan jumlah ruang buffer di node. Sayangnya, penerapan kedua solusi ini mungkin memerlukan banyak waktu dan uang. Mungkin ada alternatif lain yang lebih murah.

Apa yang terjadi jika ruang buffer penuh dan node tidak dapat menerima paket tambahan? Di banyak sistem, paket yang tiba setelah ruang buffer penuh akan dibuang. Meskipun ini bukan solusi yang elegan, ini untuk sementara memecahkan masalah memiliki terlalu banyak paket. Sayangnya, ini seperti obat yang buruk: hanya mengobati gejalanya, tetapi tidak mengobati penyakitnya. Yang dibutuhkan adalah solusi yang bereaksi cepat terhadap kemacetan jaringan dan mengatasi masalah sebenarnya: terlalu banyak paket. Mari kita periksa beberapa kemungkinan solusi yang telah disarankan atau dicoba dalam beberapa tahun terakhir.

Kemungkinan solusi kemacetan

Solusi terhadap kemacetan jaringan umumnya terbagi dalam dua kategori berbeda. Kategori pertama berisi solusi yang diterapkan setelah kemacetan terjadi. Kategori solusi kedua berisi teknik-teknik yang berupaya menghindari kemacetan sebelum hal itu terjadi. Mari kita asumsikan bahwa kemacetan telah terjadi dan periksa solusi kategori pertama. Sebagian besar, jika tidak semua, solusi dalam kategori pertama melibatkan perintah kepada stasiun pemancar untuk memperlambat atau menghentikan transmisi paket ke dalam jaringan. Contohnya, jika sebuah aplikasi pada jaringan tiba-tiba menyadari bahwa paket-paketnya dibuang, aplikasi tersebut mungkin memberitahukan stasiun pemancar untuk memperlambat kecepatan hingga pemberitahuan lebih lanjut. Karena aplikasi hanya mengamati throughputnya sendiri dan tidak bergantung pada jenis sinyal khusus apa pun yang datang dari jaringan, hal ini disebut kontrol kemacetan implisit.

Seringkali, jaringan itu sendiri mengirimkan satu atau lebih sinyal ke stasiun pemancar, memberi tahu stasiun tersebut untuk memperlambat atau menghentikan penyisipan paket ke dalam jaringan. Ketika jaringan memberi sinyal kepada stasiun pemancar untuk melambat, hal ini disebut kontrol kemacetan eksplisit. Sebagai contoh, pertimbangkan frame relay (dibahas secara lebih rinci dalam Bab Sebelas), yang dirancang untuk menggunakan dua teknik pengendalian kemacetan eksplisit: pemberitahuan kemacetan eksplisit maju dan pemberitahuan kemacetan eksplisit mundur. Dengan pemberitahuan kemacetan eksplisit ke depan (FECN), ketika router frame relay mengalami kemacetan, ia mengirimkan sinyal kemacetan (di dalam bingkai data) ke stasiun tujuan, yang pada gilirannya memberitahu stasiun asal untuk memperlambat transfer data. Dengan pemberitahuan kemacetan eksplisit mundur (BECN), router frame relay yang mengalami kemacetan mengirimkan sinyal kembali ke stasiun asal, yang kemudian memperlambat transmisinya.

Metode pengendalian kemacetan lainnya didasarkan pada teknik yang lebih sederhana seperti metode pengendalian aliran (jendela geser) yang diperkenalkan pada Bab Enam. Kontrol aliran pada lapisan data link memungkinkan dua node yang berdekatan untuk

mengontrol jumlah lalu lintas yang lewat di antara keduanya. Ketika ruang buffer suatu node penuh, node penerima menginformasikan node pengirim untuk memperlambat atau menghentikan transmisi hingga pemberitahuan lebih lanjut. Kita akan melihat di Bab Sebelas bagaimana Internet menangani kontrol aliran end-to-end menggunakan perangkat lunak TCP. Seperti pada kontrol aliran node-to-node pada lapisan data link, penerima pada kontrol aliran end-to-end mengembalikan nilai ke pengirim yang memberi tahu pengirim untuk mempertahankan kecepatan saat ini, memperlambat, atau menghentikan transmisi paket.

Sekarang mari kita pertimbangkan teknik pengendalian kemacetan kategori kedua: teknik yang mencoba mencegah kemacetan bahkan sebelum hal itu terjadi. Pepatah lama mengatakan “Satu ons pencegahan bernilai satu pon pengobatan” tentu saja berlaku untuk jaringan komputer. Menghindari kemacetan tidak hanya menyebabkan lebih sedikit paket yang hilang dan tertunda, tetapi juga pelanggan yang lebih bahagia. Salah satu solusi yang mungkin untuk mengendalikan aliran paket antara dua node adalah buffer preallocation. Dalam praalokasi buffer, sebelum satu node mengirimkan serangkaian n paket ke node lain, node pengirim menanyakan terlebih dahulu apakah node penerima memiliki cukup ruang buffer untuk n paket. Jika node penerima mempunyai ruang buffer yang cukup, ia menyisihkan n buffer dan menginformasikan node pengirim untuk memulai transmisi. Meskipun skema ini secara umum berhasil, skema ini menimbulkan penyampaian pesan tambahan, penundaan tambahan, dan kemungkinan ruang buffer yang terbuang jika semua n paket tidak terkirim. Namun alternatifnya—membuang paket karena ruang buffer tidak mencukupi—lebih buruk lagi.

Mode Transfer Asinkron (ATM), yang dibahas lebih rinci di Bab Sebelas, mendekati kemacetan jaringan dengan cara yang sangat serius. Karena jaringan ATM mentransfer data dengan kecepatan sangat tinggi, kemacetan dapat terjadi dengan cepat dan sangat merugikan. Oleh karena itu, sangat penting untuk mencegah terjadinya kemacetan.

ATM menggunakan teknik penghindaran kemacetan yang tampaknya bekerja cukup baik. Teknik ini—kontrol penerimaan koneksi—menghindari kemacetan dengan mengharuskan pengguna bernegosiasi dengan jaringan mengenai berapa banyak lalu lintas yang akan mereka kirimkan, atau sumber daya apa yang harus disediakan jaringan untuk memenuhi kebutuhan pengguna sebelum pengguna mengirimkan data apa pun. Jika jaringan tidak dapat memenuhi permintaan pengguna, koneksi pengguna akan ditolak. Dalam menegosiasikan kelayakan koneksi, pengguna dan jaringan harus menyelesaikan pertanyaan-pertanyaan seperti berikut:

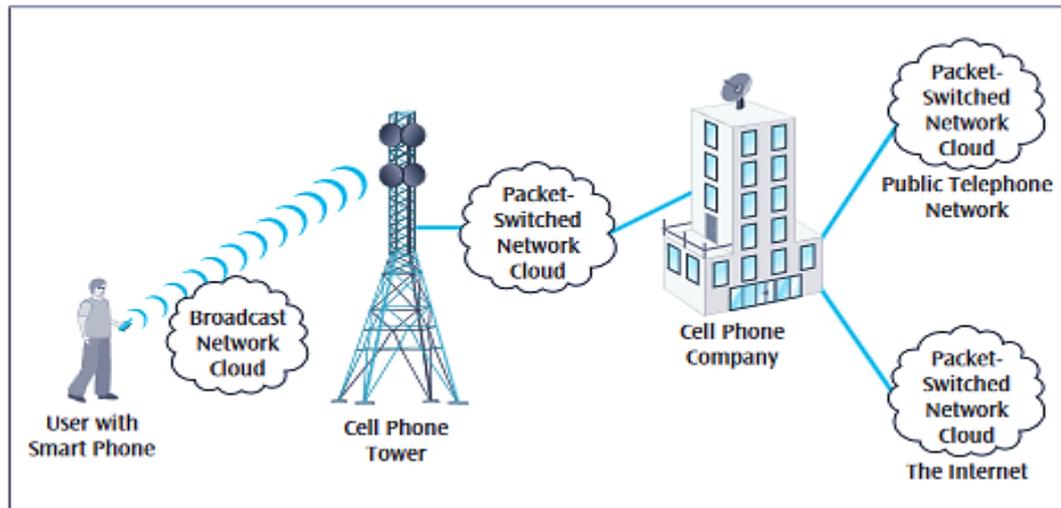
- Berapa rata-rata (atau konstan) bit rate yang digunakan pengguna untuk melakukan transmisi?
- Berapa rata-rata kecepatan bit puncak yang dapat digunakan oleh pengguna untuk melakukan transmisi?
- Berapa kecepatan jaringan yang mulai membuang paket jika terjadi kemacetan?
- Berapa bit rate rata-rata yang dapat disediakan oleh jaringan?
- Berapa rata-rata kecepatan bit puncak yang dapat disediakan oleh jaringan?

Banyak jaringan menghubungkan isu-isu ini dengan kualitas layanan (QoS), sebuah konsep di mana pengguna jaringan dan jaringan menyetujui tingkat layanan tertentu (pedoman yang dapat diterima untuk transfer data yang tepat). Misalnya, pengguna yang memerlukan koneksi real-time yang sangat cepat untuk mendukung video aksi langsung akan bernegosiasi dengan jaringan untuk mendapatkan kualitas layanan tertentu. Jika jaringan dapat memberikan tingkat kualitas ini, kontrak disepakati, pengguna dikenakan biaya yang sesuai, dan sambungan dibuat. Jika pengguna kedua memerlukan koneksi yang lebih lambat untuk email, tingkat kualitas yang berbeda akan disetujui, dan koneksi ini akan dibuat. Seringkali perjanjian antara penyedia layanan dan pengguna layanan diformalkan dalam perjanjian tingkat layanan, sebuah dokumen tertulis yang mengikat secara hukum yang dapat mencakup parameter layanan yang ditawarkan dalam layanan, berbagai jenis opsi layanan/dukungan, insentif jika tingkat layanan terlampaui, dan denda jika tingkat layanan tidak terpenuhi. Sekarang kita telah membahas semua rincian teknis yang diperlukan dari WAN, mari kita lihat contoh bisnis.

9.6 SMART PHONE BERBASIS WAN

Karena mengakses World Wide Web melalui Internet merupakan hal yang lumrah saat ini, mudah untuk melupakan bahwa belum lama ini hal tersebut dianggap sebagai pencapaian teknologi yang luar biasa. Kebanyakan orang memiliki satu atau lebih komputer pribadi di rumah dan terhubung ke Internet melalui penyedia layanan Internet (ISP) dan modem kabel, layanan DSL, atau kemungkinan besar layanan dial-up. Jika Anda seorang mahasiswa yang terdaftar di sebuah perguruan tinggi, kemungkinan besar Anda memiliki akses Internet melalui laboratorium komputer perguruan tinggi dan kampusnya serta jaringan nirkabel. Demikian pula, banyak karyawan bisnis memiliki akses Internet melalui jaringan area lokal perusahaan, yang memungkinkan mereka mengunduh halaman Web. Namun cara mengakses Internet yang berkembang pesat adalah melalui telepon pintar (ponsel). Banyak orang menggunakan ponsel cerdas untuk mengirim pesan teks, mengakses Web, mengunggah foto ke situs Web sosial, dan—ya—melakukan panggilan telepon. Mari kita periksa berbagai jenis cloud jaringan yang mendukung akses Internet melalui ponsel pintar.

Pertama, kita asumsikan bahwa ponsel cerdas Anda telah menyala selama beberapa waktu tetapi tidak digunakan. Ponsel cerdas Anda dan menara seluler terdekat meneruskan paket bolak-balik kira-kira setiap 10 detik sehingga sistem telepon seluler mengetahui keberadaan Anda. Orang mungkin berpendapat bahwa telepon seluler Anda dan menara telepon seluler terdekat adalah bagian dari jaringan siaran. Sinyal disiarkan ke semua perangkat terdekat, namun karena frekuensi yang digunakan dan nomor ID seluler yang terlibat, ada “koneksi” antara ponsel Anda dan jaringan telepon seluler. Selain itu, paket-paket ini akan tetap berada dalam sistem telepon seluler dan tidak diteruskan ke Internet. Dengan demikian, perusahaan telepon seluler Anda menyediakan jenis jaringan siaran dalam jaringan packet-switched (Gambar 9-15).



Gambar 9-15 Interkoneksi jaringan cloud

Bagaimana jika Anda ingin berbicara dengan seseorang melalui ponsel Anda, atau mengirim pesan teks kepada orang tersebut? Jika Anda menelepon orang lain yang memiliki layanan telepon seluler yang sama dengan Anda, panggilan Anda mungkin tidak akan pernah keluar dari jaringan penyedia seluler. Namun kemungkinan besar panggilan Anda akan berpindah dari jaringan telepon seluler ke jaringan telepon umum. Jika ya, maka kita tahu bahwa meskipun jaringan telepon umum di Amerika Utara dulunya merupakan jaringan Circuit-switched, kini menjadi jaringan packet-switched. Jadi panggilan telepon seluler Anda telah berpindah dari satu jaringan packet-switched ke jaringan lainnya.

Bagaimana jika Anda memeriksa halaman Facebook Anda melalui ponsel cerdas Anda? Kemudian, paket data Anda harus berpindah dari jaringan telepon seluler ke ISP dan kemudian ke Internet. Internet, tentu saja, merupakan kumpulan besar jaringan packet-switched. Permintaan Anda akan dirutekan melalui Internet (mungkin menggunakan satu atau lebih protokol perutean yang diperkenalkan dalam bab ini) dan pada akhirnya akan mencapai situs Web Facebook, tempat halaman Facebook yang dihasilkan akan dikembalikan ke ponsel cerdas Anda.

Dalam semua contoh di atas, kita melihat bahwa jaringan packet-switched adalah pekerja keras utama bagi sebagian besar komunikasi saat ini. Contoh dari jaringan penyiaran area luas dan jaringan sirkuit-switched menjadi semakin langka setiap harinya.

RINGKASAN

- Jaringan yang meluas ke wilayah metropolitan dan menunjukkan kecepatan data yang tinggi, keandalan yang tinggi, dan kehilangan data yang rendah disebut jaringan wilayah metropolitan (MAN). Banyak dari teknologi dan protokol komunikasi yang sama yang ditemukan di jaringan area lokal (dan jaringan area luas) digunakan untuk membuat jaringan area metropolitan.

- Jaringan area metropolitan didasarkan pada tulang punggung SONET atau Ethernet. Tulang punggung SONET terdiri dari cincin serat optik, sedangkan tulang punggung Ethernet adalah jaringan mesh.
- Layanan Metro Ethernet menyediakan antarmuka Ethernet ke bisnis dan dapat mentransfer data dengan kecepatan tinggi melalui wilayah metropolitan.
- Jaringan area luas mencakup wilayah geografis yang lebih luas dibandingkan jaringan area lokal dan jaringan area metropolitan, dan jaringan tersebut didasarkan pada subjaringan fisik yang mungkin berbeda, atau cloud jaringan: switching sirkuit, switch paket, dan siaran.
- Jaringan Circuit-switched menciptakan sirkuit khusus antara pengirim dan penerima, dan semua data melewati sirkuit ini.
- Jaringan packet-switched mentransmisikan paket data berukuran tetap yang disebut paket. Jaringan packet-switched terbagi dalam dua subkategori: jaringan datagram dan jaringan sirkuit virtual. Jaringan packet-switched datagram mentransmisikan setiap paket secara independen dari setiap paket lainnya. Setiap paket dianggap sebagai satu kesatuan dan bukan merupakan bagian dari pengelompokan paket yang lebih besar. Jaringan packet-switched sirkuit virtual membuat sirkuit virtual menggunakan tabel perutean dan mentransmisikan semua paket milik koneksi tertentu melalui sirkuit virtual ini.
- Jaringan siaran mengirimkan datanya ke semua stasiun kerja pada waktu yang sama. Jaringan penyiaran lebih sering digunakan pada jaringan area lokal dibandingkan jaringan area luas.
- Aplikasi jaringan yang berjalan pada suatu jaringan dapat berorientasi koneksi atau tanpa koneksi. Aplikasi jaringan yang berorientasi koneksi memberikan jaminan bahwa informasi yang melewati jaringan tidak akan hilang, dan bahwa paket informasi akan dikirimkan ke penerima yang dituju dalam urutan yang sama seperti saat pengirimannya. Untuk menyediakan layanan ini, koneksi logis dibuat sebelum transfer data dilakukan. Aplikasi jaringan tanpa koneksi tidak memerlukan koneksi logis yang dibuat sebelum data ditransfer.
- Memilih rute optimal untuk transfer paket data melalui jaringan adalah layanan umum di banyak jaringan. Rute optimal ini diperoleh dengan menggabungkan dua atau lebih dari sekian banyak algoritma dan teknik routing yang tersedia saat ini.
- Salah satu cara yang mungkin untuk memilih rute optimal melalui jaringan adalah dengan memilih jalur yang total biaya jalurnya memiliki nilai terkecil. Teknik ini didasarkan pada algoritma berbiaya terendah Dijkstra dan merupakan metode umum untuk menentukan rute optimal.
- Flooding adalah teknik routing yang mengharuskan setiap node mengambil paket masuk dan mengirimkannya kembali ke setiap link keluar. Jika salinan sebuah paket harus dikirim ke node tertentu, banjir akan membawanya ke sana—tetapi hal ini juga akan menciptakan sejumlah besar paket yang disalin yang didistribusikan ke seluruh jaringan.

- Perutean terpusat adalah teknik untuk menyediakan informasi perutean yang menentukan bahwa informasi perutean, yang dihasilkan oleh metode seperti algoritma berbiaya paling rendah, disimpan di lokasi pusat dalam jaringan.
- Teknik lain untuk menyediakan informasi routing, routing terdistribusi memungkinkan setiap node untuk memelihara tabel routingnya sendiri.
- Perutean adaptif memungkinkan jaringan membuat tabel perutean yang sering berubah seiring perubahan kondisi jaringan.
- RIP dan OSPF adalah dua protokol routing penting yang ditemukan di Internet.
- Bila jaringan atau bagian dari jaringan menjadi terlalu jenuh dengan paket data sehingga transfer paket menjadi terhambat, maka kemacetan jaringan telah terjadi. Kemacetan mungkin disebabkan oleh terlalu banyak lalu lintas, kegagalan node jaringan, kegagalan link jaringan, atau ruang buffer node yang tidak mencukupi. Solusi untuk kemacetan jaringan mencakup kontrol kemacetan implisit, kontrol kemacetan eksplisit, kontrol aliran, praalokasi buffer nodal, dan parameter kontrol penerimaan koneksi.
- Parameter kualitas layanan (QoS) dapat digunakan oleh pengguna jaringan dan penyedia layanan untuk menetapkan pedoman yang dapat diterima untuk transfer data yang tepat. Pedoman ini dapat mencakup kecepatan transmisi, tingkat kesalahan, dan throughput jaringan secara keseluruhan.

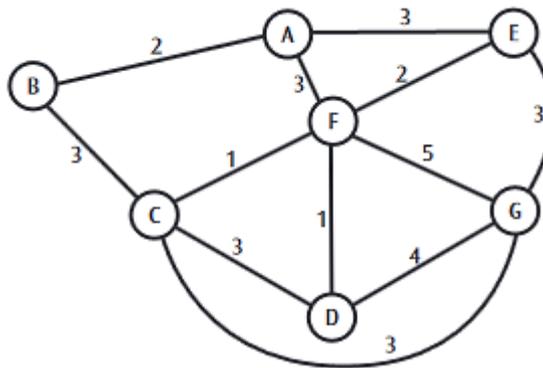
PERTANYAAN TINJAUAN

1. Apa perbedaan utama antara jaringan area lokal dan jaringan area luas?
2. Apa perbedaan jaringan area metropolitan dengan jaringan area luas? Bagaimana kemiripannya?
3. Apa yang dimaksud dengan waktu failover?
4. Apa saja dua jenis teknologi yang mendukung jaringan area metropolitan?
5. Apa itu Metro Ethernet dan apa hubungannya dengan jaringan area metropolitan?
6. Apa yang dimaksud dengan subnetwork, atau jaringan cloud, dan apa bedanya dengan jaringan area luas?
7. Apa perbedaan antara stasiun dan node?
8. Apa karakteristik utama dari jaringan Circuit-switched? Apa kelebihan dan kekurangannya?
9. Apa karakteristik utama dari jaringan packet-switched datagram? Apa kelebihan dan kekurangannya?
10. Apa karakteristik utama dari jaringan packet-switched sirkuit virtual? Apa kelebihan dan kekurangannya?
11. Apa perbedaan aplikasi jaringan tanpa koneksi dengan aplikasi jaringan berorientasi koneksi?
12. Apakah aplikasi jaringan tanpa koneksi dapat diandalkan atau tidak? Menjelaskan.
13. Apa sajakah kombinasi subjaringan sirkuit-switched dan packet-switched, serta aplikasi jaringan berorientasi koneksi dan tanpa koneksi?
14. Apa perbedaan grafik jaringan berbobot dengan grafik jaringan?

15. Untuk grafik jaringan berbobot, berapa banyak definisi bobot yang dapat Anda cantumkan?
16. Apa tujuan dasar dari algoritma berbiaya paling rendah Dijkstra?
17. Bagaimana banjir dapat digunakan untuk mengirimkan paket data dari satu ujung jaringan ke ujung lainnya?
18. Bagaimana jumlah hop dan batas hop digunakan untuk mengendalikan banjir?
19. Apa kelebihan dan kekurangan utama dari:
 - A. Perutean terpusat
 - B. Perutean terdistribusi
 - C. Perutean adaptif
20. Apa perbedaan antara RIP dan OSPF?
21. Apa yang menyebabkan kemacetan jaringan?
22. Bagaimana cara menghindari kemacetan jaringan?
23. Apa hubungan kualitas layanan dengan kemacetan jaringan?

LATIHAN SOAL

1. Sebutkan tiga keunggulan jaringan area metropolitan berbasis SONET dibandingkan jaringan area metropolitan berbasis Ethernet.
2. Sebutkan tiga keuntungan jaringan area metropolitan berbasis Ethernet dibandingkan jaringan area metropolitan berbasis SONET.
3. Jenis aplikasi jaringan manakah yang memerlukan perangkat lunak yang lebih rumit: berorientasi koneksi atau tanpa koneksi? Menjelaskan.
4. Buat analogi yang mirip dengan analogi “membuat panggilan telepon versus mengirim surat” yang menunjukkan perbedaan antara aplikasi jaringan berorientasi koneksi dan tanpa koneksi.
5. Jelaskan perbedaan antara node jaringan dan stasiun jaringan.
6. Apakah jaringan datagram memerlukan waktu setup sebelum paket dikirimkan? Jelaskan jawabanmu.
7. Apakah jaringan sirkuit virtual memerlukan waktu pengaturan sebelum paket dikirim? Jika ya, kapan, dan seberapa sering?
8. Sebutkan langkah-langkah yang terlibat dalam membuat, menggunakan, dan mengakhiri sirkuit virtual.
9. Anda sedang mendownload file melalui Internet. Apakah pengunduhan merupakan aplikasi tanpa koneksi atau aplikasi berorientasi koneksi? Menjelaskan.
10. Dengan menggunakan konsep banjir dan grafik yang ditunjukkan pada Gambar 9-16, berapa banyak paket yang akan dibuat jika sebuah paket berasal dari Node A dan terdapat batas hop jaringan sebesar 3?
11. Bagaimana cara menentukan batas hop pada banjir?



Gambar 9-16 Contoh grafik jaringan berbobot untuk Latihan 10

12. Jelaskan bagaimana routing RIP meneruskan berita buruk secara perlahan.
13. Apa yang dapat dilakukan untuk melindungi jaringan perutean terpusat jika komputer yang menampung tabel perutean pusat mengalami kegagalan?
14. Apa yang terjadi dalam jaringan packet-switched sirkuit virtual jika sebuah node atau link komunikasi di sepanjang jalur virtual gagal?
15. Apakah jaringan Ethernet mendukung kualitas layanan? Menjelaskan.
16. Frame relay mendukung dua jenis prosedur penghindaran kemacetan. Apakah stasiun tujuan mengetahui kemacetan di kedua prosedur tersebut?
17. Asumsikan dua stasiun berada pada jaringan ATM biasa yang mentransmisikan data dengan kecepatan 150 Mbps dan berada di ujung Amerika Serikat yang berlawanan (waktu propagasi untuk mengirimkan antara dua stasiun kira-kira $4,6 \cdot 10^{-2}$ detik). Kemacetan mulai terjadi di satu stasiun. Jika stasiun yang padat ingin mengirim sinyal kembali ke stasiun lain untuk memperlambat atau menghentikan transmisinya, berapa bit yang akan dibuang sebelum stasiun lain memperlambat atau menghentikan transmisinya?

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Perusahaan Anda memiliki sejumlah jaringan area lokal yang saling berhubungan dalam satu gedung. Di dalam gedung juga terdapat router yang menghubungkan LAN ke penyedia layanan Internet menggunakan beberapa saluran telepon T-1. Perusahaan Anda sedang mempertimbangkan untuk mengganti T-1 dengan koneksi ke jaringan area metropolitan. Tunjukkan interkoneksi LAN, MAN, dan Internet, dengan asumsi MAN berbasis SONET. Apakah interkoneksinya akan berbeda jika MAN berbasis Ethernet? Menjelaskan.
2. Jaringan area luas yang luas mencakup Amerika Serikat dan memiliki banyak node di setiap negara bagian. Node di Denver lumpuh total. Bagaimana node lain di negara tersebut mengetahui kerusakan tersebut jika RIP digunakan? Jika OSPF digunakan?
3. Perusahaan Anda membuat aplikasi jaringan baru yang memungkinkan karyawan melihat slip gaji mereka secara elektronik melalui Internet. Apakah aplikasi ini harus bersifat connectionless atau connection centric? Pertahankan jawaban Anda, dan

gambarlah serangkaian contoh layar yang mungkin dilihat oleh pengguna yang sedang mengakses bukti pembayaran elektroniknya.

4. Salah satu bentuk penghindaran kemacetan adalah dengan sistem perizinan, dimana suatu node harus mempunyai izin terlebih dahulu sebelum dapat melakukan transmisi. Misalkan jaringan area luas menggunakan sistem perizinan untuk mengendalikan kemacetan. Apa jadinya jika, karena alasan yang tidak diketahui, semua izin hilang? Bagaimana peristiwa ini dapat dideteksi? Bagaimana peristiwa ini dapat diperbaiki?
5. Ketika kita berbicara tentang routing dalam jaringan area luas, kita sering memperkenalkan konsep bagaimana jaringan memutuskan jalur mana yang akan diikuti oleh lalu lintas data tertentu. Kita sering menyebutkan kata “keadilan” dan “keseimbangan” ketika mencoba memutuskan perutean jaringan dan kondisi pemuatan. Namun bagaimana jika jaringannya tidak adil? Bagaimana jika ia menyukai satu jenis lalu lintas tertentu, atau lalu lintas dari jenis pengguna tertentu? Apakah itu masih adil? Apakah ini ada hubungannya dengan “netralitas jaringan”? Menjelaskan.
6. Mengingat jaringan dengan n node, buatlah rumus yang menghitung jumlah pesan yang dikirimkan antar node jika satu node berisi tabel perutean terpusat, dan masing-masing node lainnya merujuk ke tabel perutean ini setiap detik.
7. Apakah Internet menggunakan banjir dalam situasi tertentu? Buktikan jawaban Anda.
8. Mode Transfer Asinkron populer karena kualitas kemampuannya. Bagaimana hal itu mendukung kualitas layanan?
9. Tulis program komputer, menggunakan bahasa pilihan Anda, yang memasukkan data untuk grafik jaringan berbobot dan menghitung jalur berbiaya terendah menggunakan algoritma Dijkstra. Rincian algoritma Dijkstra dapat ditemukan di pendamping online siswa untuk teks ini.
10. Dengan menggunakan prosedur algoritma Dijkstra yang dijelaskan dalam pendamping online siswa untuk teks ini dan grafik jaringan tertimbang yang ditunjukkan pada Gambar 9-16, temukan rute berbiaya paling rendah dari Node A ke semua node lainnya.
11. Algoritma perutean apa yang saat ini digunakan di Internet? Apakah ada algoritma dan teknik dasar yang diperkenalkan dalam bab ini yang digunakan? Jika ya, yang mana?

BAB 10

INTERNET

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Diskusikan tanggung jawab Internet Protocol (IP) dan bagaimana IP dapat digunakan untuk membuat koneksi antar jaringan
- Mampu mengidentifikasi alamat IPv4 dan alamat IPv6
- Diskusikan tanggung jawab Protokol Kontrol Transmisi (TCP) dan bagaimana protokol ini dapat digunakan untuk menciptakan koneksi jaringan end-to-end yang andal
- Identifikasi hubungan antara TCP/IP dan ICMP, UDP, ARP,
- DHCP, NAT, dan protokol terowongan
- Jelaskan tanggung jawab Sistem Nama Domain dan cara mengubah URL menjadi alamat IP desimal bertitik
- Jelaskan aplikasi dan layanan Internet utama
- Diskusikan keuntungan bisnis World Wide Web
- Sadarilah bahwa Internet terus berkembang, dan IPv6 dan Internet2 menunjukkan evolusi tersebut

MENURUT Ipsos Reid, sebuah perusahaan jajak pendapat di Kanada, remaja Kanada menghabiskan lebih banyak waktu berselancar online dibandingkan menonton televisi. Studi tersebut menyatakan bahwa penggunaan Internet baru-baru ini meningkat sekitar 46 persen menjadi 12,7 jam seminggu, naik dari 8,7 jam pada tahun 2002. “Anak Muda Kanada Menghabiskan Lebih Banyak Waktu di Internet Dibandingkan Menonton TV,”

Amazon.com, pengecer Internet yang berbasis di Seattle, melaporkan bahwa penjualan bersihnya pada tahun 2010 berjumlah Rp. 130 Triliyun, meningkat 40 persen dari tahun 2009. “Penjualan Amazon naik 40% pada tahun 2010”.

Jika rumah lelang online eBay adalah sebuah negara, maka eBay akan menjadi salah satu dari 20 negara terbesar di dunia, dengan 157 juta pengguna terdaftar. Pada waktu tertentu, eBay memiliki sekitar 55 juta item untuk dijual. “Pembeli Tanpa Kabel Memungkinkan Pengguna eBay Menawar melalui Ponsel Apa Pun,”

Dengan banyaknya uang yang dipertaruhkan, Anda harus bertanya, “Jika terjadi masalah dengan Internet, siapa atau apa yang bertanggung jawab untuk memperbaikinya?” Jawabannya, yang mengejutkan, adalah tidak ada siapa-siapa dan tidak ada apa-apa. Internet dikelola oleh konfederasi bisnis dan organisasi nirlaba. Para pemainnya tersebar di seluruh dunia dan termotivasi untuk mencapai konsensus demi kepentingan pribadi. Menariknya, struktur ini menjadikan Internet sebagai satu-satunya asosiasi global yang tidak memiliki kedaulatan.

Apa yang disebut Internet?

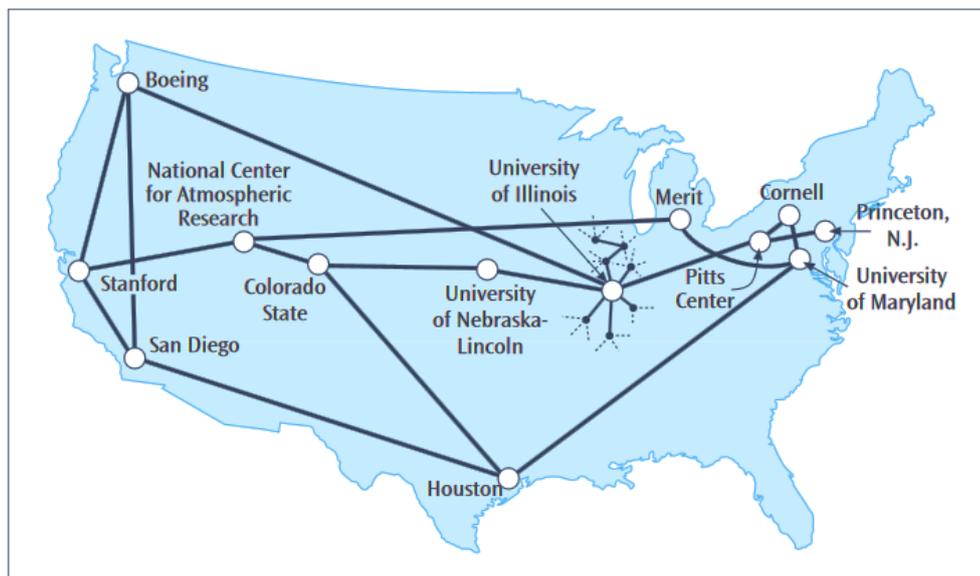
Layanan apa yang ditawarkan di Internet?

Mekanisme dasar apa yang membuat Internet tetap berfungsi?

10.1 PENDAHULUAN

Pada akhir tahun 1960-an, sebuah cabang pemerintah AS bernama Advanced Research Projects Agency (ARPA) menciptakan salah satu jaringan packet-switched area luas pertama di negara tersebut, yaitu ARPANET. Universitas riset tertentu, pangkalan militer, dan laboratorium pemerintah diizinkan mengakses ARPANET untuk layanan seperti surat elektronik, transfer file, dan login jarak jauh.

Pada tahun 1983, Departemen Pertahanan membagi ARPANET menjadi dua jaringan serupa: ARPANET asli dan MILNET, yang hanya untuk keperluan militer. Meskipun MILNET pada dasarnya tetap sama dari waktu ke waktu, ARPANET akhirnya dihapuskan dan diganti dengan teknologi yang lebih baru. Selama periode ini, National Science Foundation mendanai pembuatan tulang punggung jaringan lintas negara berkecepatan tinggi baru yang disebut NSFNET. Tulang punggung adalah jalur telekomunikasi utama melalui jaringan, menghubungkan situs router utama di seluruh negeri. Pada tulang punggung inilah jaringan-jaringan regional atau tingkat menengah (seluruh negara bagian) yang lebih kecil terhubung. Seperangkat jaringan akses atau “kampus” kemudian dihubungkan ke jaringan tingkat menengah ini (Gambar 10-1). Akhirnya, kumpulan jaringan ini dikenal sebagai Internet.



Gambar 10-1 Tulang punggung NSFNET lama dan menghubungkan jaringan tingkat menengah dan kampus

Pada awal tahun 1990an, pemerintah pada dasarnya menarik semua dukungan langsung terhadap Internet dan menyerahkannya kepada industri swasta dan universitas. Dengan demikian, tidak ada lagi satu tulang punggung melainkan banyak tulang punggung yang didukung oleh berbagai bisnis dan organisasi, yang semuanya bersaing satu sama lain. Perkiraan saat ini menunjukkan bahwa terdapat lebih dari 500 juta host (situs komputer yang menyimpan dan mengirimkan halaman Web) yang terhubung ke Internet, dan lebih dari 2 miliar orang di seluruh dunia mengakses Internet secara teratur. Satu fakta yang sangat jelas:

Penggunaan Internet telah tumbuh dengan kecepatan yang fenomenal. Pencipta awalnya tidak—tidak bisa—membayangkan Internet yang kita miliki saat ini.

Mendukung Internet adalah sejumlah protokol. Dua protokol yang paling umum adalah Internet Protocol (IP) dan Transmisi Control Protocol (TCP). Protokol-protokol ini sendiri didukung oleh sejumlah protokol sekunder, yang meliputi Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), Address Recognition Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), dan Terjemahan Alamat Jaringan (NAT).

Banyak orang mengira Internet hanyalah aplikasi yang memungkinkan seseorang menelusuri halaman Web dan mengklik tautan, padahal Internet sebenarnya mencakup berbagai layanan. Salah satu layanan pertama dan masih populer yang ditawarkan di Internet adalah surat elektronik, atau email. Layanan lain yang dimungkinkan oleh Internet termasuk pesan instan, transfer file menggunakan File Transfer Protocol (FTP), desktop jarak jauh dan administrasi jarak jauh, telepon Internet (VoIP), listservs, dan streaming audio dan video.

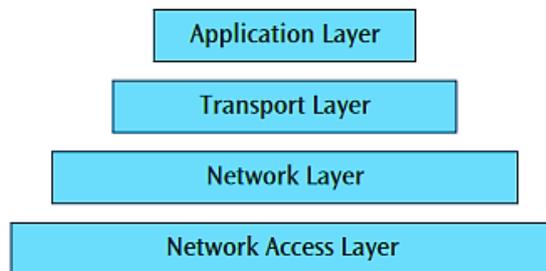
Dampak World Wide Web dan fungsi Internet lainnya terhadap komunitas bisnis sangatlah besar. Pada akhir tahun 1990an, bidang bisnis baru muncul: e-commerce. Sekarang, Anda bisa membeli apa saja secara praktis di Internet. Hiburan, obat-obatan, bahan makanan, real estate, hipotek, dan mobil hanyalah beberapa dari produk yang tersedia online melalui e-commerce.

Untuk mendukung berbagai jenis layanan Internet dan untuk mendukung lapisan rangkaian protokol TCP/IP, banyak protokol telah dibuat. Mari kita mulai studi kita tentang dunia Internet yang menakjubkan dengan memeriksa beberapa protokol Internet yang lebih penting.

10.2 PROTOKOL INTERNET

Dari email sederhana hingga kompleksitas Web, banyak layanan tersedia di Internet. Apa yang memungkinkan beragam layanan ini berfungsi? Apa yang memungkinkan Internet itu sendiri berfungsi? Jawaban atas pertanyaan-pertanyaan ini adalah protokol Internet. Meskipun pengoperasian Internet bergantung pada banyak protokol, ada beberapa protokol yang paling umum digunakan: Protokol Internet (IP), Protokol Kontrol Transmisi (TCP), Protokol Kontrol Pesan Internet (ICMP), Protokol Datagram Pengguna (UDP), Protokol Resolusi Alamat (ARP), Protokol Konfigurasi Host Dinamis (DHCP), dan Terjemahan Alamat Jaringan (NAT).

Ingat kembali lapisan rangkaian protokol TCP/IP yang diperkenalkan di Bab Satu. Hirarki ini awalnya ditetapkan oleh Departemen Pertahanan (Gambar 10-2). Perhatikan bahwa lapisan dirancang sedemikian rupa sehingga pengguna Internet yang perlu menggunakan aplikasi (seperti email atau transfer file, yang akan dibahas nanti di bab ini) memerlukan penggunaan lapisan aplikasi, yang pada gilirannya memerlukan penggunaan lapisan aplikasi. lapisan transport, yang memerlukan penggunaan lapisan jaringan, yang memerlukan penggunaan lapisan akses jaringan. Dengan kata lain, lapisan-lapisan tersebut dibangun satu sama lain dalam hierarki ini, dan pengguna tidak terpapar pada detail lapisan-lapisan tersebut yang tidak memiliki kontak langsung dengan pengguna.



Gambar 10-2 Hierarki lapisan yang dibuat oleh Departemen Pertahanan

Protokol yang berada pada lapisan jaringan dalam rangkaian protokol TCP/IP disebut Protokol Internet. Fungsi utama IP adalah melakukan perutean yang diperlukan untuk memindahkan paket data melalui Internet. IP adalah sebuah protokol connectionless yang tidak peduli dengan pelacakan paket yang hilang, terduplikasi, atau tertunda, atau paket yang dikirim tidak sesuai urutan. Selain itu, pengirim dan penerima paket ini mungkin tidak diberitahu bahwa masalah ini telah terjadi. Dengan demikian, IP juga disebut sebagai layanan yang tidak dapat diandalkan. Jika suatu aplikasi memerlukan layanan yang dapat diandalkan, maka aplikasi tersebut perlu menyertakan layanan transportasi yang dapat diandalkan “di atas” layanan pengiriman paket yang tidak dapat diandalkan dan tidak memiliki koneksi. Layanan transportasi yang andal disediakan oleh perangkat lunak yang disebut Protokol Kontrol Transmisi, yang mengubah jaringan yang tidak dapat diandalkan menjadi jaringan yang andal, bebas dari paket yang hilang dan terduplikasi. Layanan gabungan ini dikenal sebagai TCP/IP.

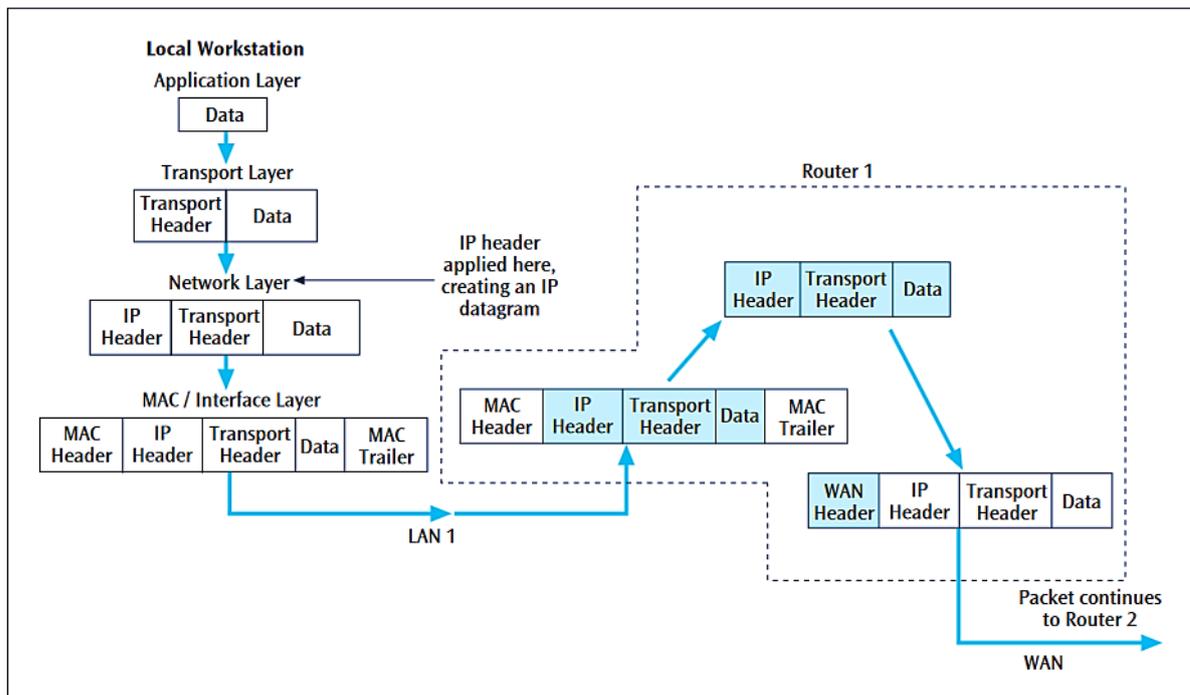
Penggunaan TCP/IP terbukti sangat efektif dalam menghubungkan jaringan-jaringan di Internet sehingga akhirnya banyak universitas dan perusahaan mulai menggunakan TCP/IP untuk interkoneksi jaringan internalnya. Faktanya, kombinasi TCP yang beroperasi pada lapisan transport dan IP yang beroperasi pada lapisan jaringan ditemukan di hampir semua jaringan yang mendukung Internet global. Karena TCP/IP pada dasarnya adalah dua protokol, kita akan memeriksa protokol-protokol ini secara independen. Kami juga akan, di bagian selanjutnya, memeriksa sejumlah protokol yang mendukung TCP, IP, dan Internet.

Protokol Internet

Internet Protocol (IP) menyediakan layanan transfer data tanpa koneksi melalui jaringan heterogen dengan meneruskan dan merutekan datagram IP. Datagram IP pada dasarnya adalah nama lain untuk paket data. Untuk diteruskan dan dirutekan di Internet, semua datagram atau paket IP yang diturunkan dari lapisan transport ke lapisan jaringan (lapisan pengiriman paket connectionless) dienkapsulasi dengan header IP (lihat sudut kiri atas Gambar 10-3) yang berisi informasi yang diperlukan untuk mengirimkan paket dari satu jaringan ke jaringan lainnya. Format header ini akan dijelaskan pada beberapa paragraf berikutnya.

Perhatikan sekali lagi contoh stasiun kerja yang melakukan operasi jaringan seperti mengirim pesan email ke stasiun kerja yang jauh, sebuah proses yang digambarkan pada Gambar 10-3. Misalkan kedua stasiun kerja berada pada jaringan area lokal dan kedua jaringan

area lokal terhubung melalui jaringan area luas. Saat stasiun kerja lokal mengirimkan paket email ke bawah melalui lapisan jaringan internal pertama, header IP dienkapsulasi di atas paket lapisan transport, menciptakan datagram IP. Proses enkapsulasi ini mirip dengan contoh enkapsulasi yang disajikan pada Bab Satu dan Tujuh. Header lapisan MAC yang sesuai dienkapsulasi melalui datagram IP yang membuat sebuah frame, dan frame ini dikirim melalui LAN 1 ke router pertama. Karena router menghubungkan LAN 1 ke jaringan area luas, informasi lapisan MAC dihilangkan, meninggalkan datagram IP. Pada saat ini, router dapat menggunakan salah satu atau semua informasi IP untuk menjalankan fungsi internetworking yang diperlukan. Informasi tingkat jaringan area luas yang diperlukan diterapkan, dan paket dikirim melalui WAN ke Router 2. Ketika paket tiba di router kedua, informasi jaringan area luas dihilangkan, sekali lagi meninggalkan datagram IP. Informasi lapisan MAC yang sesuai kemudian diterapkan untuk transfer frame melalui LAN 2, dan frame tersebut ditransmisikan. Setibanya di stasiun kerja jarak jauh, semua informasi header dihapus, meninggalkan data asli.



Gambar 10-3 Perkembangan paket dari satu jaringan ke jaringan lainnya

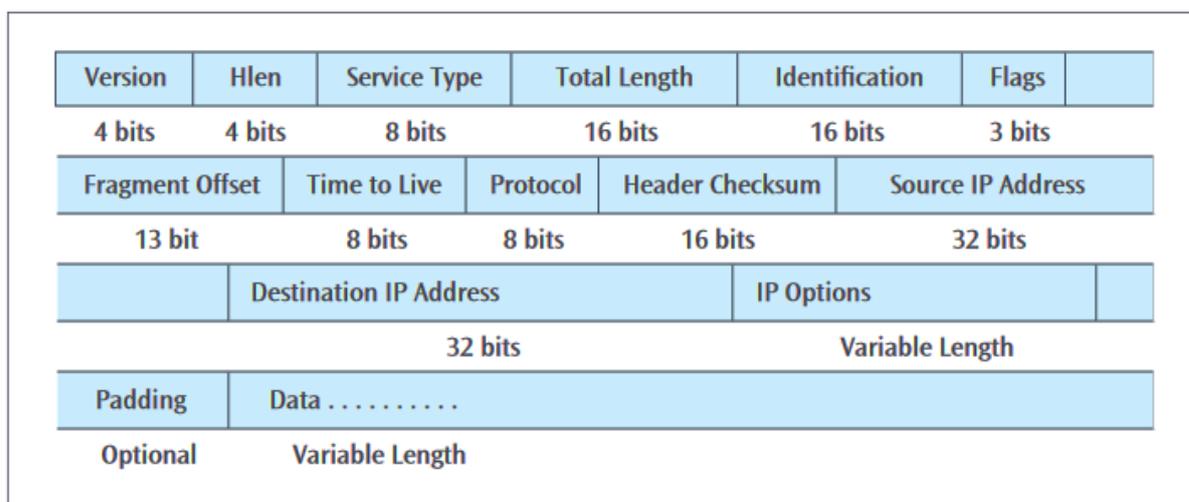
Ketika sebuah router memiliki datagram IP, ia mungkin membuat beberapa keputusan yang mempengaruhi masa depan datagram tersebut. Secara khusus, router mungkin menjalankan fungsi berikut:

- Membuat keputusan perutean berdasarkan bagian alamat dari datagram IP.
- Pecahkan datagram menjadi datagram yang lebih kecil jika jaringan berikutnya yang akan dilintasi memiliki ukuran paket maksimum yang lebih kecil dibandingkan ukuran paket saat ini.
- Putuskan bahwa datagram saat ini sudah terlalu lama berpindah-pindah jaringan dan hapus datagram tersebut.

Untuk menjalankan fungsi ini, router memerlukan informasi alamat dan ukuran datagram, serta mengetahui berapa kali datagram telah melewati router. Informasi ini ditemukan di header IP, yang merupakan informasi yang diterapkan pada paket transport di lapisan jaringan. Masing-masing fungsi router ini, beserta bidang header IP yang mendukung fungsi-fungsi ini, akan diperiksa lebih detail di bagian selanjutnya. Sebelum kita memeriksa rincian datagram ini, penting untuk dicatat bahwa saat ini ada dua versi IP: IP versi 4 (IPv4) dan IP versi 6 (IPv6). IPv4 telah ada sejak awal tahun 1980an dan kemungkinan besar masih merupakan versi yang paling umum. Untuk mendukung permintaan yang terus meningkat, IPv6 diperkenalkan pada tahun 1998. Meskipun terdapat sejumlah kemajuan, seperti yang akan segera kita lihat, IPv6 masih lambat untuk dikembangkan. Namun hal itu tidak selalu terjadi. Mari kita lihat versi 4 dulu.

Format Datagram IPv4

Gambar 10-3 menunjukkan bahwa lapisan jaringan perangkat lunak komunikasi menambahkan header IP ke paket lapisan transport—sehingga menciptakan datagram IP—sebelum meneruskan paket ke lapisan perangkat lunak berikutnya. Informasi yang disertakan dalam header IP ini dan cara header dikemas memungkinkan jaringan area lokal dan jaringan area luas untuk berbagi data dan membuat koneksi internetwork.



Gambar 10-4 Format datagram IPv4

Apa sebenarnya isi header IP ini yang memungkinkan terjadinya internetworking ini? Gambar 10-4 menunjukkan masing-masing bidang header IPv4 secara lebih rinci. Walaupun keempat belas field tersebut penting, mari kita periksa field yang menentukan versi Internet Protocol dan field-field yang mempengaruhi tiga fungsi utama IP: fragmentasi, pembuangan datagram, dan pengalamatan. Dengan memeriksa bidang-bidang ini, Anda akan mulai menemukan cara kerja IPv4 dan mengapa IPv4 mampu menghubungkan begitu banyak jenis jaringan yang berbeda.

Bidang minat pertama adalah bidang Versi. Bidang Versi berisi nomor versi IP yang digunakan. Tidak mengejutkan, IPv4 mempunyai nilai 4 pada field ini dan IPv6 mempunyai

nilai 6. Field Version penting karena memberitahu router bagaimana menginterpretasikan sisa datagram IP.

Tiga bidang minat berikutnya—Identifikasi, Bendera, dan Offset Fragmen—digunakan untuk memfragmentasi datagram menjadi bagian-bagian yang lebih kecil. Mengapa kita ingin memecah datagram? Ketika Protokol Internet dibuat, ukuran paket maksimum dari beberapa jaringan lama yang masih ada adalah kecil. Ukuran maksimum ini dibatasi oleh perangkat keras jaringan, perangkat lunak, atau faktor lainnya. Karena IP dirancang untuk bekerja pada hampir semua jenis jaringan, IP harus mampu mentransfer datagram dengan berbagai ukuran. Daripada membatasi IP ke ukuran paket maksimum terkecil yang ada (Siapa yang tahu apa itu?), Protokol Internet memungkinkan router untuk memecah atau memfragmentasi datagram besar menjadi fragmen yang lebih kecil sehingga dapat masuk ke jaringan berikutnya. Untungnya, hampir tidak ada jaringan modern yang memiliki ukuran paket maksimum yang cukup kecil untuk menjadi perhatian. Dengan demikian, suatu hari nanti, memecah-mecah datagram menjadi paket-paket yang lebih kecil tidak lagi menjadi masalah penting. Faktanya, seperti yang akan Anda pelajari sebentar lagi, IP versi 6 bahkan tidak memiliki kolom di header untuk melakukan fragmentasi. (Jika Anda ingin melihat bagaimana sebenarnya bidang ini melakukan fragmentasi, lihat bagian Detail yang berjudul “Fragmentasi IP.”)

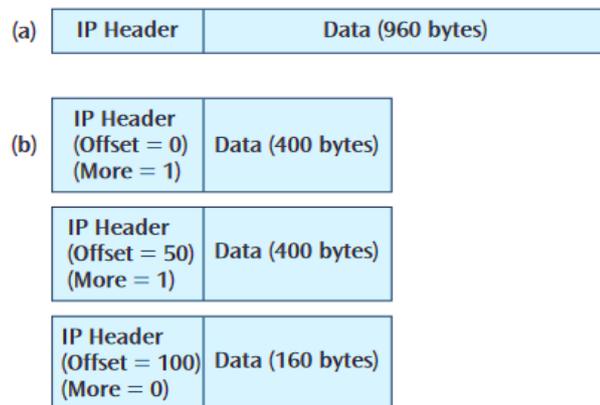
Bidang berikutnya yang akan kita periksa adalah bidang Time to Live, yang memungkinkan jaringan membuang datagram yang sudah terlalu lama menjelajahi Internet. Bidang Time to Live menunjukkan berapa lama datagram tertentu dibiarkan hidup—terpental dari router ke router—di dalam sistem. Ketika sebuah paket pertama kali dibuat, field ini diatur ke nilai maksimumnya: 255. Setiap router sepanjang rute dari sumber ke tujuan mengurangi angka di field Time to Live sebesar 1. Ketika nilai field Time to Live mencapai 0, router menghapus data-gram. Bidang Time to Live analog dengan jumlah hop dan batas hop yang diperkenalkan di Bab Sembilan. Bidang lain—Header Checksum—melakukan checksum aritmatika hanya pada bagian header paket.

Fragmentasi IP

Sebagai contoh fragmentasi IPv4, perhatikan datagram IPv4 yang ditunjukkan pada Gambar 10-5(a). Bagian data dari datagram panjangnya 960 byte. Datagram ini perlu melintasi jaringan tertentu yang membatasi porsi data datagram hingga 400 byte. Oleh karena itu, ada kebutuhan untuk membagi datagram asli menjadi tiga fragmen berukuran 400, 400, dan 160 byte. Ketiga fragmen yang dibuat memiliki header IP yang hampir sama.

Bidang Fragmen Offset berisi offset, yang merupakan hitungan, dalam satuan 8 byte, dari awal bidang data-gram asli hingga fragmen khusus ini. Gambar 10-5(b) menunjukkan offset ini. Fragmen pertama yang tidak diimbangi dari awal mempunyai nilai offset 0. Karena fragmen pertama panjangnya 400 byte, maka fragmen kedua harus memulai 400 byte ke dalam datagram asli. Kita menghitung dalam satuan 8 byte, jadi 400 dibagi 8 sama dengan offset 50. Dua fragmen pertama berjumlah 800 byte, jadi fragmen ketiga dan terakhir memulai 800 byte ke dalam datagram asli. Membagi 800 byte dengan unit 8 byte sama dengan offset 100.

Bidang berikutnya yang membantu dalam fragmentasi adalah bidang Bendera. Di dalam field Flags terdapat sedikit More, yang menunjukkan apakah ada lebih banyak fragmen dari datagram asli yang akan diikuti. Gambar 10-5(b) juga menunjukkan isi dari bit More. Sedikit lebih dari 1 menunjukkan, seperti yang Anda lihat pada dua paket pertama, bahwa lebih banyak fragmen yang akan datang; Sedikit lebih dari 0 menandakan fragmen terakhir dari sebuah paket. Bidang terakhir yang membantu dalam fragmentasi adalah bidang Identifikasi. Bidang Identifikasi berisi ID unik untuk ketiga fragmen ini yang digunakan untuk menyusun kembali ketiga fragmen tersebut kembali ke datagram asli.



Gambar 10-5 Pembagian datagram IPv4 menjadi tiga fragmen

Dua bidang terakhir yang menarik, Alamat IP Sumber dan Alamat IP Tujuan, masing-masing berisi alamat sumber awal IP 32-bit dan alamat tujuan akhir datagram. Alamat 32-bit secara unik mendefinisikan koneksi ke Internet—biasanya stasiun kerja atau perangkat, meskipun satu stasiun kerja atau perangkat mungkin mendukung beberapa koneksi Internet. Saat datagram IP bergerak melalui Internet, bidang Alamat IP Tujuan diperiksa oleh router. Router, menggunakan beberapa algoritma routing, meneruskan datagram ke link komunikasi berikutnya yang sesuai.

Alamat IPv4

Seperti yang telah disebutkan, alamat IPv4 panjangnya 32 bit. Misalnya, alamat IPv4 yang valid mungkin terlihat seperti berikut:

1000 0000 1001 1100 0000 1110 0000 0111

Untuk membuat alamat IPv4 lebih mudah dipahami manusia, alamat biner 32-bit ini diwakili oleh notasi desimal titik-titik. Notasi desimal bertitik ini dibuat dengan mengubah setiap string 8-bit dalam alamat IP 32-bit menjadi padanan desimalnya. Sehingga IP Address diatas menjadi 128.156.14.7 seperti gambar dibawah ini:

1000 0000 1001 1100 0000 1110 0000 0111
128 156 14 7

Ketika IP dan alamat IP dibuat pada tahun 1960an, sebuah alamat IP termasuk dalam kelas tertentu. Jenis pengalamatan ini disebut pengalamatan classful, dan didasarkan, seperti yang akan kita lihat sebentar lagi, pada lima kelas yang berbeda. Sekitar tahun 1996, bentuk pengalamatan baru tersedia: pengalamatan tanpa kelas. Meskipun pengalamatan tanpa kelas lebih umum saat ini, penting untuk memahami cara kerja kedua sistem ini. Untuk memulainya, kita akan memeriksa pengalamatan kelas.

Seperti yang telah Anda pelajari, alamat IPv4 panjangnya 32 bit. Namun, dalam pengalamatan classful, alamatnya bukanlah bilangan bulat 32-bit sederhana. Sebaliknya, mereka dapat terdiri dari tiga informasi spesifik. Ukuran dan nilai ketiga informasi ini bergantung pada bentuk dasar alamatnya. Ada lima bentuk dasar alamat IP: Kelas A, B, C, D, dan E (Tabel 10-1).

Tabel 10-1 Lima bentuk dasar alamat IP 32-bit

Tipe Alamat	Pola Bit Awal	Alamat Jaringan (Net ID)	Alamat Host (Host ID)
Kelas A	0	128 Alamat (7 Bit)	16.777.216 Alamat (24 Bit)
Kelas B	10	16.384 Alamat (14 Bit)	65.536 Alamat (16 Bit)
Kelas C	110	2.097.152 Alamat (21 Bit)	256 Alamat (8 Bit)
Kelas D	1110	Alamat Multicast	
Kelas E	1111	Alamat yang Dicadangkan	

Seperti disebutkan sebelumnya, setiap alamat IP dapat terdiri dari tiga bagian:

- Bidang pengenalan 1-, 2-, 3-, atau 4-bit (juga dikenal sebagai pola bit awal)
- ID bersih, yang menunjukkan jaringan tertentu
- ID host, yang menunjukkan host atau komputer tertentu pada jaringan tersebut

Seperti yang ditunjukkan Tabel 10-1, dengan pola bit awal 0, terdapat 128 alamat atau jaringan Kelas A. Setiap alamat Kelas A dapat memiliki 16.777.216 host, atau komputer. Jelasnya, 128 bukanlah jaringan yang banyak; faktanya, seluruh 128 alamat Kelas A telah diberikan sejak lama. Fitur lain yang tidak praktis dari tipe alamat Kelas A adalah alokasi 16.777.216 komputer per jaringan. Melampirkan 16.777.216 komputer ke satu jaringan sungguh di luar imajinasi. Seperti yang telah kita lihat, banyak jaringan area lokal jarang mempunyai lebih dari beberapa ribu komputer yang terpasang padanya. Sayangnya, karena alasan ini, banyak alamat Kelas A yang tidak digunakan. Alamat kelas B memungkinkan 16.384 net ID, atau jaringan, masing-masing mendukung 65.536 host ID—artinya masing-masing dari 16.384 jaringan dapat memiliki 65.536 komputer host yang terpasang padanya. Alamat Kelas C memungkinkan 2.097.152 ID bersih, atau jaringan, dan 256 ID host. Dalam kasus tipe alamat Kelas C, jumlah komputer host yang diperbolehkan terlalu kecil untuk mengakomodasi jaringan apa pun kecuali yang terkecil.

Alamat kelas D tersedia untuk jaringan yang memungkinkan multicasting pesan. Multicasting IP adalah kemampuan server jaringan untuk mengirimkan aliran data ke lebih dari satu host pada satu waktu. Pertimbangkan skenario di mana perusahaan ingin mengunduh video streaming latihan kepada 20 pengguna yang duduk di stasiun kerja terpisah.

Jika server harus mengirimkan 20 salinan individual ke 20 stasiun kerja (unicast), diperlukan sinyal bandwidth yang sangat tinggi. Jika server dapat melakukan multicast satu salinan aliran video ke 20 stasiun kerja, diperlukan bandwidth yang jauh lebih kecil. Untuk multicast, server dapat memasukkan alamat Kelas D ke dalam datagram IP, dan masing-masing dari 20 stasiun kerja dapat memberitahu perangkat lunak IP-nya untuk menerima datagram apa pun dengan alamat Kelas D ini.

Meskipun multicasting IP memiliki beberapa keuntungan yang sangat menjanjikan, namun memiliki kelemahan dalam hal keamanan. Karena relatif mudah bagi stasiun kerja untuk memberi tahu perangkat lunak IP-nya agar menerima alamat Kelas D tertentu, stasiun kerja mana pun—bahkan yang tidak memiliki izin—berpotensi menerima multicast. Meskipun demikian, aplikasi baru yang mengatasi kekurangan multicasting IP telah diumumkan, membuka pintu bagi kemungkinan-kemungkinan di masa depan.

Ketika sebuah perusahaan mengajukan serangkaian alamat Internet yang menggunakan pengalamatan classful, sejumlah opsi dapat dilakukan. Pertama, perusahaan dapat mengajukan alamat Kelas B. Dengan alamat Kelas B, ia dapat mengalokasikan 65.536 workstation pada jaringan Kelas B-nya. Jika jumlah stasiun kerja ini terlalu besar, perusahaan dapat mempertimbangkan alamat Kelas C. Alamat Kelas C memungkinkan 256 komputer dalam satu jaringan. Namun jika perusahaan memiliki 400 hingga 500 pengguna, alamat Kelas C akan terlalu kecil. Oleh karena itu, perusahaan dapat mengajukan dua alamat Kelas C.

Misalkan sebuah perusahaan mengajukan permohonan dan menerima alamat Kelas B dalam jumlah besar. Bagaimana cara menggunakan ini secara efisien? Dalam hal ini, perusahaan dapat memecah alamat IP-nya menjadi subnet menggunakan subnet masking, sebuah teknik yang memungkinkan pengelolaan jaringan lebih mudah. Ide dasar di balik subnet masking adalah mengambil bagian ID host dari sebuah alamat IP dan selanjutnya membaginya menjadi ID subnet dan ID host. Dengan menggunakan teknik ini, ISP dan perusahaan dapat mengambil ID host dalam jumlah besar dan memecahnya menjadi subnet. Setiap subnet kemudian dapat mendukung sejumlah kecil host.

Dengan pengalamatan tanpa kelas, perusahaan (pengguna) tidak mengajukan permohonan untuk kelas alamat tertentu. Sebaliknya, perusahaan akan mendapatkan alamat IP-nya dari ISP. Sebagian besar ISP telah mengajukan permohonan untuk sejumlah besar alamat IP dan bersedia untuk menyewakan alamat tersebut kepada perusahaan. Kembali ke contoh sebelumnya, alih-alih mengajukan dua alamat Kelas C, perusahaan dengan 400 hingga 500 pengguna dapat menghubungi ISP dan meminta untuk menyewa 512 alamat IP (jumlah alamat yang diminta harus pangkat 2). Alamat-alamat ini, setidaknya dari sudut pandang perusahaan, tidak teridentifikasi oleh kelas mana pun—alamat-alamat tersebut hanyalah sebuah blok alamat IP yang berdekatan. Misalnya, ISP dapat memberikan 512 alamat kepada sebuah perusahaan dan menunjukkannya sebagai berikut:

162.48.128.0/23

Bentuk ini disebut notasi garis miring. Alamat 162.48.128.0 adalah alamat awal dari blok alamat. /23 menunjukkan berapa banyak dari 32 bit alamat yang dialokasikan ke bagian ID jaringan. Jadi, 23 bit pertama dialokasikan ke ID jaringan, menyisakan 9 bit untuk ID host. Jika kita mempunyai ID host 9-bit, maka kita mempunyai 29, atau 512 ID host.

Seperti yang sudah Anda duga, pengalamatan tanpa kelas telah menghasilkan alokasi ruang alamat IP yang jauh lebih efisien. Sebuah perusahaan sekarang dapat menyewa alamat yang mendekati jumlah pasti yang dibutuhkannya tanpa membuang alamat yang tidak terpakai.

Ketika pengalamatan tanpa kelas digabungkan dengan DHCP dan NAT, perusahaan dapat menggunakan lebih sedikit alamat IP secara efisien. Hal ini karena ketiga konsep tersebut lebih efektif memanfaatkan ruang alamat IP. Meskipun alamat IP 32-bit mendukung lebih dari 4 miliar alamat, pengalamatan classful sangat boros sehingga terdapat kekhawatiran serius di kalangan pakar industri bahwa persediaan alamat IP akan segera habis. Munculnya pengalamatan tanpa kelas (bersama dengan protokol DHCP dan NAT) telah sangat membantu memperlambat pengurusan alamat IP. Meskipun demikian, ada dorongan untuk memasukkan versi baru dari Protokol Internet, IPv6, yang memiliki ruang alamat yang jauh lebih besar. Kami akan menyelidiki protokol baru ini selanjutnya.

Protokol Internet versi 6

Ketika Protokol Internet diciptakan pada tahun 1960an, iklim komputasi tidak sama seperti sekarang. Jumlah pengguna yang saat ini menggunakan Internet sangatlah sedikit, dan jalur telekomunikasi yang digunakan untuk mendukung jaringan berkecepatan tinggi tidak secepat dan bebas kesalahan seperti saat ini. Selain itu, aplikasi yang dikirimkan melalui Internet melibatkan paket data yang lebih kecil, dan tidak ada permintaan untuk mengirimkannya secara real time. Ketika tuntutan terhadap Internet mulai meningkat, para perancang memutuskan sudah waktunya untuk menciptakan Protokol Internet yang lebih modern yang memanfaatkan teknologi saat ini. Dengan demikian, IPv6 telah dibuat.

Ada beberapa perbedaan penting antara IPv6 dan IPv4 lama. Yang pertama menyangkut penanganan. Seperti yang telah Anda pelajari, IPv4 menggunakan alamat 32-bit. Dengan pesatnya pertumbuhan Internet, muncul kekhawatiran bahwa sistem yang ada saat ini akan kehabisan alamat IP dalam waktu yang tidak lama lagi. Mereka benar: Kami kehabisan alamat IPv4 pada tahun 2011. Akibatnya, IPv6 memerlukan alamat yang panjangnya 128 bit. Alamat 128-bit memberi kita alamat yang hampir tidak terbatas. Dengan alamat 128-bit, Internet akan mampu menetapkan 1 juta alamat IP setiap pikodetik (10–12 detik) sesuai usia alam semesta yang diketahui! Tentu saja, dengan IPv6, kita tidak akan pernah kehabisan alamat.

Version	Priority	Flow Label	Payload Length	
4 bits	4 bits	24 bits	16 bits	
Next Header	Hop Limit	Source Address		
8 bits	8 bits	128 bits		
		Destination Address		
		128 bits		
		Payload + Extension Headers		

Gambar 10-6 Bidang di header IPv6

Perubahan signifikan juga dilakukan pada header IP antara versi 4 dan versi 6. Seperti yang Anda ingat dari Gambar 10-4, header IP di versi 4 berisi 14 kolom. Di IPv6, header IP berisi delapan kolom, ditambah payload (data) dan header ekstensi opsional, seperti yang ditunjukkan pada Gambar 10-6. Seperti halnya header IPv4, kolom pertama panjangnya empat bit dan mewakili nomor versi. Bidang kedua adalah bidang Prioritas, yang memungkinkan nilai 0 hingga 7 untuk transmisi yang mampu memperlambat, dan nilai 8 hingga 15 untuk menunjukkan data waktu nyata. Bidang ini berguna untuk menetapkan prioritas pada satu atau lebih paket; aliran data dengan prioritas lebih tinggi dapat dilayani lebih cepat daripada paket dengan prioritas lebih rendah. Bidang ketiga adalah Label Aliran; bidang ini memungkinkan sumber dan tujuan untuk membuat koneksi semu yang memiliki properti dan persyaratan tertentu. Hal ini akan memungkinkan aplikasi dan koneksi tertentu merutekan paketnya melalui Internet dengan lebih cepat. Bidang keempat adalah Panjang Payload, yang mengidentifikasi berapa banyak byte yang mengikuti header 40-byte. Bidang kelima disebut Header Berikutnya dan memberitahukan yang mana, jika ada, dari enam header ekstensi yang menyusul. Jika tidak ada header ekstensi yang mengikuti Header Berikutnya, maka Header Berikutnya hanya memberi tahu header lapisan transport mana (TCP, UDP, dan seterusnya) yang mengikuti. Bidang keenam adalah Hop Limit, yang menyatakan berapa lama datagram tertentu dibiarkan hidup—melompat dari satu jaringan ke jaringan lain—di dalam sistem; ini memberikan informasi yang sama seperti bidang Time to Live di IPv4. Dua kolom terakhir adalah Alamat Sumber dan Alamat Tujuan. Perhatikan bahwa kedua bidang alamat panjangnya 128 bit.

Bidang mana di IPv4 yang tidak lagi ada di header IPv6? IPv6 tidak memiliki bidang Panjang Header. Karena header di versi baru memiliki panjang yang tetap, bidang panjang tidak diperlukan. Bidang lain yang tidak termasuk dalam IPv6 adalah bidang yang memungkinkan fragmentasi. Pencipta IPv6 merasa bahwa sebagian besar jaringan yang beroperasi saat ini dapat menangani paket berukuran sangat besar, dan tidak perlu lagi memecah (atau memfragmentasi) sebuah paket menjadi bagian-bagian yang lebih kecil. Jadi, meskipun IPv6 dapat melakukan fragmentasi, fungsi ini hanya tersedia sebagai opsi di header ekstensi. Namun bidang lain yang ketidakhadirannya di IPv6 mengejutkan adalah bidang Checksum. Menghilangkan bidang Checksum tampaknya menjadi tren di sebagian besar

jaringan modern, karena kualitas jaringan meningkat dan aplikasi tingkat yang lebih tinggi berperan sebagai pendeteksi kesalahan.

Meskipun modifikasi pada header IP menunjukkan perubahan besar dalam protokol, terdapat perbedaan yang lebih signifikan antara IPv4 dan IPv6. Yaitu, IPv6 memiliki:

- Dukungan yang lebih baik untuk opsi menggunakan header ekstensi
- Keamanan yang lebih baik, dengan dua header ekstensi yang ditujukan sepenuhnya untuk keamanan
- Lebih banyak pilihan dalam jenis layanan

Peningkatan terakhir pada IP berkaitan dengan kualitas layanan (QoS), yang merupakan bagian penting dari jaringan modern. Ini adalah alat yang sangat berguna jika pengguna dapat menentukan tingkat layanan tertentu dan jaringan dapat mendukung tingkat tersebut. IPv6 seharusnya memberikan kualitas layanan yang jauh lebih baik daripada IPv4.

Sayangnya, meskipun terdapat perbaikan-perbaikan ini, masih belum diketahui kapan IPv6 akan menggantikan IPv4. Meskipun Kantor Manajemen dan Anggaran A.S. mengumumkan pada tahun 2005 bahwa mereka bermaksud untuk memerlukan dukungan protokol di seluruh lembaga pemerintah pada tahun 2008, perusahaan-perusahaan Amerika sangat lambat dalam mengadopsi protokol baru ini. Ada beberapa alasan untuk hal ini. Banyak pengguna yang mengeluh bahwa fitur-fitur baru yang ditawarkan oleh IPv6 tidak jauh berbeda dengan fitur-fitur yang telah ditambahkan ke IPv4 selama beberapa tahun terakhir. Selain itu, meskipun ruang alamat 128-bit menawarkan jumlah alamat yang tak terbayangkan, ia menghabiskan 16 byte ruang paket. Jika perangkat perlu mengirim paket kecil, ruang alamat saja akan mencakup sebagian besar paket. Terakhir, banyak pengelola jaringan suka menggunakan protokol NAT dan DHCP IPv4. Protokol ini memungkinkan mereka untuk menggunakan ruang alamat IP perusahaan secara konservatif, sekaligus menjaga kerahasiaan struktur alamat IP internal dari dunia luar. Mungkin tahun 2012 akan menjadi tahun dimana IPv6 benar-benar lepas landas.

Alamat IPv6

Alamat IPv6 memiliki beberapa properti unik yang membuatnya menonjol dari alamat IPv4. Yang pertama dan terpenting adalah ukurannya. Seperti yang telah disebutkan, alamat IPv6 memiliki panjang 128 bit. Ini menyediakan sumber alamat IP yang hampir tidak terbatas. Ukurannya saja membuat sulit untuk mereferensikannya. Misalnya, biasanya ditulis dalam bentuk heksadesimal, di mana setiap kuantitas empat bit diganti dengan digit heksadesimal dari 0 hingga F. Berikut salah satu contoh alamat IPv6:

Biner:

0110 1010 0011 1110 1011 1010 ... 11101111

Heksadesimal:

6A3E : BA91 : 7221 : 0000 : 01FC : 922C : 877B : FFEF

Jika ada empat hex 0 berturut-turut, seperti di atas, kita dapat menghemat sedikit pengetikan dan memasukkan singkatan kecil:

```
6A3E : BA91 : 7221 : 0 : 01FC : 922C : 877B : FFEF
```

String 0 yang lebih panjang dapat disingkat lebih lanjut. Misalnya,

```
6A3E : BA91 : 0 : 0 : 0 : 0 : 877B : FFEF
```

dapat disingkat menjadi

```
6A3E : BA91 : : 877B : FFEF
```

Perhatikan bahwa singkatan seperti ini hanya dapat muncul satu kali dalam sebuah alamat IP (untuk menghindari kebingungan). Alamat IPv6 juga tidak berkelas dan menggunakan notasi garis miring. Jadi alamat seperti

```
6A3E : BA91 : : 877B : FFEF/104
```

memberitahu kita bahwa 104 bit pertama adalah bagian dari ID jaringan, dan 24 bit sisanya adalah bagian dari ID host.

Protokol Internet jelas merupakan salah satu protokol komunikasi yang paling penting. Karena desainnya yang sederhana, maka relatif mudah untuk diterapkan di berbagai macam perangkat. Dan karena kekuatannya, ia mampu menghubungkan jaringan apa pun jenisnya. Meskipun Protokol Internet sangat kuat, tujuan utamanya adalah mendapatkan data melalui satu atau lebih jaringan. Itu tidak bertanggung jawab untuk membuat koneksi ujung ke ujung yang bebas kesalahan. Untuk mencapai hal ini, Protokol Internet bergantung pada Protokol Kontrol Transmisi.

Protokol Kontrol Transmisi

Mungkin salah satu contoh paling umum dari protokol lapisan transport adalah separuh protokol TCP/IP yang populer. Fungsi utama dari Protokol Kontrol Transmisi (TCP) adalah untuk mengubah jaringan yang tidak dapat diandalkan (seperti jaringan yang dibuat oleh IP) menjadi jaringan yang dapat diandalkan yang bebas dari paket yang hilang dan terduplikasi. Jadi, TCP pada dasarnya mengisi beberapa lubang yang dibuat oleh IP. Namun bagaimana protokol lapisan transport dapat membuat jaringan yang tidak dapat diandalkan menjadi dapat diandalkan? Untuk membuat jaringan lebih handal, TCP melakukan enam fungsi berikut:

- **Buat koneksi**—Header TCP menyertakan alamat port yang menunjukkan aplikasi tertentu pada mesin. Digunakan bersama, alamat port dan alamat IP mengidentifikasi aplikasi tertentu dari mesin tertentu. Ketika TCP membuat koneksi antara pengirim dan penerima, kedua ujung koneksi menggunakan nomor port untuk mengidentifikasi koneksi aplikasi

tertentu. Nomor port ini ditemukan dalam datagram TCP dan diteruskan bolak-balik antara pengirim dan penerima.

- **Melepaskan sambungan**—Perangkat lunak TCP juga dapat memutuskan sambungan setelah semua data dikirim dan diterima.
- **Menerapkan kontrol aliran**—Untuk memastikan stasiun pengirim tidak membebani stasiun penerima dengan terlalu banyak data, header TCP menyertakan sebuah field, yang disebut nilai Window, yang memungkinkan penerima memberitahu pengirim untuk memperlambat. Nilai Window ini serupa dalam pengoperasiannya dengan jendela geser yang digunakan pada lapisan data link. Perbedaan antara dua operasi jendela ini adalah bahwa jendela geser lapisan data link beroperasi antara dua node atau antara stasiun kerja dan sebuah node, sedangkan jendela TCP beroperasi antara dua titik akhir (pengirim dan penerima) dari koneksi jaringan.
- **Membangun multiplexing**—Karena header TCP menyertakan nomor port dan bukan alamat IP, maka dimungkinkan untuk melakukan multipleks beberapa koneksi melalui satu koneksi IP. Multiplexing ini dapat dilakukan dengan membuat koneksi berbeda yang mempunyai nomor port berbeda dengan koneksi sebelumnya.
- **Lakukan pemulihan kesalahan**—TCP memberi nomor pada setiap byte untuk transmisi dengan nomor urut. Ketika paket byte tiba di lokasi tujuan, perangkat lunak TCP penerima memeriksa nomor urut ini untuk kontinuitas. Jika ada hilangnya kontinuitas, perangkat lunak TCP penerima menggunakan nomor pengakuan untuk menginformasikan perangkat lunak TCP pengirim tentang kemungkinan kondisi kesalahan.
- **Tetapkan prioritas**—Jika pengirim harus mengirimkan data dengan prioritas lebih tinggi, seperti kondisi kesalahan, TCP dapat menetapkan nilai dalam bidang (Penunjuk Urgent) yang menunjukkan bahwa semua atau sebagian data terlampir bersifat mendesak. alam.

Untuk menjalankan enam fungsi ini, TCP menempatkan header di depan setiap paket data yang berpindah dari pengirim ke penerima, atau dari satu ujung koneksi ke ujung lainnya. Seperti yang kita lakukan dengan header IP, mari kita periksa bidang yang lebih penting di header TCP.

Format Datagram TCP

Seorang pengguna sedang duduk di stasiun kerja dan menjalankan aplikasi jaringan—misalnya, program email. Ketika pengguna ingin mengirim pesan email, program email mengambil pesan email tersebut dan meneruskannya ke lapisan transport perangkat lunak. Jika email dikirim ke Internet, lapisan transport menambahkan header TCP di bagian depan pesan email. Informasi dalam header ini digunakan oleh lapisan TCP di stasiun kerja penerima untuk melakukan satu atau lebih dari enam fungsi transport. Header TCP berisi bidang yang ditunjukkan pada Gambar 10-7. Mari kita periksa hanya bidang-bidang yang membantu TCP dalam menjalankan enam fungsi yang disebutkan sebelumnya.

Source Port	Destination Port	Sequence Number		
16 bits	16 bits	32 bits		
Acknowledgment Number	Hlen	Reserved	Flags	Window
32 bits	4 bits	6 bits	6 bits	16 bits
Checksum	Urgent Pointer	Options		Padding
16 bits	16 bits	Variable Length		Optional
Data				
Variable Length				

Gambar 10-7 Bidang header TCP

Dua bidang header TCP pertama, Port Sumber dan Port Tujuan, berisi alamat program aplikasi di kedua ujung koneksi transport. Alamat port ini digunakan dalam membuat dan mengakhiri koneksi. Nomor port juga dapat digunakan untuk multipleks beberapa koneksi transport melalui satu koneksi IP.

Penting untuk memperhatikan perbedaan antara alamat IP dan nomor port. Alamat IP mengidentifikasi perangkat yang terhubung ke Internet, sedangkan nomor port mengidentifikasi aplikasi pada perangkat tersebut. Bekerja sama, keduanya menciptakan apa yang disebut soket—identifikasi tepat dari aplikasi tertentu pada perangkat tertentu. Bagaimana jika perusahaan Anda memiliki satu server yang menangani koneksi email dan FTP? Server akan memiliki satu alamat IP tetapi dua nomor port berbeda: satu untuk aplikasi email dan satu lagi untuk aplikasi FTP. Sekarang mari kita tambahkan fakta bahwa server ini kemungkinan besar berada di jaringan area lokal, dan karenanya memiliki kartu antarmuka jaringan dengan alamat NIC 48-bit yang unik. Sekarang kami memiliki tiga alamat. Alamat NIC hanya digunakan pada jaringan area lokal untuk menemukan perangkat tertentu. Alamat IP digunakan untuk memindahkan paket data melalui Internet. Nomor port digunakan untuk mengidentifikasi aplikasi tertentu pada perangkat.

Bidang Nomor Urutan berisi nilai 32-bit yang menghitung byte dan menunjukkan posisi data paket dalam koneksi. Misalnya, jika Anda berada di tengah-tengah koneksi panjang di mana ribuan byte sedang ditransfer, Nomor Urutan memberi tahu Anda posisi pasti paket ini dalam urutan tersebut. Bidang ini dapat digunakan untuk memasang kembali bagian-bagian di stasiun kerja penerima dan menentukan apakah ada paket data yang hilang.

Bidang Window berisi nilai jendela geser yang memberikan kontrol aliran antara dua titik akhir. Jika salah satu ujung koneksi ingin ujung koneksi lainnya berhenti mengirim data, field Window dapat diatur ke 0. Field Checksum adalah field berikutnya, dan menyediakan checksum aritmatika dari header dan data. bidang yang mengikuti header. Urgent Pointer digunakan untuk menginformasikan stasiun kerja penerima bahwa paket data ini berisi data penting.

Seperti IP mitranya, TCP adalah protokol yang cukup efisien. Tujuan utamanya adalah menciptakan koneksi end-to-end yang bebas kesalahan di satu atau lebih jaringan. Namun TCP dan IP mempunyai kekurangan, dan hal ini biasanya menyebabkan masalah seperti kelemahan

keamanan, masalah kualitas layanan, dan pengendalian kemacetan. Oleh karena itu, kedua protokol ini perlu terus berkembang. Namun meski begitu, komponen dasarnya harus tetap ada dalam jangka waktu yang lama.

Protokol Pesan Kontrol Internet

Saat datagram IP bergerak melalui jaringan, ada beberapa hal yang bisa salah. Ketika datagram mendekati tujuan yang dituju, router mungkin menentukan bahwa host tujuan tidak dapat dijangkau (alamat IP salah, atau host tidak ada), port tujuan tidak diketahui (tidak ada aplikasi yang cocok dengan nomor port TCP), atau jaringan tujuan tidak diketahui (sekali lagi, alamat IP salah). Jika suatu datagram telah berada di jaringan terlalu lama dan nilai Time to Live-nya habis masa berlakunya, datagram tersebut akan dibuang. Selain itu, mungkin ada yang salah dengan keseluruhan header IP datagram. Dalam setiap kasus ini, langkah baiknya jika router atau perangkat lain mengirimkan pesan kesalahan kembali ke stasiun kerja sumber, memberi tahu pengguna atau perangkat lunak aplikasi tentang suatu masalah. Protokol Internet tidak dirancang untuk mengembalikan pesan kesalahan, jadi ada hal lain yang harus dilakukan untuk melakukan operasi ini.

Internet Control Message Protocol (ICMP), yang digunakan oleh router dan node, melakukan pelaporan kesalahan ini untuk Protokol Internet. Semua pesan ICMP berisi setidaknya tiga bidang: tipe, kode, dan delapan byte pertama dari datagram IP yang menyebabkan pesan ICMP dihasilkan. Tipe hanyalah angka dari 0 hingga n yang secara unik mengidentifikasi jenis pesan ICMP, misalnya nomor port tidak valid atau alamat IP tidak valid. Kode adalah nilai yang memberikan informasi lebih lanjut tentang jenis pesan. Bersama-sama, ICMP dan IP menyediakan operasi jaringan yang relatif stabil yang dapat melaporkan beberapa bentuk dasar kesalahan jaringan.

Protokol Datagram Pengguna

TCP adalah protokol yang digunakan oleh sebagian besar jaringan dan aplikasi jaringan untuk membuat koneksi jaringan ujung ke ujung yang bebas kesalahan. TCP berorientasi pada koneksi di mana koneksi melalui nomor port harus dibuat sebelum data apa pun dapat ditransfer antara pengirim dan penerima. Bagaimana jika Anda tidak ingin membuat sambungan dengan penerima tetapi hanya ingin mengirim paket data? Dalam hal ini, User Datagram Protocol adalah protokol yang digunakan. User Datagram Protocol (UDP) adalah protokol transport tanpa embel-embel yang tidak membuat koneksi, tidak berusaha menjaga paket data secara berurutan, dan tidak memperhatikan datagram yang sudah ada terlalu lama. Headernya hanya berisi empat bidang— Port Sumber, Port Tujuan, Panjang, dan Checksum—dan digunakan oleh sejumlah kecil layanan jaringan, seperti DNS yang tidak perlu membuat sambungan sebelum mengirim data.

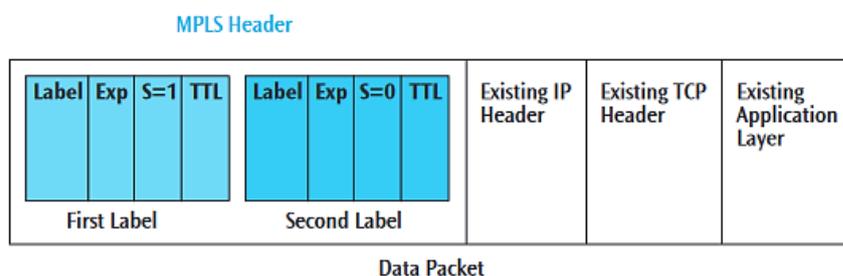
Peralihan Label Multiprotokol

Sepanjang buku teks sejauh ini, enkapsulasi telah menjadi konsep kunci. Ingatlah bahwa enkapsulasi adalah pelapisan header satu lapisan di atas paket data yang ada. Seperti yang baru saja kita lihat, dalam rangkaian protokol TCP/IP, header TCP ditempatkan di atas (ditempatkan di depan) paket yang berasal dari lapisan aplikasi. Informasi dalam header TCP digunakan untuk menjalankan fungsi koneksi lapisan transport pada titik akhir koneksi.

Kemudian header IP ditempatkan di atas paket TCP, dan informasi dalam header IP digunakan untuk melakukan perutean jaringan dan operasi Time to Live. Biasanya, langkah selanjutnya adalah menempatkan informasi lapisan akses jaringan di atas paket IP. Namun jaringan area luas tidak menggunakan informasi lapisan akses jaringan untuk merutekan paket data. Oleh karena itu, router harus “menggali” paket data, mengekstrak informasi IP, dan menggunakannya untuk routing. Ini biasanya bukan proses yang cepat, setidaknya tidak jika dibandingkan dengan operasi penerusan yang dapat dilakukan oleh switch jaringan area lokal. Jika jaringan area luas dapat melakukan operasi peralihan dengan cepat, Internet (serta jaringan area luas lainnya) akan beroperasi lebih efisien.

Untuk menyediakan tingkat peralihan ini di tingkat jaringan, perancang jaringan telah menciptakan Peralihan Label Multiprotokol. *Multiprotocol Label Switching* (MPLS) adalah teknik yang memungkinkan router untuk mengalihkan data dari satu jalur ke jalur lainnya. Untuk memungkinkan hal ini, satu atau lebih label (header dengan informasi MPLS) dienkapsulasi ke bagian depan paket IP (Gambar 10-8). Setiap label berisi empat bidang:

- Bidang Nilai Label 20-bit (Label)
- Bidang Eksperimental 3-bit (dicadangkan untuk penggunaan di masa mendatang) (Exp)
- Bidang Bendera Tumpukan Bagian Bawah 1-bit ($S = 0$)
- Bidang Time to Live (TTL) 8-bit



Gambar 10-8 Dua header MPLS dan empat fieldnya

Nilai label 20-bit pada dasarnya memberi tahu router berkemampuan MPLS yang menghubungkan paket ini dan bagaimana meneruskan paket tersebut. Bidang Bottom of Stack Flag 1-bit menunjukkan apakah ada beberapa label pada paket ini (0 jika ini adalah label terakhir dan 1 jika sebaliknya). Bidang Time to Live 8-bit berfungsi serupa dengan bidang Time to Live di header IP. Ketika sebuah paket dimasukkan ke dalam jaringan, router berkemampuan MPLS menentukan koneksi paket tersebut dan memasukkan satu atau lebih label ke dalam header MPLS yang baru dibuat. Paket tersebut sekarang disebut paket berlabel. Router berkemampuan MPLS berikutnya melihat informasi di header MPLS dan meneruskan paket berlabel ke arah yang sesuai. Untuk setiap paket berlabel yang masuk, router berkemampuan MPLS dapat memiliki tabel perutean bawaan yang memberi tahu router jenis operasi apa yang harus dilakukan berdasarkan label MPLS paling atas dari paket tersebut. Operasi ini dilakukan dengan cepat, seringkali di perangkat keras.

Ketika paket berlabel tiba di router tujuan, router berkemampuan MPLS menghapus header MPLS, meninggalkan paket IP asli. MPLS semakin populer di jaringan besar dan merupakan standar Satuan Tugas Rekayasa Internet. Seperti yang akan kita lihat di Bab Sebelas, suatu hari nanti mungkin akan menggantikan atau setidaknya membantu penggantian protokol jaringan area luas lainnya.

Protokol Resolusi Alamat

Protokol Resolusi Alamat adalah protokol kecil namun penting lainnya yang digunakan untuk mendukung jaringan TCP/IP. Address Resolusi Protocol (ARP) mengambil alamat IP dalam datagram IP dan menerjemahkannya ke dalam alamat lapisan kontrol akses media yang sesuai untuk pengiriman pada jaringan area lokal. Seperti disebutkan sebelumnya, setiap workstation yang memiliki koneksi ke Internet diberi alamat IP. Alamat IP inilah yang digunakan paket untuk menemukan jalannya ke tujuan yang dituju. Namun ada satu masalah ketika workstation aktif, misalnya jaringan area lokal Ethernet atau CSMA/CD. Ingatlah bahwa bagian data yang melintasi LAN CSMA/CD disebut frame. Frame ini terdiri dari sejumlah field informasi, tidak ada satupun yang merupakan alamat IP. Jika frame seharusnya menuju ke workstation tertentu dengan alamat IP yang unik, namun frame tersebut tidak berisi alamat IP, bagaimana frame mengetahui ke mana harus pergi? ARP memberikan jawaban atas pertanyaan ini. Setelah datagram IP memasuki LAN CSMA/CD melalui router, dan sebelum header IP-nya dilepas sehingga hanya menyisakan frame CSMA/CD, ARP menyiarkan pesan di LAN yajumatan ng menanyakan stasiun kerja mana yang memiliki alamat IP ini. Workstation yang mengenali alamat IP-nya mengirimkan pesan kembali yang mengatakan, “Ya, itu adalah alamat IP saya, dan ini adalah alamat CSMA/CD (NIC) 48-bit saya. Tolong teruskan paket IP itu kepada saya melalui alamat saya.” (Alamat NIC 48-bit disimpan dalam buffer untuk berjajaga-jaga jika diperlukan lagi dalam waktu dekat.)

Protokol Konfigurasi Host Dinamis

Ketika sebuah perusahaan memasang sejumlah stasiun kerja komputer dan bermaksud memberi mereka semua akses Internet, perusahaan tersebut harus memberikan alamat IP kepada masing-masing stasiun kerja tersebut. Alamat IP ini, seperti yang telah kita pelajari, memungkinkan stasiun kerja mengirim dan menerima informasi melalui Internet. Dua metode dasar yang digunakan untuk menetapkan alamat IP ke stasiun kerja: penetapan statis dan penetapan dinamis. Dengan penugasan statis, seseorang duduk di depan setiap mesin dan, dengan menggunakan sistem operasi jaringan, menetapkan alamat IP. Orang yang memasang alamat tersebut kemudian harus mencatat alamat IP tersebut di atas kertas di suatu tempat sehingga alamat IP tersebut tidak secara tidak sengaja diberikan ke komputer lain.

Apa yang terjadi jika stasiun kerja dengan alamat IP yang ditetapkan secara statis kemudian dihapus dari layanan? Seseorang harus memastikan alamat IP yang ditetapkan untuk mesin tersebut dihapus untuk digunakan di mesin lain. Bagaimana jika terjadi kesalahan, dan alamat IP yang sama diberikan ke dua mesin? Dalam hal ini, akan terjadi konflik alamat IP, dan administrator jaringan harus menemukan dua mesin dengan alamat IP yang sama dan memperbaiki situasinya. Masalah lain yang perlu dipertimbangkan adalah terkait

pengadaan alamat IP. Jika sebuah perusahaan mempunyai 1000 stasiun kerja dan setiap stasiun kerja mempunyai akses ke Internet, maka perusahaan tersebut harus memperoleh (biasanya menyewakan) 1000 alamat IP. Hal ini tidak hemat biaya, terutama jika hanya setengah dari pengguna yang menggunakan Internet (menggunakan alamat IP mereka) pada satu waktu. Penetapan alamat IP secara statis dapat menyebabkan pemborosan sumber daya. Penetapan alamat IP secara dinamis memecahkan ketiga masalah ini.

Protokol paling populer yang menangani penugasan dinamis adalah Dynamic Host Configuration Protocol (DHCP). Ketika stasiun kerja yang menjalankan perangkat lunak klien DHCP perlu terhubung ke Internet, protokol mengeluarkan permintaan IP, yang meminta server DHCP untuk mencari tabel alamat IP statis. Jika stasiun kerja tertentu ini memiliki entri, maka alamat IP tersebut diberikan ke stasiun kerja tersebut. Namun jika tidak ada entri dalam tabel statis, server DHCP memilih alamat IP dari kumpulan alamat yang tersedia dan menugaskannya ke stasiun kerja. Penetapan alamat IP bersifat sementara, dengan batas waktu default adalah satu jam. Klien DHCP dapat menegosiasikan pembaruan penugasan jika stasiun kerja masih mengakses Internet ketika penugasan sementara hampir habis masa berlakunya. Jadi, dengan DHCP, tiga masalah yang disebabkan oleh penugasan statis dapat diselesaikan. Tidak ada individu yang harus menetapkan alamat IP ke stasiun kerja; dua stasiun kerja tidak pernah diberi alamat IP yang sama; dan jika hanya 200 dari 1000 stasiun kerja yang menggunakan Internet pada saat yang sama, perusahaan mungkin dapat bertahan dengan hanya memperoleh 200 alamat IP.

Pengguna yang terhubung ke Internet dari rumah sering kali menggunakan DHCP tanpa menyadarinya. Daripada menetapkan alamat IP untuk setiap pengguna potensial, server DHCP penyedia layanan Internet memberikan alamat IP selama periode pembuatan sesi. Komputer menggunakan alamat IP sementara ini sampai pengguna logout, dan pada saat itu alamat tersebut ditempatkan kembali ke dalam kumpulan, siap untuk pengguna berikutnya.

Terjemahan Alamat Jaringan

Protokol lain yang digunakan untuk menetapkan alamat IP adalah Network Address Translation (NAT). Lebih tepatnya, NAT memungkinkan router mewakili seluruh jaringan area lokal ke Internet sebagai satu alamat IP. Ketika stasiun kerja pengguna di jaringan area lokal perusahaan mengirimkan paket ke Internet, NAT menggantikan alamat IP stasiun kerja pengguna dengan alamat IP global perusahaan. Faktanya, semua paket yang meninggalkan jaringan perusahaan berisi alamat IP global ini. Jadi, satu-satunya alamat IP yang dilihat siapa pun di luar jaringan perusahaan adalah satu alamat IP global. Jika semua paket dari semua workstation meninggalkan jaringan perusahaan dengan alamat IP yang sama, bagaimana respon yang datang dari Internet bisa diarahkan ke mesin yang tepat? Perangkat lunak NAT menyimpan daftar cache semua paket IP yang dikirim dan siapa yang mengirim setiap paket. Ketika respon datang kembali, NAT memeriksa cache untuk melihat siapa yang mengirim permintaan tersebut. Ketika NAT menemukan kecocokan, ia akan menghapus alamat IP global, memasukkan kembali alamat IP stasiun kerja pengguna, dan menempatkan paket di jaringan perusahaan.

Apa yang terjadi jika sebuah paket tiba di perangkat lunak NAT perusahaan dan tidak ada entri cache dengan permintaan keluar yang cocok? Dalam hal ini, paket tersebut dimusnahkan. Rupanya, seseorang telah mengirimkan paket ke jaringan perusahaan yang tidak diminta oleh stasiun kerja perusahaan. Ada satu pengecualian untuk aturan ini: Jika perusahaan mendukung server, seperti server Web, sebuah paket mungkin berasal dari pengguna di suatu tempat di Internet. Ketika paket permintaan halaman Web tiba di perangkat lunak NAT, alamat IP asal paket tidak akan cocok dengan alamat IP mana pun di cache lokal. Sebelum perangkat lunak NAT menghancurkan paket tersebut, ia memeriksa nomor port tujuan pesan. Jika paket tersebut merupakan permintaan halaman Web dari server Web perusahaan, perangkat lunak NAT mengizinkan paket tersebut masuk.

Fitur menarik dari penggunaan NAT adalah, karena dunia luar tidak pernah melihat alamat IP apa pun yang digunakan dalam jaringan perusahaan, tingkat keamanan telah ditambahkan. Selain itu, perusahaan tidak perlu menggunakan alamat IP yang dibeli di jaringan perusahaan. Untuk mendukung fitur ini, sejumlah alamat IP telah ditetapkan sebagai alamat IP “palsu”. Ketika stasiun kerja dengan alamat IP palsu mengeluarkan permintaan Internet, perangkat lunak NAT menggantikan alamat IP palsu tersebut dengan alamat IP global perusahaan. Penggunaan NAT dan alamat IP palsu adalah cara lain untuk menghemat uang dalam menyewa alamat IP.

Jaringan area lokal rumah dan bisnis kecil sering kali menggunakan NAT untuk menghemat alamat IP. Dengan melacak setiap permintaan dalam cache internalnya, NAT memungkinkan beberapa workstation mengakses Internet hanya dengan satu alamat IP. Jika komputer juga menggunakan DHCP, pengguna rumahan dapat terhubung ke Internet, menetapkan alamat IP secara dinamis, dan menggunakan alamat IP tersebut untuk operasi NAT. NAT sangat berguna sehingga banyak router sekarang memasukkannya sebagai fitur keamanan standar (firewall).

Protokol terowongan dan jaringan pribadi virtual

Salah satu masalah yang lebih serius dengan Internet adalah kurangnya keamanan. Setiap kali transmisi dilakukan, transmisi tersebut rentan terhadap intersepsi. Pengecer telah memecahkan sebagian masalah dengan menggunakan teknik enkripsi untuk mengamankan transaksi yang berhubungan dengan nomor kartu kredit dan informasi pribadi lainnya. Bisnis yang ingin karyawannya mengakses sistem komputasi perusahaan dari lokasi jarak jauh telah menemukan solusi serupa: jaringan pribadi virtual. Jaringan pribadi virtual (VPN) adalah koneksi jaringan data yang memanfaatkan infrastruktur telekomunikasi publik namun tetap menjaga privasi melalui penggunaan protokol penerowongan dan prosedur keamanan. Protokol penerowongan, seperti Point-to-Point Tunneling Protocol (PPTP), adalah kumpulan perintah yang memungkinkan organisasi membuat sambungan aman menggunakan sumber daya publik seperti Internet. Diusulkan oleh Cisco Systems, PPTP adalah standar yang disponsori oleh Microsoft dan perusahaan lain. Ini merupakan perpanjangan dari Point-to-Point Protocol (PPP) Internet, yang digunakan untuk komunikasi antara dua komputer menggunakan koneksi serial. Contoh koneksi serial yang paling umum adalah koneksi DSL atau modem kabel antara stasiun kerja pengguna dan penyedia layanan Internet. (PPP biasanya

merupakan standar yang lebih disukai daripada protokol sebelumnya, Serial Line Internet Protocol, atau SLIP.)

Karyawan yang berlokasi di luar gedung perusahaan dapat menggunakan PPTP untuk membuat terowongan melalui Internet ke dalam sumber daya komputasi perusahaan. Karena koneksi ini berjalan melalui Internet dan dapat digunakan untuk mengirimkan data rahasia perusahaan, maka koneksi ini harus aman. Keamanan koneksi seringkali didukung oleh IPSec. IPSec, singkatan dari IP Security, adalah seperangkat protokol yang dikembangkan oleh Internet Engineering Task Force untuk mendukung pertukaran paket data yang aman pada lapisan IP. Agar IPSec dapat berfungsi, pengirim dan penerima harus bertukar kunci enkripsi publik (dijelaskan secara rinci di Bab Dua Belas).

Selain sebagai koneksi yang aman, terowongan juga merupakan koneksi yang relatif murah karena menggunakan Internet sebagai bentuk komunikasi utamanya. Alternatif untuk membuat terowongan adalah dengan membeli saluran telepon dial-up atau menyewa saluran telepon—keduanya bisa lebih mahal.

Sekarang setelah kita memahami protokol-protokol yang memungkinkan Internet berfungsi, mari kita lihat lebih dekat World Wide Web—bidang Internet yang paling akrab bagi kita semua.

10.3 WORLD WIDE WEB (www)

World Wide Web (WWW) adalah kumpulan besar dokumen elektronik yang terletak di banyak server Web berbeda, dan berisi teks dan gambar yang dapat diakses hanya dengan mengklik link dalam halaman Web browser. Dengan menggunakan browser Web, Anda dapat mendownload dan melihat halaman Web di komputer pribadi. Dari semua layanan Internet, World Wide Web mungkin merupakan salah satu layanan yang mempunyai dampak paling besar terhadap bisnis. Penjualan ritel internet dan dukungan layanan telah meledak dengan penggunaan komputer pribadi dan browser Web. Hampir setiap produk dan layanan yang bisa dibayangkan kini dijual di Web. Dalam satu hari, Anda dapat membeli pakaian dan bahan makanan, membeli tiket pesawat, memilih dan membeli mobil, merencanakan pemakaman, mengajukan tawaran lelang untuk mainan yang Anda miliki saat kecil, mencari pekerjaan baru, menyewa DVD, dan memesan pizza untuk makan malam—semuanya online. Untuk melakukan hal ini, yang Anda butuhkan hanyalah ponsel pintar atau komputer dengan koneksi ke Internet dan browser Web. Halaman Web yang Anda download dapat terdiri dari teks, grafik, link ke halaman Web lain, terkadang musik dan video, dan bahkan program yang dapat dijalankan.

Halaman web dibuat menggunakan *Hypertext Markup Language* (HTML), yang dapat dibuat secara manual dengan editor berbasis teks seperti Notepad, atau melalui penggunaan alat pembuat halaman Web. Alat pembuat halaman Web mirip dengan pengolah kata, kecuali bahwa alih-alih membuat dokumen teks, Anda membuat halaman Web berbasis HTML. Alat pembuat halaman Web memiliki antarmuka pengguna grafis yang memungkinkan Anda memasukkan teks dan menyisipkan grafik dan elemen halaman Web lainnya, dan juga mengatur elemen-elemen ini pada halaman menggunakan teknik drag-and-drop.

Setelah Anda membuat halaman Web, Anda menyimpannya di komputer yang berisi perangkat lunak server Web dan memiliki koneksi ke Internet. Perangkat lunak server Web menerima permintaan Hypertext Transfer Protocol dari browser Web yang terhubung ke Internet, mengambil halaman Web yang diminta dari penyimpanan, dan mengembalikan halaman Web tersebut ke komputer yang meminta melalui Internet. Hypertext Transfer Protocol (HTTP) adalah protokol lapisan aplikasi. Seperti yang dijelaskan di Bab Satu, ketika pengguna yang duduk di stasiun kerja yang menjalankan browser mengklik link pada halaman Web, perangkat lunak browser melihat klik ini dan membuat perintah HTTP lapisan aplikasi untuk mengambil halaman Web. Perintah HTTP ini melewati lapisan transport, lapisan jaringan, dan lapisan akses jaringan sebelum ditempatkan pada media jaringan. Ketika permintaan halaman Web diterima di server situs Web, halaman Web tersebut diambil dan dikembalikan melalui Internet ke browser pengguna, di mana halaman tersebut ditampilkan pada monitor.

Kini setelah kita memahami bagaimana dokumen disebarkan melalui Internet, pertanyaannya tetap: Bagaimana dokumen Internet ditangani dan ditemukan? Untuk menjawab pertanyaan ini, kita perlu memeriksa URL, Sistem Nama Domain, dan alamat IP.

HTTP

Seluruh tujuan HTTP adalah untuk mengirim dan menerima halaman Web. Untuk menyelesaikan operasi ini, HTTP dapat melakukan sejumlah perintah berbeda yang disebut metode. Beberapa metode yang lebih umum adalah sebagai berikut:

- GET—Mengambil halaman Web tertentu, yang diidentifikasi oleh URL
- HEAD—Menggunakan URL tertentu untuk mengambil header HTTP saja (bukan isi dokumen) halaman Web
- PUT—Mengirim data dari browser pengguna ke situs Web jarak jauh (metode ini digunakan, misalnya, untuk mengirim nomor kartu kredit pembeli ke pedagang Web selama transaksi pembelian)
- DELETE—Meminta server menghapus informasi yang terkait dengan URL tertentu

Sebagai contoh bagaimana metode ini digunakan, misalkan Anda mengklik link selama sesi browser Web. Perangkat lunak browser membuat perintah GET dan mengirimkan perintah itu ke server Web. Server Web kemudian mengembalikan halaman Web ke browser. Sekarang anggaplah Anda membeli produk melalui Web, dan Anda mengisi formulir. Saat Anda mengklik tombol Kirim, HTTP membuat perintah PUT dan menggunakannya untuk mengirim data ke server Web.

Menemukan dokumen di Internet

Saat pengguna menjalankan browser dan mengklik link, browser mencoba menemukan objek link tersebut dan membawanya melalui Internet ke perangkat pengguna. Objek ini dapat berupa dokumen, halaman Web, gambar, file FTP, atau sejumlah tipe objek data yang berbeda. Bagaimana Internet menemukan setiap objek? Sederhananya, setiap objek di Internet memiliki alamat unik berbasis bahasa Inggris yang disebut Uniform Resource Locator (URL). Namun Internet tidak mengenali URL secara langsung. Agar Internet dapat

menemukan dokumen atau objek, bagian dari URL objek tersebut harus diterjemahkan ke dalam alamat IP yang mengidentifikasi server Web tempat dokumen atau objek tersebut disimpan. Terjemahan dari URL ke alamat IP ini dilakukan oleh Sistem Nama Domain (DNS).

Mari kita periksa URL dan DNS lebih jauh untuk mendapatkan pemahaman yang lebih baik tentang bagaimana Internet menemukan satu dokumen dari miliaran dokumen.

Pencari Sumber Daya Seragam

Agar pengguna dapat menemukan sesuatu di Internet, setiap objek yang terletak di Internet harus memiliki “alamat” yang unik. Alamat ini, atau Uniform Resource Locator (URL), secara unik mengidentifikasi file, halaman Web, gambar, atau jenis dokumen elektronik lainnya yang ada di Internet. Saat Anda menggunakan browser Web dan mengklik link ke halaman Web, Anda sebenarnya mengirimkan perintah ke Internet untuk mengambil halaman Web tersebut dari lokasi tertentu yang didasarkan pada URL halaman Web tersebut.

Semua Uniform Resource Locator terdiri dari empat bagian, seperti yang ditunjukkan pada Gambar 10-9. Bagian pertama, yang ditandai dengan angka 1 pada gambar, adalah jenis layanan. Jenis layanan mengidentifikasi protokol yang digunakan untuk mengangkut dokumen yang diminta. Misalnya, jika Anda meminta halaman Web, maka Hypertext Transfer Protocol (<http://>) adalah jenis layanan yang digunakan untuk mengambil halaman Web, seperti yang ditunjukkan pada Gambar 10-9(a). Jika Anda meminta dokumen FTP, maka protokol FTP (<ftp://>) digunakan, seperti pada Gambar 10-9(b). Jenis layanan lainnya termasuk <telnet://> untuk melakukan login jarak jauh, <news://> untuk mengakses grup Usenet, dan <mailto://> untuk mengirim pesan surat elektronik.

<http://cs.depaul.edu/public/utilities/ada/example.htm>

1 2 3 4
(a)

<ftp://gatekeeper.dec.com/pub/games/starwars.exe>

1 2 3 4
(b)

Gambar 10-9 Bagian-bagian Uniform Resource Locator untuk HTTP (a) dan FTP

Bagian kedua dari URL, ditandai dengan angka 2 pada Gambar 10-9, adalah nama domain. Bagian URL ini menentukan server tertentu di situs tertentu yang berisi item yang diminta. Pada contoh pada Gambar 10-9, cs.depaul.edu merupakan salah satu server pendukung program ilmu komputer di DePaul University. Mulai dari kanan, edu adalah domain tingkat teratas dan menunjukkan bahwa situs Web adalah situs pendidikan. Beberapa domain tingkat atas lainnya adalah com (komersial), gov (pemerintah), mil (militer), org (organisasi nirlaba), net (berbasis jaringan), biz, nama, info, pro, museum, aero, dan mengurung. Setiap negara juga memiliki nama domain tingkat atas sendiri. Misalnya, Kanada adalah ca dan Inggris adalah Inggris. Nama domain pada tingkat berikutnya—disebut nama domain tingkat menengah—biasanya merupakan nama organisasi (seringkali perusahaan atau sekolah) atau host, seperti depaul. Domain tingkat rendah lainnya merupakan subdivisi lebih lanjut dari host dan

biasanya dibuat oleh host. Misalnya, sebuah perusahaan bernama FiberLock mengajukan permohonan kepada lembaga yang menangani pendaftaran nama domain untuk meminta fiberlock nama domain tingkat menengah. Karena FiberLock adalah bisnis komersial, domain level teratasnya adalah com. Jika tidak ada orang lain yang menggunakan fiberlock, perusahaan akan diberikan fiberlock.com sebagai nama domainnya. Perusahaan kemudian dapat menambahkan lebih banyak tingkat domain, seperti www atau email, untuk membuat entitas seperti www.fiberlock.com atau email.fiberlock.com, yang masing-masing dapat berhubungan dengan server halaman Web dan server email perusahaan.

Bagian ketiga dari URL, diberi label 3 pada Gambar 10-9, adalah informasi direktori atau subdirektori. Misalnya, URL <http://cs.depaul.edu/public/utilities/> ada menetapkan bahwa item yang diminta terletak di subdirektori ada, di bawah subdirektori utilitas, di bawah subdirektori publik.

Bagian terakhir dari URL, yang ditentukan dengan angka 4 pada Gambar 10-9, adalah nama file dari objek yang diminta. Pada Gambar 10-9(a), ini adalah dokumen berjudul `example.htm`. Jika tidak ada nama file yang ditentukan dalam URL, maka file default, seperti `default.htm` atau `index.html`, akan diambil.

Sistem Nama Domain (DNS)

Semua koneksi ke Internet ditentukan oleh alamat biner 32-bit (IPv4) atau alamat biner 128-bit (IPv6). Meminta pengguna untuk memasukkan alamat 32-bit ke dalam browser Web akan menjadi hukuman yang kejam dan tidak biasa. (Dapatkah Anda bayangkan mencoba memasukkan alamat 128-bit?!) Bahkan notasi desimal bertitik untuk alamat IPv4 dan bentuk heksadesimal untuk alamat IPv6 tidak nyaman bagi kebanyakan manusia. Saat mereferensikan situs Internet, kita sering merujuk pada nama domainnya. Namun komputer tidak menggunakan nama domain. Karena komputer menggunakan alamat biner dan hampir semua manusia menggunakan bentuk nama domain, Internet mengubah bentuk biner menjadi nama domain berbasis bahasa Inggris, dan sebaliknya. Untuk melakukan hal ini, ia menggunakan Sistem Nama Domain (DNS), yang merupakan basis data alamat Internet dan nama domain yang besar dan terdistribusi. Basis data terdistribusi ini terdiri dari jaringan server DNS lokal, server DNS tingkat menengah, dan server DNS tingkat tinggi. Agar sistem tetap dapat dikelola, database DNS didistribusikan menurut domain tingkat teratas: edu, gov, com, mil, dan seterusnya.

Mengubah nama domain menjadi alamat IP biner bisa sederhana atau rumit. Tingkat kerumitannya bergantung pada apakah server jaringan lokal di jaringan area lokal asal mengenali nama domain atau tidak. Jika server jaringan tidak dapat menyelesaikan suatu alamat secara lokal, server tersebut akan memanggil otoritas yang lebih tinggi. Server DNS lokal akan mengirimkan pesan DNS ke server DNS berikutnya yang lebih tinggi hingga alamat ditemukan, atau ditentukan bahwa alamat tersebut tidak ada. Jika alamatnya tidak ada, pesan yang sesuai akan dikembalikan.

Pertimbangkan, pertama-tama, apa yang terjadi ketika server lokal mengenali nama domain. Ketika nama domain baru muncul, program aplikasi, seperti browser Web, memanggil prosedur perpustakaan yang diberi nama penyelesai. Penyelesai mengirimkan

pesan DNS ke server DNS lokal, yang mencari nama dan mengembalikan alamat IP ke penyelesaian. Resolver kemudian mengembalikan alamat IP ke program aplikasi. Namun apa yang terjadi jika server DNS lokal tidak memiliki informasi yang diminta? Ini mungkin menanyakan server DNS lokal lainnya, jika ada. Informasi mengenai keberadaan server lokal lain dan lokasi server jauh akan disimpan dalam file di jaringan komputer lokal. Jika jawabannya lagi adalah tidak, server DNS lokal akan mencoba tingkat berikutnya—mungkin server tingkat menengah. Jika server tingkat menengah tidak mengenali nama domain, atau jika tidak ada server tingkat menengah, server nama tingkat atas untuk domain tersebut akan ditanyakan. Jika server nama tingkat atas tidak mengenali nama domain, ia akan mengembalikan pesan “URL Tidak Ditemukan” atau turun satu tingkat dan menanyakan server DNS lokal. Untuk memahami hal ini dengan lebih baik, mari kita lihat sebuah contoh.

Pertimbangkan skenario di mana pengguna di `cs.waynestate.edu` di Wayne State University ingin mengambil halaman Web dari `www.trinity.edu` di Trinity University. Pesan berasal dari `cs.waynestate.edu` dan masuk ke server nama `waynestate.edu`. Server nama `waynestate.edu` tidak mengenali `www.trinity.edu` karena nama domain `www.trinity.edu` tidak ada dalam daftar situs Web yang baru-baru ini direferensikan. Oleh karena itu, server nama `waynestate.edu` mengirimkan permintaan DNS ke `edu-server.net`. Meskipun `edu-server.net` tidak mengenali `www.trinity.edu`, namun ia mengenali `trinity.edu`, sehingga mengirimkan query ke `trinity.edu`. Server nama `trinity.edu` mengenali `www.trinity.edu` miliknya dan mengembalikan hasilnya ke `edu-server.net`, yang mengembalikan hasilnya ke server nama `waynestate.edu`, yang mengembalikan hasilnya ke komputer pengguna, yang kemudian memasukkan hasilnya—yaitu, alamat IP biner 32-bit atau 128-bit yang sesuai—ke dalam permintaan browser.

10.4 LAYANAN INTERNET

Ketika Internet muncul sebagai ARPANET, kebanyakan orang menggunakannya untuk email, transfer file, dan login jarak jauh. Selain mempelajari layanan-layanan tersebut, mari kita periksa beberapa layanan populer yang disediakan Internet saat ini.

Surat elektronik (email)

Surat elektronik, atau email, adalah versi komputerisasi dari penulisan surat dan mengirimkannya ke kantor pos setempat. Banyak orang yang begitu berkomitmen untuk menggunakan email sehingga jika email tersebut dihapuskan besok, dampak sosial dan ekonomi yang serius akan dirasakan di seluruh Amerika Serikat dan seluruh dunia.

Banyak program email komersial yang ada, serta sejumlah program gratis yang dapat diunduh dari Internet. Meskipun setiap program email memiliki nuansa dan pilihan uniknya sendiri, sebagian besar program email menawarkan layanan berikut:

- Membuat pesan email
- Mengirim pesan email ke satu penerima, beberapa penerima, atau milis
- Menerima, menyimpan, membalas, dan meneruskan pesan email
- Melampirkan file—seperti dokumen pengolah kata, spreadsheet, gambar, atau program—ke pesan email keluar

Kebanyakan sistem email terdiri dari dua bagian: (1) agen pengguna, yaitu bagian dari program email yang memungkinkan pengguna membuat, mengedit, menyimpan, dan meneruskan pesan email; dan (2) agen transfer pesan, yaitu bagian dari program email yang menyiapkan dan mentransfer pesan email. Setiap email yang dikirimkan juga terdiri dari dua komponen dasar: amplop, yang berisi informasi yang menjelaskan pesan email, dan pesan, yaitu isi amplop.

Sebagian besar pesan terdiri dari teks biasa dan ditulis dalam karakter ASCII sederhana. Bagaimana jika Anda ingin mengirim (atau melampirkan) item berbasis nonteks, seperti spreadsheet, database, atau gambar? Program email kemudian membuat dokumen Multiguna Internet Mail Extensions (MIME) dan melampirkannya ke pesan email.

Setelah email dan lampiran opsional dibuat, sekarang saatnya untuk mengirimkan pesan. Simple Mail Transfer Protocol (SMTP) adalah protokol Internet untuk mengirim dan menerima email, dan digunakan untuk melakukan transfer. Untuk mengirim pesan email, komputer sumber membuat koneksi TCP ke port nomor 25 (biasanya) di komputer tujuan. Komputer tujuan mempunyai daemon email—sebuah program yang selalu berjalan di latar belakang dan menunggu untuk menjalankan fungsinya—yang mendukung protokol SMTP. Daemon email mengawasi port 25, menerima koneksi masuk, dan menyalin pesan ke kotak surat yang sesuai. Setara dengan SMTP di Eropa dan Kanada adalah protokol X.

Berapa kali Anda menerima pesan email meskipun mesin Anda tidak dihidupkan? Saat Anda menghidupkan komputer dan menjalankan program email, sebuah pesan memberitahukan bahwa Anda memiliki n pesan email baru yang menunggu. Perangkat lunak apa yang melakukan operasi ini? Post Office Protocol versi 3 (POP3) adalah perangkat lunak yang memungkinkan pengguna menyimpan pesan email di kotak surat server dan mendownloadnya bila diinginkan dari server. POP3 berguna jika Anda tidak memiliki koneksi permanen ke suatu jaringan dan harus melakukan panggilan menggunakan koneksi Internet sementara. POP3 akan menyimpan pesan email Anda hingga saat berikutnya Anda menelepon dan mengakses kotak surat Anda. Dengan demikian, perangkat lunak POP3 umumnya ditemukan pada komputer laptop seluler atau komputer rumah tanpa koneksi jaringan permanen, tetapi juga pada sistem komputer yang memiliki koneksi permanen.

Alternatif untuk POP3 adalah Internet Message Access Protocol (IMAP) yang lebih canggih. IMAP (versi terbaru adalah IMAP4) adalah protokol klien/server tempat email diterima dan disimpan untuk Anda di server Internet Anda. Anda dapat melihat judul email saja, atau melihat pengirim pesan, lalu memutuskan apakah Anda ingin mendownload email tersebut. Anda juga dapat membuat dan memanipulasi folder atau kotak surat di server, menghapus pesan email lama, atau mencari bagian tertentu dari pesan email.

Banyak paket email yang memungkinkan pengguna mengenkripsi pesan email untuk transfer aman melalui jaringan area lokal internal atau melalui jaringan area luas seperti Internet. Ketika pesan email dienkripsi, hampir tidak mungkin untuk mencegat dan memecahkan kode pesan tersebut tanpa algoritma dan kunci enkripsi yang tepat. Pesan email penting juga dapat diterapkan tanda tangan digital sehingga, di kemudian hari, pemilik pesan

email dapat membuktikan bahwa pesan email tersebut bukan milik siapa pun kecuali dirinya. Teknik enkripsi akan dibahas lebih rinci pada Bab Dua Belas.

Protokol Transfer File

File Transfer Protocol, atau FTP, adalah salah satu layanan pertama yang ditawarkan di Internet. Fungsi utamanya adalah memungkinkan pengguna mengunduh file dari situs jarak jauh ke komputer pengguna, dan mengunggah file dari komputer pengguna ke situs jarak jauh. File-file ini dapat berisi data, seperti angka, teks, atau gambar, atau program komputer yang dapat dijalankan. Meskipun World Wide Web telah menjadi sarana utama untuk mengambil dokumen berbasis teks dan gambar, banyak organisasi masih merasa berguna untuk membuat repositori data dan file program FTP. Dengan menggunakan browser Web atau perangkat lunak FTP khusus, Anda dapat dengan mudah mengakses situs FTP. Jika Anda menginginkan privasi dan ingin membatasi akses ke situs FTP, situs tersebut dapat dirancang untuk memerlukan ID pengguna dan kata sandi untuk masuk.

Untuk mengakses situs FTP melalui browser Web dan mendownload file, Anda memerlukan setidaknya tiga informasi. Pertama, Anda harus mengetahui nama situs FTPnya. Kedua, Anda harus mengetahui nama direktori atau subdirektori tempat mencari file tersebut. Ketiga, Anda harus mengetahui nama file yang ingin Anda download. Jadi, mengunduh file FTP bukanlah aktivitas “browsing”. Anda harus mempunyai gagasan bagus tentang apa yang Anda cari dan di mana lokasinya.

Sebagai contoh, katakanlah Anda sedang membaca sebuah artikel di majalah komputer, dan artikel tersebut menjelaskan sebuah program utilitas gratis yang mengatur waktu Anda, membuat Anda tetap pada jadwal, dan membantu Anda mendapatkan teman baru. Anda harus memiliki program ini, tetapi program ini ada di beberapa situs FTP entah dari mana. Tidak masalah. Yang Anda butuhkan hanyalah URL program utilitas dan browser Web. Seperti yang dijelaskan di bagian sebelumnya, setiap dokumen di Internet memiliki URL unik. Sebagai contoh, anggaplah URL program ini adalah `ftp://ftp.goodstuff.com/public/util/` dan nama filenya adalah `perfect.exe`. Pada prompt lokasi atau alamat browser Web, ketikkan URL ini. Ketika Anda tiba di situs FTP `ftp.goodstuff.com` dan berada di subdirektori `public/util`, Anda akan melihat file `perfect.exe` terdaftar. Mengklik nama file dan menentukan lokasi penerimaan materi yang diunduh akan memulai proses pengunduhan. Perangkat lunak FTP mengirimkan perintah permintaan FTP yang sesuai ke situs FTP, yang membuka koneksi transfer file antara stasiun kerja Anda dan situs jarak jauh. File tersebut dipecah menjadi beberapa paket, dan paket tersebut ditransfer satu per satu melalui Internet ke stasiun kerja Anda. Ketika semua paket untuk file tersebut telah tiba, koneksi terputus. Sebenarnya, dua koneksi telah dibuat. Koneksi pertama mentransfer informasi kontrol, yang mengatur transfer file, dan koneksi kedua mentransfer data sebenarnya.

Bagaimana Sistem MIME Bekerja

Lima header tipe MIME yang berbeda memberikan informasi tentang file yang telah dilampirkan ke pesan email: versi MIME, deskripsi konten, ID konten, tipe konten, dan pengkodean transfer konten. Versi MIME menyatakan nomor versi protokol MIME yang digunakan. Deskripsi konten adalah dokumen sebenarnya yang dilampirkan. ID konten

mengidentifikasi lampiran MIME dan pesan email terkait. Header tipe konten menjelaskan apakah lampiran berupa file teks, gambar, audio, video, aplikasi, pesan, atau multibagian.

Header pengkodean transfer konten menjelaskan bagaimana materi non-ASCII dalam lampiran dikodekan, sehingga karakter non-ASCII tidak menimbulkan kekacauan saat dikirimkan. Sebuah program email dapat menggunakan salah satu dari lima skema berbeda saat menyandikan materi non-ASCII untuk transmisi:

- ASCII 7-bit biasa, bentuk ASCII yang lebih umum.
- ASCII 8-bit, yang tidak didukung oleh banyak sistem.
- Pengkodean biner, yaitu kode mesin. Pengkodean biner berbahaya untuk digunakan karena nilai biner tertentu dapat menandakan karakter kontrol khusus, seperti pengangkutan kembali, yang mungkin menyebabkan perangkat penerima berperilaku tidak menentu.
- Pengkodean Base64, yang merupakan metode terbaik. Untuk melakukan pengkodean Base64, komputer memecah 24 bit data biner menjadi empat kelompok 6-bit, dan kemudian mengkodekan setiap kelompok 6-bit menjadi karakter ASCII tertentu (berdasarkan bagan karakter ASCII standar).
- Pengkodean kutipan yang dapat dicetak, yang menggunakan ASCII 7-bit. Dalam pengkodean kutipan yang dapat dicetak, setiap karakter dengan nilai ASCII desimal lebih besar dari 127 dikodekan dengan tanda sama dengan (=) diikuti dengan nilai karakter dalam dua digit heksadesimal.

Login jarak jauh (Telnet)

Login jarak jauh, atau Telnet, adalah program emulasi terminal untuk jaringan TCP/IP, seperti Internet, yang memungkinkan pengguna untuk masuk ke komputer jarak jauh. Program Telnet berjalan di komputer Anda dan menghubungkan stasiun kerja Anda ke server jarak jauh di Internet. Setelah Anda terhubung ke server atau host jarak jauh, Anda dapat memasukkan perintah melalui program Telnet, dan perintah tersebut akan dijalankan seolah-olah Anda memasukkannya langsung di terminal komputer jarak jauh.

Ada sejumlah alasan untuk menggunakan program Telnet. Pertama, Telnet memungkinkan pengguna untuk masuk ke akun pribadi dan menjalankan program di mana pun dia berada. Misalnya, Anda mungkin memiliki akun komputer di dua perusahaan berbeda atau di dua sekolah berbeda. Meskipun Anda mungkin secara fisik berada di satu situs, Anda dapat menggunakan Telnet untuk masuk ke situs komputer lain. Melalui login ini, Anda dapat memeriksa email atau menjalankan aplikasi. Kedua, login jarak jauh memungkinkan pengguna untuk mengakses layanan publik di situs komputer jarak jauh. Ketiga, Telnet memungkinkan administrator jaringan untuk mengontrol server jaringan dan berkomunikasi dengan server lain di jaringan. Pengendalian ini dapat dilakukan dari jarak jauh, seperti kota lain atau rumah administrator jaringan.

Telnet telah mengalami penurunan penggunaan dalam dekade terakhir ini. Salah satu program populer yang menggantikannya adalah Remote Desktop Connection yang ditawarkan oleh Microsoft dan disebut rdesktop pada sistem Unix dan Linux.

Suara melalui IP

Layanan populer yang menarik minat perusahaan dan pengguna rumahan adalah pengiriman sinyal suara melalui jaringan berbasis IP seperti Internet. Praktek melakukan panggilan telepon melalui Internet mempunyai beberapa nama yang berbeda, termasuk suara paket, suara melalui paket, suara melalui Internet, telepon Internet, dan Voice over IP (VoIP). Namun nampaknya industri ini sudah menggunakan istilah “Voice over IP” yang mengacu pada Protokol Internet, yang mengontrol transfer data melalui Internet.

Saat ini ada tiga cara untuk mengirimkan VoIP ke pengguna. Teknik pertama ditemukan di tingkat korporasi. Banyak perusahaan menawarkan sistem VoIP yang beroperasi melalui jaringan area lokal. Sistem ini melibatkan cukup banyak peralatan, seperti server VoIP, telepon khusus yang mendukung IP, dan router yang dapat mengarahkan panggilan telepon. Saat ini, sebagian besar situs perusahaan telah mengubah sistem telepon internal lama mereka menjadi sistem VoIP yang beroperasi melalui LAN, sehingga menggabungkan dua sistem menjadi satu. Solusi umum kedua adalah solusi yang sering ditemui di rumah. Dengan menggunakan telepon yang ada, konverter khusus ditambahkan antara telepon dan koneksi Internet kecepatan tinggi (DSL atau modem kabel). Konverter mendigitalkan sinyal suara dan membuat aliran paket yang kemudian dikirim melalui koneksi IP. Teknik ketiga melibatkan ponsel pintar. Teknologi telepon seluler yang lebih baru semuanya berbasis paket, sehingga memerlukan panggilan telepon untuk diubah menjadi paket digital dan mengirimkan paket tersebut melalui jaringan IP.

Ketika sistem telepon yang andal dan berkualitas tinggi sudah tersedia, mengapa harus mencari teknologi alternatif yang menyediakan layanan yang sama? Salah satu keunggulan VoIP sebelumnya hanya terkait dengan fakta bahwa panggilan jarak jauh, terutama panggilan luar negeri, berbiaya mahal, sedangkan pengiriman data—atau suara—melalui Internet pada dasarnya gratis. Ternyata, keuntungan dari panggilan jarak jauh yang murah menjadi kurang penting bagi banyak pengguna korporat (namun masih sama dengan sejumlah pengguna rumahan). Salah satu alasannya adalah tarif telepon jarak jauh telah turun secara signifikan selama bertahun-tahun; hal lainnya adalah kualitas panggilan VoIP jarak jauh seringkali lebih buruk daripada kualitas panggilan jarak jauh konvensional. Namun banyak perusahaan menemukan keuntungan lain yang lebih penting karena mampu memperlakukan data suara seperti bentuk data lainnya. Pertama, jika suara dan data dapat dikirimkan melalui jaringan yang sama, perusahaan akan menghemat peralatan dan infrastruktur. Hal ini akan memberikan keuntungan signifikan lainnya, yaitu menghilangkan kebutuhan akan telepon terpisah. Dengan demikian, pengelolaan suatu perusahaan dapat disederhanakan. Seperti yang akan kita lihat sebentar lagi, menjalankan suara dan data melalui sistem yang sama akan membuka pintu bagi aplikasi yang menarik dan kuat.

VoIP juga memiliki sejumlah kelemahan. Pernyataan bahwa pengiriman data melalui Internet pada dasarnya gratis adalah pernyataan yang menyesatkan. Tentu saja tidak ada yang gratis. Semua pengguna Internet harus membayar penyedia layanan Internet untuk akses, saluran telepon interkoneksi, dan perangkat keras dan perangkat lunak apa pun yang diperlukan. Selain itu, diperlukan lebih banyak perangkat keras dan perangkat lunak tambahan

untuk menangani transmisi paket suara melalui jaringan data perusahaan. Meskipun demikian, jika Anda sudah memiliki akses Internet berkecepatan tinggi, menambahkan VoIP mungkin merupakan cara yang masuk akal untuk mendapatkan layanan telepon lokal dan jarak jauh.

Kerugian kedua, dan yang lebih penting, adalah transmisi suara melalui jaringan perusahaan dapat menguras sumber daya jaringan. Jika sistem jaringan perusahaan saat ini mengalami kesulitan dalam mengirimkan data, menambahkan suara ke sistem ini dapat menyebabkan masalah layanan yang parah. Masalah layanan ini dapat diperparah karena sistem suara memerlukan jaringan yang dapat meneruskan data suara dalam waktu yang relatif singkat. Jaringan yang menunda data suara lebih dari 20 milidetik dari ujung ke ujung akan menimbulkan gema yang nyata ke dalam transmisi. Jika penundaan menjadi lebih lama dari 250 milidetik (yaitu hanya seperempat detik), sistem pada dasarnya tidak dapat digunakan.

Yang lebih memperburuk masalah penundaan ini adalah kenyataan bahwa Internet pada dasarnya adalah jaringan area luas packet-switched datagram yang besar. Ingat dari Bab Sembilan bahwa dalam jaringan packet-switched datagram, setiap paket data dirutekan secara individual. Perutean individual ini dapat menimbulkan penundaan perutean untuk setiap paket, bahkan dengan penggunaan protokol yang lebih baru seperti MPLS. (Untuk informasi lebih lanjut mengenai protokol ini, lihat bagian Detail yang berjudul “Peralihan Label Multiprotokol.”) Sebaliknya, jaringan telepon umum pertama-tama menetapkan sebuah rute (sirkuit) dan kemudian mengirimkan semua paket berikutnya melalui rute yang telah ditentukan. Karena rutenya tetap, setiap paket tidak mengalami penundaan perutean. Untuk mempertahankan percakapan telepon melalui Internet, paket suara harus tiba di tujuannya secara terus menerus. Jika tidak, percakapan suara akan terputus dan kualitasnya buruk. Saat ini, VoIP biasanya berfungsi dengan baik namun terkadang tidak.

Masalah lain yang menjadi tantangan bagi VoIP termasuk keamanan, layanan darurat, kerentanan terhadap kegagalan daya, dan portabilitas nomor. Keamanan dapat menjadi masalah karena paket suara melintasi Internet yang sama dengan paket lainnya, sehingga selalu rentan terhadap intersepsi. Layanan darurat telah menimbulkan masalah yang menarik. Saluran telepon tradisional dikaitkan dengan nomor telepon tetap. Jadi ketika seseorang menelepon 911 dari saluran telepon tradisional, operator darurat segera mengetahui lokasi sumber panggilan tersebut. Hal ini tidak terjadi pada VoIP. Layanan 911 yang ditingkatkan telah memberikan solusi yang masuk akal untuk masalah ini. Sistem VoIP juga rentan terhadap kegagalan daya karena panggilan telepon melintasi LAN, yang memerlukan daya konstan. Sistem telepon tradisional menyuplai dayanya sendiri dan sering kali bertahan saat listrik mati (kecuali telepon nirkabel di rumah Anda). Terakhir, sekarang sudah menjadi hal yang lumrah untuk menyimpan nomor rumah atau ponsel Anda ke mana pun Anda pergi. Hal ini mungkin tidak terjadi pada VoIP, yang memerlukan pembaruan tabel manual.

Bagi perusahaan yang mempertimbangkan Voice over IP, satu fakta penting dan menarik untuk diingat adalah bahwa teknologinya tidak perlu melibatkan penggunaan Internet. Sebuah perusahaan dapat menggunakan IP untuk transmisi data dalam jaringannya

sendiri, namun menggunakan saluran telepon tradisional di luar jaringan perusahaan. Banyak orang menyebut sistem seperti VoIP pribadi. Karena sistem ini tidak menggunakan Internet melainkan tetap internal, penundaan paket menjadi minimal, dan ini membuat VoIP menarik. Sistem baru mulai bermunculan yang dapat mendukung pengoperasian telepon dan pengoperasian data komputer melalui rangkaian kabel yang sama. Bidang studi ini—integrasi telepon komputer—merupakan perpaduan baru yang menarik antara sistem komputer dan sistem telepon.

Untuk mendapatkan pemahaman yang lebih baik tentang VoIP, mari kita periksa berbagai langkah yang diperlukan untuk membuat paket VoIP dari suara seseorang dan memperkenalkan protokol yang lebih umum yang digunakan untuk mendukung teknologi baru ini. Langkah pertama dalam mengkonversi paket suara ke IP adalah melakukan konversi analog-ke-digital menggunakan codec. Setelah suara didigitalkan, suara tersebut dikompresi menjadi paket yang jauh lebih kecil dan kemudian diubah menjadi format datagram. Datagram suara kemudian dienkapsulasi dengan UDP dan header IP yang sesuai, dan dikirim melalui jaringan IP.

Perangkat umum yang melakukan konversi dari panggilan telepon analog (suara dan sinyal) menjadi data IP yang dipaketkan adalah gateway VoIP. Gerbang VoIP dapat melakukan digitalisasi, kompresi, dan enkapsulasi yang diperlukan, dan mengontrol pengaturan panggilan VoIP antara perangkat pemanggil dan perangkat yang dipanggil. Saat ini, dua set protokol dasar mendukung semua langkah ini. Kumpulan standar pertama, H.323, berasal dari ITU-T dan pertama kali dikeluarkan pada tahun 1996.

H.323 sebenarnya adalah sekumpulan protokol yang disebut protokol multimedia berbasis paket, dan dirancang untuk berbagai aplikasi (audio dan video). Menariknya, H.323 awalnya tidak dirancang untuk jaringan TCP/IP tetapi untuk jaringan X.25 dan ATM.

Protokol kedua, Session Initiation Protocol, adalah protokol yang diyakini banyak orang akan menjadi standar VoIP utama, namun tampaknya hal ini belum terjadi. Session Initiation Protocol (SIP) diperkenalkan pada tahun 1998 oleh Internet Engineering Task Force khusus untuk mendukung transfer suara melalui Internet. SIP pada dasarnya adalah protokol lapisan aplikasi yang dapat membuat, memodifikasi, dan mengakhiri sesi suara antara dua pihak atau lebih. Sesi suara ini tidak terbatas pada panggilan telepon sederhana, namun juga dapat mencakup panggilan konferensi dan transmisi multimedia. SIP juga memanggil protokol lain untuk mendukung VoIP. Salah satu protokol ini adalah ENUM. ENUM adalah protokol yang mengubah nomor telepon menjadi alamat nama domain yang sepenuhnya memenuhi syarat. Misalnya, jika Anda ingin memanggil nomor 555-1212 di kode area 312, ENUM akan mengubahnya menjadi alamat nama domain dalam bentuk 2.1.2.1.5.5.5.2.1.3.1.e164.arpa (ini sepenuhnya nomor kualifikasi 1(312)555-1212 dibalik, dengan e164.arpa ditambahkan di akhir).

Terakhir, meskipun tidak persis sama dengan Voice over IP, Voice over Wireless LAN (VoWLAN) (juga dikenal sebagai Voice over Wi-Fi) sangat mirip. Alih-alih mentransmisikan suara melalui jaringan IP kabel, Voice over WLAN memungkinkan pengguna menjelajah di

dalam gedung atau kampus dan, menggunakan handset nirkabel, berkomunikasi dengan satu atau lebih orang menggunakan jaringan LAN nirkabel.

Ada sejumlah alasan menarik untuk menggunakan VoWLAN. Pertama, meskipun banyak orang berpikir tentang telepon seluler ketika mereka berpikir untuk berbicara melalui telepon nirkabel, banyak sinyal telepon seluler yang tidak menjangkau terlalu jauh ke dalam gedung-gedung besar. Karena banyak bisnis sudah memiliki atau sedang merencanakan jaringan LAN nirkabel, sinyal mereka biasanya lebih tersebar di gedung-gedung besar. Keuntungan lain dari VoWLAN dibandingkan telepon seluler adalah biayanya. Layanan telepon seluler disediakan oleh penyedia telepon seluler, yang harus Anda bayar. Berbicara melalui jaringan LAN nirkabel yang ada pada perusahaan pada dasarnya “gratis.”

Tentu saja, VoWLAN bukannya tanpa kekurangan. Salah satu masalah potensial adalah handoff—ketika pengguna seluler berpindah dari satu layanan dasar ke layanan dasar lainnya dalam jaringan. Untuk memberikan panggilan telepon yang berkualitas, handoff harus cepat dan lancar. Banyak jaringan area lokal dapat dengan cepat dipenuhi oleh banyak pengguna suara yang menggunakan sinyal nirkabel. Meskipun demikian, ini adalah satu lagi teknologi yang harus kita waspadai dalam waktu dekat.

Listserv

Listserv adalah program perangkat lunak populer yang digunakan untuk membuat dan mengelola milis Internet. Perangkat lunak Listserv memelihara tabel alamat email yang mencerminkan anggota listserv saat ini. Ketika seseorang mengirim email ke alamat listserv, listserv mengirimkan salinan pesan email ini ke setiap alamat email yang disimpan dalam tabel listserv. Dengan demikian, setiap anggota listserv menerima pesan email. Nama lain untuk listserv atau jenis perangkat lunak listserv lainnya termasuk mailserv, mayordomo, dan almanak.

Untuk berlangganan listserv, Anda mengirim pesan berformat khusus ke alamat listserv khusus. Alamat ini berbeda dengan alamat pengiriman email ke semua anggota listserv. Misalnya, Anda dapat berlangganan listserv Universitas Southern Michigan di Copper Harbor tentang penghapus dengan mengirimkan pesan SUBSCRIBE EASERS ke listserv@copper.usm.edu. Untuk mengirim pesan email ke semua pelanggan, Anda akan mengirim email ke erars@copper.usm.edu.

Listservs dapat menjadi alat bisnis yang berguna jika Anda mencari informasi mengenai topik tertentu, atau jika Anda ingin menjadi bagian dari diskusi berkelanjutan mengenai topik tertentu. Dengan berlangganan listserv tentang topik yang Anda minati, Anda dapat menerima email terus-menerus dari anggota lain di seluruh dunia yang tertarik dengan topik yang sama. Bisnis juga dapat menggunakan listservs untuk berkomunikasi dengan pelanggan mereka tentang produk dan layanan. Untuk mengetahui listservs apa saja yang tersedia, kunjungi situs Web www.lsoft.com/lists/listref.html.

Streaming audio dan video

Streaming audio dan video melibatkan pengunduhan file audio atau video terkompresi secara terus-menerus, yang kemudian dapat didengar atau dilihat di stasiun kerja pengguna. Contoh umum dari audio streaming adalah musik populer dan klasik, siaran radio langsung,

dan ceramah sejarah atau arsip, musik, dan siaran radio. Contoh umum dari video streaming mencakup rekaman acara televisi dan produksi video lainnya, ceramah, dan produksi video langsung. Bisnis dapat menggunakan streaming audio dan video untuk menyediakan video pelatihan, sampel produk, dan siaran langsung dari kantor perusahaan, dan masih banyak lagi. Untuk mengirim dan menerima streaming audio dan video, server jaringan memerlukan ruang yang diperlukan untuk menyimpan data dan perangkat lunak untuk mengirimkan streaming, dan browser pengguna memerlukan produk streaming seperti RealPlayer dari RealNetworks untuk menerima dan menampilkan streaming. Semua file audio dan video harus dikompresi karena aliran data yang tidak dikompresi akan menghabiskan terlalu banyak bandwidth dan tidak akan mengalir secara real-time (ingat teknik kompresi dari Bab Lima).

Real-Time Protocol (RTP) dan Real-Time Streaming Protocol (RTSP) adalah dua protokol lapisan aplikasi umum yang digunakan server dan Internet untuk mengirimkan data streaming audio dan video ke browser pengguna. Baik RTP dan RTSP adalah protokol domain publik dan tersedia di sejumlah produk perangkat lunak yang mendukung streaming data.

Pesan instan, tweet, dan blog

Pesan instan (IM) memungkinkan pengguna untuk melihat apakah orang sedang login ke jaringan dan, jika ya, mengirimi mereka pesan singkat secara real time. Banyak pengguna, terutama di lingkungan korporat, yang beralih dari email dan menggunakan pesan instan sebagai sarana berkomunikasi. Keuntungan dari pesan instan mencakup percakapan real-time, penghematan penyimpanan server (karena Anda tidak menyimpan dan meneruskan pesan instan, seperti yang Anda lakukan melalui email), dan kemampuan untuk melakukan percakapan “diam” antara banyak pihak. Penyedia layanan seperti AOL, MSN Microsoft, dan Yahoo!, serta sejumlah perusahaan perangkat lunak lainnya, memasukkan pesan instan ke dalam produk mereka.

Beberapa isu yang melibatkan pembuatan dan dukungan sistem pesan instan meliputi:

- Identifikasi pengguna yang tepat
- Bagaimana cara mengetahui apakah pengguna yang Anda coba hubungi ada
- Apakah mungkin untuk membatasi siapa yang dapat melihat kehadiran Anda dan kapan
- Apakah Anda dapat mengirim pesan singkat satu kalimat saja atau sesuatu yang lebih rumit
- Apakah sistem dapat mendukung mode percakapan antara dua pengguna
- Apakah sistem dapat mendukung mode ruang obrolan yang melibatkan banyak pengguna

Salah satu layanan terbaru yang ditawarkan di Internet adalah Twitter. Twitter adalah layanan yang memungkinkan individu mengirim pesan singkat (maksimum 140 karakter) ke banyak pengguna. Ini pada dasarnya adalah persilangan antara pesan instan dan blogging (blogging adalah ketika seseorang memposting komentar berkelanjutan—sebuah blog—untuk satu atau lebih pembaca). Pesan yang dikirim di Twitter disebut tweet. Pembuat tweet hanya dapat mengizinkan pengguna tertentu untuk membaca atau mengizinkan masyarakat umum untuk membaca tweet tersebut.

Sekarang setelah kita memiliki pemahaman teknis tentang Internet, mari kita lihat bagaimana Internet dapat berdampak pada bisnis.

10.5 INTERNET DAN BISNIS

Sepanjang bab ini, banyak referensi telah dibuat mengenai bagaimana Internet mempengaruhi bisnis. Istilah yang mewakili transaksi komersial suatu bisnis melalui Internet adalah e-commerce. E-commerce juga dapat didefinisikan sebagai pembelian dan penjualan barang dan jasa melalui Internet, dan khususnya melalui World Wide Web. Untuk memahami isu dan tren penting yang terkait dengan persinggungan antara teknologi dan bisnis, mari kita bagi lagi e-commerce menjadi empat bidang berikut:

- *E-retailing*—E-retailing adalah penjualan dan pembelian barang dagangan secara elektronik menggunakan Web. Hampir semua jenis produk tersedia untuk dibeli melalui Web. Merchandiser Web yang canggih dapat melacak kebiasaan pembelian pelanggan mereka, menyediakan pemesanan online, mengizinkan pembelian dengan kartu kredit, dan menawarkan berbagai pilihan produk dan harga yang biasanya tidak ditawarkan di toko fisik.
- *Pertukaran data elektronik*—Pertukaran data elektronik (EDI) adalah transaksi komersial elektronik antara dua perusahaan atau lebih. Misalnya, perusahaan yang ingin membeli telepon seluler dalam jumlah besar dapat mengirimkan permintaan elektronik ke sejumlah produsen telepon seluler. Produsen dapat mengajukan penawaran secara elektronik, dan perusahaan dapat menerima tawaran serta melakukan pemesanan secara elektronik. Dana bank juga akan ditransfer secara elektronik antara perusahaan dan banknya.
- *Pemasaran mikro*—Pemasaran mikro adalah pengumpulan dan penggunaan kebiasaan penelusuran pelanggan potensial dan pelanggan saat ini, yang merupakan data penting bagi banyak perusahaan. Ketika sebuah perusahaan mengetahui dan memahami kebiasaan pelanggannya, perusahaan dapat menargetkan produk tertentu kepada individu tertentu.
- *Keamanan Internet*—Sistem keamanan yang mendukung semua transaksi Internet juga dianggap sebagai bagian penting dari e-commerce.

Banyak analis memperkirakan bahwa, meskipun terjadi kehancuran dot-com pada awal abad kedua puluh satu, e-commerce tidak akan hilang—bahkan, e-commerce akan terus mengalami pertumbuhan yang luar biasa di tahun-tahun mendatang. Tidak ada keraguan bahwa e-commerce mempunyai potensi menjadi industri luar biasa yang akan menghasilkan banyak lapangan kerja.

Cookie dan informasi negara

Salah satu fitur Web yang digunakan banyak bisnis dan telah menerima banyak publisitas negatif di masa lalu adalah cookie. Cookie adalah data yang dibuat oleh server Web yang disimpan di hard drive stasiun kerja pengguna. Data ini, disebut informasi negara, menyediakan cara bagi situs Web yang menyimpan cookie untuk melacak pola dan preferensi penjelajahan Web pengguna. Server Web dapat menggunakan informasi negara untuk

memprediksi kebutuhan masa depan, dan informasi negara dapat membantu situs Web melanjutkan aktivitas yang dimulai pada waktu sebelumnya. Misalnya, jika Anda menjelajahi situs Web yang menjual produk, situs Web tersebut mungkin menyimpan cookie di mesin Anda yang menjelaskan produk apa yang Anda lihat. Ketika Anda mengunjungi situs tersebut di kemudian hari, situs Web tersebut dapat mengekstrak informasi negara bagian dari cookie dan menanyakan apakah Anda ingin melihat kembali produk tertentu tersebut atau produk serupa. Aplikasi umum lainnya yang menyimpan cookie pada mesin pengguna termasuk mesin pencari, keranjang belanja yang digunakan oleh pengecer Web, dan aplikasi e-commerce yang aman.

Informasi tentang kebiasaan menonton sebelumnya yang disimpan dalam cookie juga dapat digunakan oleh situs Web lain untuk menyediakan konten yang disesuaikan. Salah satu penggunaan cookie baru-baru ini melibatkan penyimpanan informasi yang membantu situs Web memutuskan spanduk iklan mana yang akan ditampilkan di layar pengguna. Dengan teknik ini, situs Web dapat menyesuaikan iklan dengan profil pengguna aktivitas Web sebelumnya.

Meskipun pemilik situs Web membela penggunaan cookie karena bermanfaat bagi konsumen Web, banyak pengguna merasa bahwa penyimpanan informasi oleh situs Web di komputer mereka merupakan pelanggaran privasi. Pengguna yang prihatin dengan masalah privasi ini dapat menginstruksikan browser mereka untuk memberi tahu mereka setiap kali situs Web menyimpan cookie dan memberikan opsi untuk menonaktifkan penyimpanan cookie. Pengguna juga dapat melihat cookie mereka (yang mungkin tidak dapat dibaca) dan menghapus file cookie mereka. Browser Firefox menyimpan cookie dalam file bernama Cookies.txt; Internet Explorer menyimpan setiap cookie sebagai file terpisah dalam subdirektori cookie khusus.

Intranet dan ekstranet

Salah satu keunggulan Internet yang paling hebat adalah siapa pun di mana pun di dunia dapat mengakses informasi yang Anda kirimkan, baik itu halaman Web atau file FTP. Bagi banyak orang, aksesibilitas inilah yang diinginkan. Namun, sebuah perusahaan mungkin tidak ingin seluruh dunia melihat satu atau lebih halaman Web-nya. Misalnya, sebuah perusahaan mungkin ingin mengizinkan karyawannya mengakses database dengan mudah, namun melarang akses oleh siapa pun di luar perusahaan. Apakah mungkin untuk menawarkan layanan seperti Internet di dalam perusahaan, yang hanya dapat diakses oleh karyawan perusahaan tersebut? Jawabannya adalah ya, dan layanan tersebut disebut intranet. Intranet adalah jaringan TCP/IP di dalam perusahaan yang memungkinkan karyawan mengakses sumber informasi perusahaan melalui antarmuka seperti Internet. Dengan menggunakan browser Web di stasiun kerja, seorang karyawan dapat melakukan operasi penelusuran, namun aplikasi yang dapat diakses melalui browser hanya tersedia untuk karyawan di dalam perusahaan. Misalnya, intranet perusahaan dapat digunakan untuk menyediakan email karyawan dan akses ke perangkat lunak groupware, database klien/server perusahaan, aplikasi sumber daya manusia perusahaan, atau aplikasi khusus dan aplikasi lama.

Intranet pada dasarnya menggunakan perangkat keras dan perangkat lunak yang sama dengan yang digunakan oleh aplikasi jaringan lain seperti penjelajahan Web Internet, sehingga menyederhanakan biaya instalasi, pemeliharaan, serta perangkat keras dan perangkat lunak. Jika diinginkan oleh perusahaan, perusahaan dapat mengizinkan intranet dan sumber dayanya diakses dari luar tembok perusahaan. Dalam keadaan seperti ini, ID pengguna dan kata sandi sering kali diperlukan untuk mendapatkan akses. Perusahaan dapat menggunakan intranet untuk membangun akses ke database internal seperti informasi sumber daya manusia, data penggajian, dan catatan personalia; untuk berinteraksi dengan aplikasi perusahaan; untuk melakukan pencarian teks lengkap pada dokumen perusahaan; dan untuk memungkinkan karyawan mengakses dan mengunduh materi dan manual pelatihan, dan melakukan operasi bisnis sehari-hari, seperti mengisi laporan biaya perjalanan. Kemungkinan Anda mendaftar untuk kelas menggunakan intranet perguruan tinggi Anda.

Ketika intranet diperluas ke luar tembok perusahaan untuk mencakup pemasok, pelanggan, atau agen eksternal lainnya, itu menjadi ekstranet. Karena ekstranet memungkinkan agen eksternal memiliki akses ke sumber daya komputasi perusahaan, biasanya tingkat keamanan yang jauh lebih tinggi ditetapkan. Pada dasarnya, ekstranet adalah interkoneksi intranet perusahaan. Interkoneksi biasanya dilakukan melalui Internet, menggunakan jaringan pribadi virtual. Ingatlah bahwa jaringan pribadi virtual menggunakan protokol terowongan untuk membuat koneksi yang tidak dapat disadap oleh pihak luar.

Tentu saja, bisnis telah memanfaatkan Internet dalam berbagai bentuknya. Banyak perusahaan yang memperoleh keuntungan dengan memperkenalkan Internet ke dalam operasi bisnis mereka, dan jumlah yang sama juga mengalami kerugian. Naik turunnya kekayaan berdasarkan Internet dan teknologi terkait mungkin terlalu sulit diprediksi oleh siapa pun. Meskipun kita tidak dapat memprediksi masa depan dari sisi bisnis Internet, kita dapat melihat masa depan teknologi Internet.

10.6 MASA DEPAN INTERNET

Internet bukanlah entitas statis. Ini terus berkembang dengan menambah jaringan baru dan pengguna baru setiap hari. Orang-orang terus berupaya memperbaiki dan merevisi berbagai komponen Internet. Kekuatan pendorong di balik semua perubahan ini, serta semua protokol Internet, adalah pemerintahan Internet yang mengatur dirinya sendiri. Berdasarkan struktur komite, pemerintahan ini terdiri dari banyak komite dan kelompok, antara lain:

- **Internet Society (ISOC)**—Sebuah organisasi sukarelawan yang menentukan arah masa depan Internet
- **Intrnet Architecture Board (IAB)**—Sekelompok sukarelawan yang diundang dan menyetujui standar
- **Internet Engineering Task Force (IETF)**—Kelompok relawan yang mendiskusikan permasalahan operasional dan teknis
- **Internet Research Task Force (IRTF)**—Kelompok yang mengkoordinasikan kegiatan penelitian

- **World Wide Web Consortium (W3C)**—Konsorsium industri Web yang mengembangkan protokol umum dan berupaya memastikan interoperabilitas di antara protokol-protokol tersebut
- **Internet Corporation for Assigned Names and Numbers (ICANN)**—Sebuah organisasi internasional yang anggotanya mengontrol nama dan nomor yang terkait dengan alamat Web
- Lebih banyak lagi kelompok pengarah, kelompok penelitian, dan kelompok kerja

Tempat terbaik untuk mencari perubahan yang baru saja diselesaikan dan perubahan yang sedang berlangsung adalah halaman Web Kelompok Kerja Satuan Tugas Rekayasa Internet. Situs web IETF adalah www.ietf.org; ini berisi semua informasi terkini yang tersedia tentang Internet dan protokolnya.

Salah satu perubahan terbesar yang mempengaruhi Internet dalam waktu dekat adalah penerapan IPv6. (Jika Anda bertanya-tanya, IPv5 bukanlah versi yang terbuka untuk umum tetapi digunakan untuk menguji konsep-konsep baru.) Selain transisi dari IPv4 ke IPv6, sebuah konsorsium universitas, dunia usaha, dan pemerintah menciptakan sebuah proyek yang sangat -jaringan berkecepatan tinggi yang mencakup Amerika Serikat, menghubungkan universitas dan pusat penelitian dengan kecepatan transmisi hingga gigabit per detik (1000 Mbps). Jaringan berkecepatan tinggi baru disebut Internet2.

Pencipta Internet2 bertujuan untuk menyediakan akses berkecepatan tinggi ke gambar digital, video, dan musik, serta item berbasis teks yang lebih tradisional. Secara khusus, Internet2 telah menargetkan sejumlah area aplikasi utama, termasuk perpustakaan digital, tele-immersion, dan laboratorium virtual.

Perpustakaan digital adalah representasi elektronik dari buku, majalah, makalah, seni, video, dan musik. Pelanggan yang mengakses perpustakaan digital dapat dengan cepat mengambil dokumen apa pun menggunakan bahasa kueri yang kuat. Bahkan seni, video, dan musik dapat diambil dengan menentukan satu atau lebih kata kunci yang menggambarkan isi karya tersebut.

Tele-immersion memungkinkan pengguna di lokasi yang berbeda secara geografis untuk berkolaborasi secara real-time dalam lingkungan simulasi bersama. Teknologi ini memiliki kemampuan audio dan video interaktif berkekuatan tinggi yang memungkinkannya membuat pengguna merasa seolah-olah berada di ruangan yang sama. Beberapa alat canggih ini mencakup pemindaian lingkungan tiga dimensi dan teknologi proyektif, pelacakan, dan tampilan.

Dengan laboratorium virtual Internet2, dimungkinkan untuk menciptakan lingkungan laboratorium yang realistis tanpa mengorbankan fasilitas fisik. Melalui laboratorium virtual, mahasiswa dan peneliti dapat melakukan eksperimen yang tidak dapat dilakukan di dunia nyata, seperti ledakan atom. Ditambah lagi, jika laboratorium virtual dipadukan dengan area penerapan tele-immersion, mahasiswa dan peneliti dari seluruh dunia akan dapat berkolaborasi dalam satu atau lebih proyek.

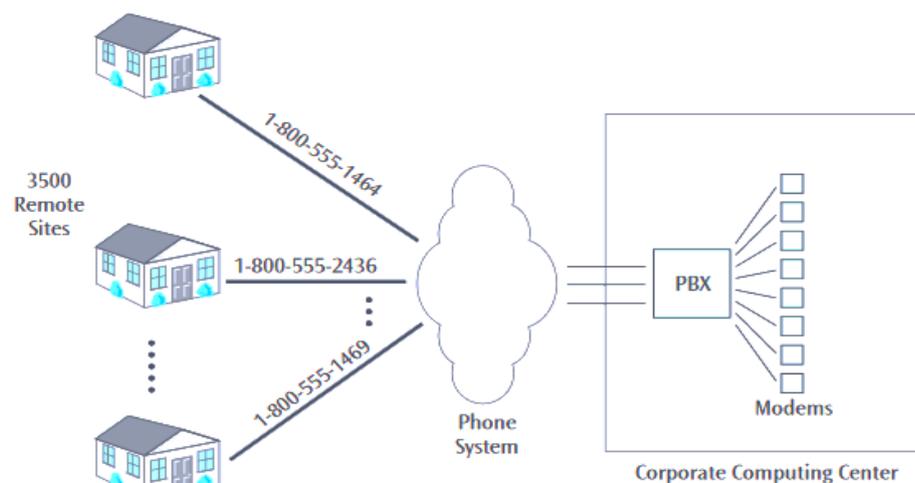
Dari segi teknologi, Internet2 bukan sekadar jaringan fisik, sebagaimana Internet saat ini, dan tidak akan menggantikan Internet. Sebaliknya, Internet2 merupakan hasil kemitraan

antara universitas (lebih dari 200 sekolah yang berpartisipasi), industri (puluhan perusahaan terkemuka), dan pemerintah; organisasi-organisasi ini memiliki tujuan yang sama untuk mengembangkan teknologi dan kemampuan baru yang pada akhirnya akan dapat diakses oleh banyak pengguna. Baik dunia usaha maupun komunitas akademis akan mendapatkan manfaat dari penciptaan dan penerapan teknologi dan kemampuan baru ini.

Sekarang, mari kita lihat contoh yang menerapkan apa yang telah kita pelajari tentang aspek teknologi dan bisnis di Internet.

10.7 PERUSAHAAN MENCIPTAKAN VPN

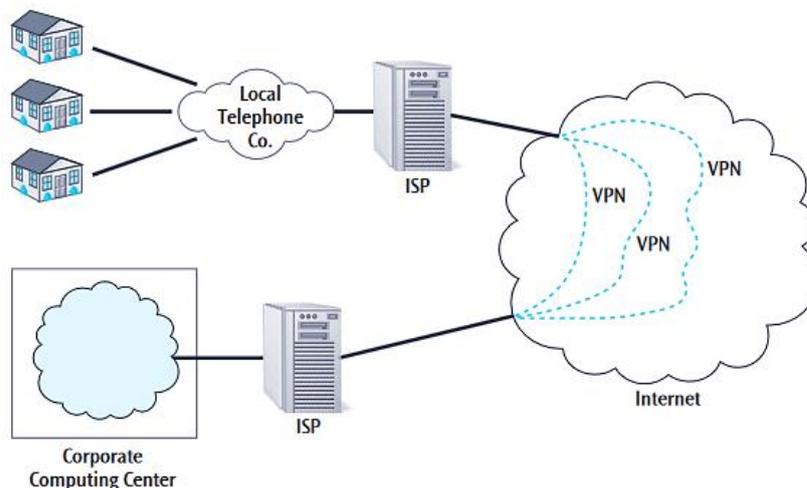
CompuCom, reseller workstation fiktif, sedang mencari cara untuk membuat tenaga penjualannya lebih produktif dan menghemat uang. Salah satu opsi yang mungkin dilakukan adalah mengizinkan tenaga penjualan bekerja dari rumah. Dengan menggunakan komputer di rumah, setiap karyawan dapat mengakses jaringan perusahaan untuk mengirim dan mengambil pesan serta mengakses database perusahaan. Manajemen di CompuCom mengetahui bahwa ada sejumlah cara yang dapat diatur perusahaan agar karyawan dapat mengakses jaringan perusahaan.



Gambar 10-10 Karyawan CompuCom melakukan panggilan langsung ke pusat komputasi perusahaan

Pertama, karyawan dapat menggunakan modem dial-up untuk terhubung dengan sistem perusahaan. Masalah dengan solusi ini adalah modem dial-up lambat, dan perusahaan memerlukan satu modem di lokasi untuk setiap karyawan yang melakukan panggilan (Gambar 10-10). Pilihan lainnya adalah mengatur setiap karyawan untuk menggunakan DSL atau modem kabel, yang keduanya jauh lebih cepat dibandingkan modem dial-up. DSL atau modem kabel karyawan akan terhubung ke penyedia layanan Internet, melalui Internet, dan ke jaringan perusahaan. Masalah terbesar di sini adalah keamanan. Kecuali jika tindakan khusus diambil, data apa pun yang ditransfer melalui Internet tidak akan aman. CompuCom ingin memanfaatkan Internet karena tersebar luas dan harganya ekonomis, namun perusahaan juga memerlukan cara untuk menciptakan koneksi yang aman.

Pada akhirnya, CompuCom memutuskan untuk membuat jaringan pribadi virtual. VPN adalah koneksi jaringan data yang memanfaatkan infrastruktur telekomunikasi publik namun tetap menjaga privasi melalui penggunaan protokol terowongan dan prosedur keamanan. Protokol terowongan, seperti Protokol Tunneling Point-to-Point, adalah kumpulan perintah yang memungkinkan organisasi membuat koneksi aman menggunakan sumber daya publik seperti Internet. Perhatikan bahwa jalur komunikasi ini bukanlah sambungan pribadi sepenuhnya, sebagaimana saluran telepon sewaan. Untuk membuat jaringan dengan saluran sewaan, CompuCom memerlukan perusahaan telepon untuk memasang sirkuit khusus antara dua lokasi yang tidak dapat digunakan oleh orang lain. Sebaliknya, VPN melalui Internet menggunakan sirkuit publik yang digunakan bersama oleh ribuan pengguna setiap detiknya. Namun, dengan informasi perutean khusus dan langkah-langkah keamanan tinggi, VPN dapat dibuat yang hanya dapat diakses dan dipahami oleh Anda.



Gambar 10-11 Karyawan CompuCom menggunakan terowongan melintasi Internet ke pusat komputasi perusahaan

Dengan menggunakan Internet sebagai media transfer, VPN menawarkan sejumlah keuntungan. Karena Internet praktis ada di mana-mana, VPN dapat dibuat antara dua titik mana pun. Karena Internet relatif ekonomis, VPN juga relatif ekonomis. Setelah koneksi ke Internet tercapai (melalui penyedia layanan Internet), data yang ditransfer melalui Internet—dan melalui VPN—gratis. Internet—dan juga VPN—menjaga lingkungan yang relatif stabil dengan keluaran yang wajar.

Dengan VPN CompuCom, karyawan di rumah terhubung ke penyedia layanan Internet lokalnya melalui koneksi DSL atau modem kabel. Setelah pengguna terhubung ke Internet, perangkat lunak tunneling membuat koneksi aman melalui Internet ke pusat komputasi perusahaan (Gambar 10-11).

VPN adalah salah satu contoh penggunaan kreatif dari Internet yang sangat populer dan kuat. Ketika bisnis terus belajar menggunakan Internet, mereka akan mampu memperluas jangkauannya ke wilayah baru dan meningkatkan strategi komunikasi yang ada.

RINGKASAN

- Untuk mendukung Internet, diperlukan banyak protokol, seperti IP, TCP, ICMP, UDP, ARP, DHCP, dan NAT.
- Protokol Internet menyediakan transfer data tanpa koneksi melalui berbagai jenis jaringan. Saat ini ada dua versi IP: IPv4 dan IPv6.
- Protokol Kontrol Transmisi berada pada lapisan transport model komunikasi dan menyediakan koneksi end-to-end yang bebas kesalahan.
- Internet Control Message Protocol melakukan pelaporan kesalahan untuk Protokol Internet.
- Protokol Datagram Pengguna menyediakan protokol lapisan transport tanpa koneksi, sebagai pengganti TCP.
- Protokol Resolusi Alamat menerjemahkan alamat IP menjadi alamat MAC CSMA/CD untuk pengiriman data pada jaringan area lokal.
- Protokol Konfigurasi Host Dinamis memungkinkan jaringan untuk secara dinamis menetapkan alamat IP ke stasiun kerja sesuai kebutuhan.
- Terjemahan Alamat Jaringan memungkinkan jaringan mengganti alamat IP lokal dengan satu alamat IP tipe global.
- Protokol terowongan memungkinkan perusahaan untuk membuat koneksi jaringan pribadi virtual ke dalam sistem komputasi perusahaan.
- *World Wide Web* adalah kumpulan besar dokumen elektronik yang berisi teks dan gambar yang dapat diakses hanya dengan mengklik link di halaman Web browser. Browser menggunakan HTTP untuk mengirim dan menerima halaman Web, dan HTML untuk menampilkan halaman Web tersebut.
- Untuk mencari lokasi dokumen di Internet, Anda biasanya mengacu pada *Uniform Resource Locator*. URL secara unik mengidentifikasi setiap dokumen di setiap server di Internet. Salah satu komponen URL adalah alamat situs dokumen yang diminta. Setiap alamat situs terdiri dari ID jaringan dan ID host atau perangkat. Alamat situs diubah menjadi alamat IP 32-bit atau 128-bit oleh Sistem Nama Domain.
- Internet terdiri dari banyak aplikasi jaringan yang umum digunakan.
- Surat elektronik, atau email, merupakan persyaratan standar untuk sebagian besar operasi bisnis dan dapat mentransfer pesan teks standar serta menyertakan lampiran berkode MIME. Protokol seperti *Simple Mail Transfer Protocol*, *Post Office Protocol* versi 3, dan *Internet Message Access Protocol* mendukung pengoperasian email.
- File Transfer Protocol berguna untuk mengunggah atau mengunduh file melalui Internet.
- Login jarak jauh menggunakan Telnet memungkinkan seseorang untuk login ke situs komputer jarak jauh dan melakukan operasi seolah-olah pengguna secara fisik berada di situs jarak jauh tersebut.
- VoIP (telepon Internet) menawarkan alternatif yang murah dibandingkan panggilan jarak jauh, namun kualitasnya dipertanyakan. Internet tidak dirancang untuk mentransfer data secara real-time, yang merupakan kemampuan yang diperlukan untuk

mendukung suara interaktif. Namun demikian, banyak bisnis yang menggunakan VoIP secara internal sebagai cara untuk menghadirkan gabungan aplikasi suara dan data.

- Listserv adalah program perangkat lunak populer yang digunakan untuk membuat dan mengelola milis Internet.
- Streaming audio dan video adalah pengunduhan file audio atau video terkompresi secara terus-menerus, yang kemudian didengar atau ditampilkan di stasiun kerja pengguna. Streaming audio dan video memerlukan protokol pendukung seperti *Real-Time Protocol* dan *Real-Time Streaming Protocol*.
- Pesan instan semakin populer sebagai cara untuk menjaga komunikasi real-time di antara banyak pengguna.
- Twitter dan blog adalah dua aplikasi Internet yang memungkinkan individu mengirimkan informasi untuk satu atau lebih pengguna.
- *E-commerce* adalah pembelian dan penjualan barang dan jasa secara elektronik. Banyak perusahaan yang melakukan investasi besar-besaran pada *e-commerce* dengan harapan hal ini akan meningkatkan pangsa pasar dan menurunkan biaya.
- Cookies menyimpan informasi status pada *hard drive* pengguna dan menyediakan cara bagi situs Web untuk melacak pola dan preferensi penjelajahan Web pengguna.
- Intranet adalah Internet internal dengan layanan seperti Web yang hanya tersedia bagi karyawan perusahaan atau pelanggan dan pemasok melalui ekstranet.
- Internet terus berkembang, dengan Protokol Internet versi 6 serta Internet2 yang benar-benar baru dan berkecepatan lebih tinggi.

PERTANYAAN

1. Apa cikal bakal Internet saat ini?
2. Sebutkan tanggung jawab utama Protokol Internet.
3. Sebutkan tanggung jawab utama Protokol Pengendalian Transmisi.
4. Jelaskan hubungan nomor port dengan alamat IP.
5. Apakah UDP sama dengan TCP? Menjelaskan.
6. Apa tujuan MPLS?
7. Apa hubungan antara IP dan ICMP?
8. Apakah DHCP sama dengan NAT? Menjelaskan.
9. Apa hubungan antara Internet dan World Wide Web?
10. Untuk apa HTTP digunakan?
11. Apa perbedaan bahasa markup Web dengan bahasa pemrograman?
12. Apa tujuan dari Uniform Resource Locator?
13. Sebutkan empat bagian dasar URL.
14. Bagaimana Sistem Nama Domain menerjemahkan URL menjadi alamat biner 32-bit?
15. Apa saja kelas alamat IP yang berbeda?
16. Untuk apa Protokol Transfer File digunakan?
17. Apa fungsi utama Telnet?
18. Apakah VoIP lebih dapat diandalkan dalam bisnis atau melalui Internet? Menjelaskan.

19. Pilihan lain apa yang tersedia untuk transmisi suara melalui teknologi Internet selain Voice over IP?
20. Sebutkan ciri-ciri dasar sistem surat elektronik yang umum.
21. Apa tugas SMTP, POP3, dan IMAP jika mengacu pada sistem email?
22. Untuk apa listserv digunakan?
23. Alat apa saja yang diperlukan untuk mendukung streaming audio atau video?
24. Apa perbedaan pesan instan dengan email?
25. Apa dua protokol bersaing yang digunakan untuk mendukung pesan instan?
26. Apa hubungan antara pertukaran data elektronik dan e-commerce?
27. Apa itu kue? Siapa yang membuat kue dan di mana disimpan?
28. Apa perbedaan intranet dan ekstranet dengan Internet?
29. Bagaimana sebuah bisnis dapat menggunakan jaringan pribadi virtual dan terowongan untuk mendukung koneksi di luar lokasi?
30. Apa perbedaan IPv6 dengan versi IP saat ini (4)?
31. Apa saja fitur utama Internet2?
32. Apa perbedaan antara VoIP dan VoWLAN?

LATIHAN SOAL

1. Apakah pemerintah AS mendukung Internet? Menjelaskan.
2. Mengingat paket IP sebesar 540 byte dan ukuran paket maksimum 200 byte, berapakah IP Fragment Offsets dan More Flags untuk fragmen paket yang sesuai?
3. Bidang Batas Hop di IPv6 panjangnya 8 bit (ukuran sama dengan bidang Time to Live yang setara di IPv4). Mengingat bahwa jumlah hop ini berkurang setiap kali datagram IP memasuki router, apa implikasi dari memiliki ukuran field yang kecil?
4. Misalkan ada sebuah bangunan ritel komersial kecil di kota Anda yang pada dasarnya mempunyai satu ruangan. Di satu sisi ruangan ada agen real estat, dan di sisi lain ruangan ada seorang lelaki yang menjual teh. Bagaimana situasi ini dapat dianalogikan dengan konsep alamat IP dengan nomor port TCP?
5. Di suatu tempat di Amerika Serikat terdapat dua router Internet dengan tabel perutean yang semuanya kacau. Kedua router terus mengirimkan paketnya bolak-balik satu sama lain, tanpa henti. Akankah pesan kesalahan dihasilkan dari tindakan ini? Jika ya, siapa yang akan menghasilkan pesan kesalahan tersebut, dan seperti apa tampilannya?
6. Mengapa ARP diperlukan jika setiap workstation yang terhubung ke Internet memiliki alamat IP unik?
7. Jika saya menyambung ke Internet dari rumah, apakah workstation saya mungkin menggunakan DHCP? Menjelaskan.
8. Jika seseorang di Internet mengirim Anda email, apakah NAT akan menghapusnya sebelum dikirimkan kepada Anda? Mengapa atau mengapa tidak?

9. Jika tiga pengguna di satu jaringan area lokal semuanya meminta halaman Web pada saat yang sama, bagaimana NAT mengetahui hasil mana yang masuk ke stasiun kerja mana?
10. Jika stasiun kerja komputer Anda memiliki alamat IP berkelas 167.54.200.32, apakah itu alamat IP Kelas A, B, C, D, atau E? Berapa banyak perangkat/host di kelas itu?
11. Jika suatu perusahaan diberi alamat jaringan 177.56.42.0/26, berapa banyak alamat perangkat/host yang tersedia?
12. Apa keuntungan dan kerugian menggunakan penetapan alamat IP dinamis?
13. Temukan dan beri label layanan, nama host, direktori, dan nama file dalam URL hipotetis berikut: <http://www.reliable.com/listings/pages/web.htm> .
14. Dengan menggunakan browser Web, buka situs ftp.hpl.hp.com dan daftarkan tiga subdirektori di direktori pub.
15. Jika Anda menggunakan komputer Anda terutama untuk mengakses komputer jarak jauh melalui Telnet, apakah Anda akan dikenakan tagihan telepon jarak jauh yang besar? Menjelaskan.
16. Apa perbedaan antara suara melalui Internet dan VoIP pribadi?
17. Ubah nomor telepon 413 555-2068 menjadi bentuk ENUM.
18. Sehubungan dengan email, apa hubungan antara SMTP dan POP3? Bisakah yang satu beroperasi tanpa yang lain? Menjelaskan.
19. Perusahaan Anda meminta Anda untuk selalu mengikuti etika kerja. Layanan Internet manakah yang diperkenalkan dalam bab ini yang paling membantu Anda menyelesaikan tugas ini?
20. Apakah HTTP dan HTML merupakan dua protokol yang memiliki fungsi yang sama? Menjelaskan.
21. Beberapa protokol baru, seperti IPv6, tidak menyertakan skema deteksi kesalahan apa pun pada bagian data paket. Apa signifikansi tren ini?

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Anda bekerja di perusahaan yang ingin memulai pertukaran data elektronik dengan dua perusahaan lain yang memasok suku cadang. Perusahaan Anda memproduksi telepon seluler, dan dua perusahaan lainnya memproduksi baterai dan papan tombol telepon. Saat perusahaan Anda memesan ke perusahaan baterai, perusahaan tersebut akan menentukan ukuran baterai, jenis baterai, daya baterai, dan kuantitas. Saat perusahaan Anda memesan ke perusahaan papan tombol, perusahaan tersebut akan menentukan konfigurasi papan tombol, konsumsi daya, dimensi papan tombol, dan warna papan tombol. Bagaimana XML dapat digunakan untuk mendukung EDI di antara perusahaan-perusahaan ini?
2. Dua bank ingin membangun hubungan elektronik antara mereka, dimana mereka dapat mengirimkan transfer uang. Bisakah mereka menggunakan jaringan pribadi virtual dan protokol penerowongan, atau apakah tersedia teknik yang lebih baik? Pertahankan jawaban Anda.

3. Anda bekerja di perusahaan yang menjual sepeda kelas atas dan memutuskan untuk membuat serangkaian halaman Web untuk mempromosikan penjualan. Jenis layanan apa yang mungkin Anda tawarkan di halaman Web Anda? Apakah halaman Web Anda akan menggunakan HTML, HTML dinamis, atau bahasa lain? Bagaimana perusahaan Anda dapat menggunakan cookie untuk keuntungannya?
4. Anda berpikir untuk membuat solusi jaringan untuk bisnis kecil dengan sekitar 10 pengguna. Anda memberi setiap pengguna stasiun kerja dan akses ke Internet. Protokol Internet manakah yang perlu didukung oleh jaringan dan stasiun kerja Anda? Protokol Internet opsional manakah yang mungkin Anda terapkan?
5. Suatu perusahaan saat ini memiliki sistem telepon dan sistem jaringan area lokal yang terpisah. Perusahaan ini sedang mempertimbangkan untuk mengubah sistem teleponnya menjadi VoIP, dan menjalankan suara dan data melalui sistem jaringan area lokal. Apa yang harus dipertimbangkan perusahaan sebelum mengambil langkah ini?
6. Dengan menggunakan komputer Anda di rumah atau di sekolah, temukan semua cookie yang tersimpan di hard disk drive Anda. Bisakah Anda mengetahuinya dengan memeriksa kue siapa yang menaruhnya di sana? Mengapa atau mengapa tidak?
7. Di Web, temukan salinan gratis pemutar audio atau video streaming dan unduh ke mesin Anda. Kemudian, temukan situs Web yang menyediakan program streaming audio atau video. Seberapa sulit pengunduhan dan pemasangan pemutar? Seberapa bagus kualitas streaming audio atau videonya?
8. Baik dengan menggunakan editor halaman Web atau dengan menulis kode HTML secara manual, buatlah halaman Web yang memiliki judul H1, beberapa teks, satu atau lebih link, dan satu atau lebih gambar.
9. Temukan contoh perusahaan yang melakukan pertukaran data elektronik. Perusahaan apa saja yang terlibat dalam pertukaran ini? Data apa yang ditransfer selama pertukaran? Detail apa lagi yang bisa Anda jelaskan?
10. Jika Anda memiliki akses Internet di kantor, sekolah, atau rumah, apa alamat IP stasiun kerja Anda? Apakah ditetapkan secara statis atau ditetapkan secara dinamis? Apakah alamat IP Anda berasal dari penyedia layanan Internet atau dari tempat lain? Jelaskan alasan Anda.
11. Siapakah “pemain” yang terlibat dengan Internet2 baru? Apa yang diperlukan untuk menjadi salah satu pemain ini?
12. Protokol lain apa yang digunakan untuk mendukung H.323?

BAB 11

JARINGAN PENGIRIMAN SUARA DAN DATA

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Identifikasi elemen dasar sistem telepon dan diskusikan keterbatasan sinyal telepon
- Jelaskan komposisi industri telepon sebelum dan sesudah Perubahan Keputusan Akhir tahun 1984 dan jelaskan perbedaannya
- Jelaskan perbedaan antara operator pertukaran lokal dan operator pertukaran, dan daftarkan layanan yang ditawarkan masing-masing
- Membedakan peran perusahaan telepon lokal sebelum dan sesudah UU Telekomunikasi tahun 1996
- Jelaskan karakteristik dasar koneksi Internet dial-up
- Sebutkan jenis-jenis saluran sewaan yang tersedia dan karakteristik dasarnya
- Identifikasi ciri-ciri utama saluran pelanggan digital, dan kenali perbedaan antara sistem simetris dan sistem asimetris
- Identifikasi karakteristik utama modem kabel
- Buat daftar karakteristik dasar frame relay, seperti sirkuit virtual permanen dan kecepatan informasi yang berkomitmen
- Identifikasi karakteristik utama Mode Transfer Asinkron, termasuk peran koneksi jalur virtual dan koneksi saluran virtual, pentingnya kelas layanan yang tersedia, serta kelebihan dan kekurangan ATM
- Sebutkan karakteristik dasar terowongan MPLS dan VPN, dan bagaimana pertumbuhannya dalam industri berdampak pada frame relay dan ATM
- Jelaskan konsep konvergensi dan identifikasi beberapa contohnya dalam industri jaringan

DULU, sebagian besar rumah dan apartemen hanya memiliki satu telepon. Telepon itu mempunyai nomor, dan selama Anda tidak pernah berpindah, Anda mungkin menyimpan nomor telepon itu untuk waktu yang lama. Dan karena tidak ada telepon seluler, nomor telepon rumah Anda adalah satu-satunya nomor telepon yang Anda miliki. Saat ini, orang cenderung lebih sering berpindah-pindah, dan hampir semua orang memiliki ponsel. Jika Anda berpindah dari satu kota ke kota lain, kemungkinan besar Anda memerlukan nomor telepon rumah baru.

Mengganti nomor telepon selalu merepotkan hingga saat ini. Pemerintah federal telah memberikan izin kepada perusahaan-perusahaan telepon seluler untuk memperbolehkan pelanggan menyimpan nomor telepon seluler mereka jika mereka berganti layanan, dan terdapat banyak spekulasi bahwa perusahaan-perusahaan non-telepon seluler pada akhirnya

akan mengikuti langkah yang sama. Jika dan ketika hal ini terjadi, ada kemungkinan seseorang memiliki satu nomor telepon seumur hidup, di mana pun dia tinggal.

Bayangkan suatu hari Anda berada di rumah sakit untuk kelahiran anak Anda. Saat menyelesaikan dokumen rumah sakit biasa, Anda menemukan tiga formulir yang menonjol dari yang lain. Yang pertama adalah formulir untuk bayi baru lahir Anda untuk menerima nomor Jaminan Sosial. Yang kedua adalah bayi menerima nomor telepon. Yang ketiga adalah agar anak Anda menerima URL untuk kebutuhan Internetnya di masa depan.

Apakah ini tampak tidak masuk akal?

Bisakah rumah sakit menetapkan hanya satu nomor untuk semua layanan?

Seberapa pentingkah sistem telepon umum?

Apakah ada layanan telepon lain yang mungkin berguna bagi kita?

11.1 PENDAHULUAN

Di Bab Sembilan, kita diperkenalkan dengan jaringan area luas. Kemudian di Bab Sepuluh, kita membahas salah satu kumpulan jaringan area luas yang paling terkenal: Internet. Meskipun Internet dapat mentransfer data konvensional dan data suara, Internet bukanlah satu-satunya jaringan area luas yang dapat melakukan hal ini. Faktanya, banyak jenis jaringan lain yang telah mengirimkan data dan suara melalui jarak lokal dan jarak jauh selama bertahun-tahun. Contoh paling jelas dari jaringan tersebut adalah sistem telepon. Meskipun awalnya dirancang untuk mengirimkan sinyal suara, jaringan telepon kini mentransfer lebih banyak data daripada suara.

Selain sistem telepon, sejumlah jaringan penting lainnya dapat mengirimkan data dan suara baik lokal maupun luas. Berbeda dengan jaringan telepon, jaringan ini awalnya dirancang untuk data. Lebih tepatnya, jaringan ini menyediakan beberapa bentuk layanan pengiriman data. Pelanggan menghubungi penyedia layanan dan meminta koneksi antara dua lokasi geografis. Setelah koneksi terbentuk, pelanggan dapat mentransfer data dengan kecepatan yang disesuaikan antara dua titik akhir. Seperti yang akan kita lihat segera, beberapa jaringan pengiriman data ini hanya bekerja pada jarak lokal, sementara yang lain bekerja pada jarak lokal dan jarak jauh. Namun sebelum kita memeriksa layanan pengiriman data yang lebih baru ini, mari kita periksa sistem teleponnya.

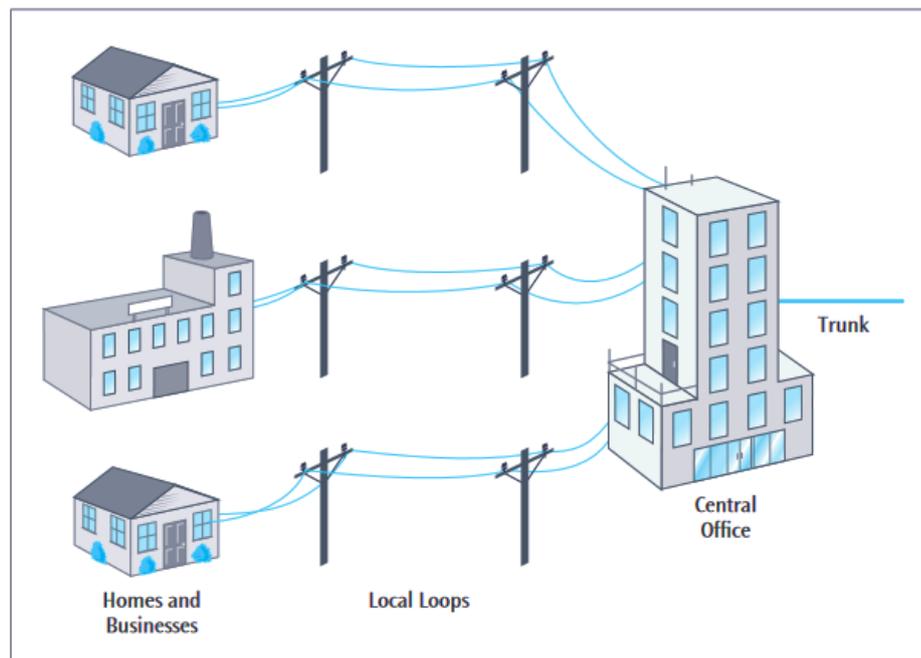
11.2 SISTEM TELEPON DASAR

Sistem telepon dasar, atau layanan telepon biasa (POTS), telah ada sejak awal tahun 1900-an. Selama sebagian besar tahun tersebut, POTS merupakan sistem analog yang mampu mendukung percakapan suara. Baru pada tahun 1970an POTS mulai membawa sinyal data komputer dan juga sinyal suara. Jumlah data yang dikirimkan melalui POTS akhirnya bertambah begitu besar sehingga menjelang akhir abad ke-20, sistem tersebut membawa lebih banyak data daripada suara. Meskipun telah mengalami sejumlah perubahan teknologi selama masa pakainya yang panjang, seperti meningkatnya penggunaan sinyal digital sebagai pengganti sinyal analog, POTS pada dasarnya masih merupakan media pembawa suara. Karena persyaratan yang terkait dengan pembawaan suara, POTS memiliki keterbatasan. Mari

kita mulai diskusi kita tentang jaringan telepon dengan mengkaji komposisi sistem telepon dasar, diikuti dengan bagaimana sistem telepon dipengaruhi oleh dua peristiwa besar dalam sejarah telepon: pecahnya AT&T pada tahun 1984 dan Undang-undang Telekomunikasi tahun 1996. .

Saluran telepon dan trunk

Di tengah semua perubahan hukum dan berbasis industri yang terjadi di bidang telekomunikasi selama bertahun-tahun, satu hal yang relatif konstan adalah saluran telepon dasar. Loop lokal adalah saluran telepon analog yang meninggalkan rumah atau bisnis Anda dan terdiri dari empat atau delapan kabel (Gambar 11-1). Meskipun hanya dua kabel yang diperlukan untuk melengkapi rangkaian telepon, perusahaan telepon sering kali memasang beberapa saluran jika pemilik rumah menginginkan layanan tambahan di masa mendatang. Di ujung lain dari lingkaran lokal adalah kantor pusat perusahaan telepon lokal. Kantor pusat (CO) berisi peralatan yang menghasilkan nada panggil, menafsirkan nomor telepon yang dihubungi, memeriksa layanan khusus, dan menghubungkan panggilan masuk ke titik berikutnya. Mulai dari kantor pusat dan seluruh jaringan telepon, semua sirkuit telepon bersifat digital.



Gambar 11-1 Loop lokal analog yang menghubungkan rumah Anda ke kantor pusat perusahaan telepon

Dari kantor pusat, sinyal dapat menuju ke salah satu dari tiga tempat:

- Lewatkan panggilan lokal lainnya ke sebuah rumah di lingkungan Anda, jika panggilannya bersifat lokal
- Ke kantor pusat lain di komunitas tetangga, jika panggilan tidak berada di lingkungan yang sama tetapi tidak jarak jauh
- Kepada penyedia layanan sambungan jarak jauh, jika panggilan telepon tersebut merupakan panggilan jarak jauh

Bagaimana jaringan telepon mengetahui bila panggilan telepon merupakan panggilan jarak jauh? Amerika Utara dibagi menjadi wilayah transportasi akses lokal. Area transportasi akses lokal (LATA) adalah wilayah geografis seperti wilayah metropolitan besar atau bagian dari negara bagian yang besar. Selama panggilan telepon tetap berada dalam LATA (panggilan intraLATA), panggilan telepon tersebut bersifat lokal dan ditangani oleh perusahaan telepon lokal. Jika panggilan telepon berpindah dari satu LATA ke LATA lainnya (panggilan interLATA), maka panggilan tersebut merupakan panggilan jarak jauh dan harus ditangani oleh perusahaan telepon jarak jauh. Karena banyaknya badan pengatur, terkadang melintasi batas negara bagian dapat berdampak pada biaya lokal versus jarak jauh. Namun perbedaan antara panggilan lokal dan panggilan jarak jauh mulai menghilang. Banyak, jika bukan sebagian besar, perusahaan telepon seluler kini menawarkan paket “satu tarif” yang tidak membedakan antara panggilan lokal dan jarak jauh. Kita sekarang melihat layanan jenis ini juga muncul di telepon non-seluler (kabel). Jika hal ini terus berlanjut, suatu saat nanti fungsi LATA akan menjadi mubazir.

Kembali ke dasar, jaringan telepon terdiri dari dua tipe dasar saluran telepon: loop pelanggan, atau saluran telepon standar, dan saluran induk. Lingkaran pelanggan, seperti kabel yang menghubungkan rumah dan kantor pusat, memiliki nomor telepon unik yang terkait dengannya. Sebuah bagasi tidak mempunyai nomor telepon yang terkait dengannya karena dapat membawa ratusan saluran suara dan data. Ratusan saluran suara dan data ini biasanya dibawa antara kantor pusat dan pusat peralihan telepon lainnya (gedung di mana sambungan telepon dibuat antar saluran utama). Kebanyakan trunk mengirimkan sinyal digital, dan akibatnya memerlukan repeater setiap beberapa kilometer. Sebaliknya, loop pelanggan biasanya mengirimkan sinyal analog, yang memerlukan amplifier setiap beberapa kilometer.

Sekarang kita telah melihat sistem telepon dasar. Sebelum kita memperkenalkan berbagai layanan yang ditawarkan oleh perusahaan telepon, mari kita periksa dua peristiwa besar baru-baru ini dalam sejarah jaringan telepon.

Jaringan telepon sebelum dan sesudah tahun 1984

Sebelum tahun 1984, AT&T (American Telephone and Telegraph) memiliki semua saluran telepon jarak jauh di Amerika Serikat, sebagian besar sistem telepon lokal, dan Bell Laboratories. Pada tahun 1970-an, pemerintah federal menggugat AT&T ke pengadilan dengan alasan pelanggaran antimonopoli. AT&T kalah dalam kasus ini, dan pada tahun 1984, keputusan akhir pengadilan, yang dikenal sebagai Modified Final Judgment, mengharuskan divestasi, atau pemisahan, AT&T menjadi beberapa perusahaan terpisah. Perpecahan ini memungkinkan AT&T untuk mempertahankan jalur jarak jauh dan Bell Labs, namun perusahaan tersebut harus melepaskan diri dari semua perusahaan telepon lokal, dan harus mengizinkan penyedia telepon jarak jauh lainnya mengakses kantornya.

Pada saat itu, AT&T terdiri dari 23 Bell Operating Companies (BOCs), yang menyediakan layanan telepon lokal di seluruh negeri. Terdapat juga 14.000 perusahaan telepon lokal lainnya yang tidak dimiliki oleh AT&T, namun biasanya melayani wilayah yang sangat terbatas. Sebagai bagian dari divestasi, Dewan Komisaris dipisahkan dari AT&T dan,

agar mereka dapat bertahan, direorganisasi menjadi tujuh Regional Bell Operating Companies (RBOCs), seperti yang ditunjukkan pada Gambar 11-2. Ketujuh RBOC ini kemudian bersaing dengan 14.000 lebih perusahaan telepon lokal lainnya untuk menyediakan layanan lokal ke setiap rumah dan bisnis di negara tersebut. Akibat persaingan dan besarnya kekuasaan serta besarnya tujuh RBOC, jumlah perusahaan telepon lokal telah menurun drastis selama bertahun-tahun. Merger juga berdampak buruk pada industri ini; dan pada musim panas 2011, tiga RBOC besar tetap ada: AT&T (sebelumnya Southwestern Bell, BellSouth, dan Ameritech), CenturyLink (sebelumnya Qwest, yang sebelumnya merupakan US West), dan Verizon (sebelumnya Bell Atlantic). (Secara teknis, Verizon memisahkan beberapa segmen yang lebih kecil menjadi RBOC terpisah di bagian utara New England dan West Virginia.)



Gambar 11-2 23 perusahaan Bell yang asli dan tujuh perusahaan telepon regional yang lebih baru (per 1985)

Sejumlah hasil lain dari divestasi tahun 1984 benar-benar mengubah lanskap sistem telepon AS. Pertama, Amerika Serikat terbagi menjadi wilayah transportasi akses lokal yang baru saja kita pelajari. LATA ini menentukan kapan panggilan telepon bersifat lokal atau jarak jauh. Perpecahan ini juga memungkinkan perusahaan telepon jarak jauh selain Bell Telephone, seperti MCI dan Sprint, untuk menawarkan layanan jarak jauh yang bersaing. Untuk mendukung persaingan di antara penyedia layanan sambungan jarak jauh, perusahaan telepon lokal diharuskan memberikan akses yang sama kepada semua perusahaan telepon jarak jauh terhadap saluran telepon yang terhubung ke setiap rumah dan tempat bisnis. Selain itu, orang dapat membeli telepon mereka sendiri. Sebelumnya, seseorang hanya dapat menyewa telepon dari perusahaan telepon. Terakhir, perusahaan telepon lokal dikenal sebagai local exchange operator (LECs), dan perusahaan telepon jarak jauh dikenal sebagai interexchange operator (IECs atau IXC).

Operator pertukaran lokal menawarkan sejumlah layanan, termasuk Centrex, private dan tie line, dan banyak layanan telekomunikasi lainnya seperti panggilan tunggu dan panggilan konferensi. Centrex (layanan pertukaran kantor pusat) adalah layanan dari perusahaan telepon lokal di mana fasilitas telepon terkini di kantor pusat (lokal) perusahaan telepon ditawarkan kepada pengguna bisnis, sehingga mereka tidak perlu membeli fasilitas sendiri. . Bisnis terhindar dari biaya untuk mengikuti perubahan teknologi yang bergerak cepat karena perusahaan telepon menyediakan perangkat keras dan layanan, dan bisnis hanya membayar biaya bulanan. Jika suatu perusahaan tidak ingin menyewa layanan Centrex dari perusahaan telepon lokal, maka perusahaan tersebut dapat membeli bursa cabang swasta miliknya sendiri, yang merupakan pesaing utama Centrex. Private Branch Exchange (PBX) adalah sistem telepon mandiri yang besar, terkomputerisasi, dan berada di ruang telepon di lokasi perusahaan. Sebuah PBX menangani semua panggilan internal dan melakukan panggilan ke saluran telepon luar. Sebuah PBX juga dapat menawarkan banyak layanan telepon seperti pesan suara, penerusan panggilan, dan rencana panggilan yang menggunakan sirkuit telepon lokal dan jarak jauh yang paling murah.

Saluran pribadi dan saluran penghubung adalah saluran telepon sewaan yang tidak memerlukan panggilan. Mereka adalah hubungan langsung permanen antara dua titik tertentu. Bayangkan sebuah perusahaan yang memiliki dua kantor di kota yang sama yang selalu mentransfer data bolak-balik. Untuk menghubungkan kantor-kantor tersebut, perusahaan dapat menggunakan saluran telepon dial-up dengan dua modem; namun karena banyak perusahaan telepon mengenakan biaya untuk semua panggilan yang dilakukan, saluran dial-up akan sangat mahal. Jalur sewaan mungkin menawarkan alternatif yang lebih murah, dan akan selalu terhubung—yang berarti karyawan di satu kantor tidak perlu menghubungi nomor telepon untuk menghubungi karyawan di kantor lain.

Operator pertukaran, atau perusahaan telepon jarak jauh, juga dapat menawarkan sejumlah besar layanan, termasuk panggilan kartu kredit dan kartu telepon; akses 700, 800, 888, dan 900; akses internasional; dan bantuan operator dan direktori.

Jaringan telepon setelah tahun 1996

Peristiwa besar kedua dalam sejarah industri telekomunikasi baru-baru ini terjadi pada tahun 1996, dengan disahkannya Undang-Undang Telekomunikasi tahun 1996. Undang-undang Telekomunikasi tahun 1996 yang disahkan oleh Kongres dan dikelola oleh Komisi Komunikasi Federal (FCC) membuka jalan bagi perkembangan industri telekomunikasi. bagi siapa saja untuk menawarkan layanan telepon lokal ke rumah dan bisnis. Penyedia baru layanan telepon lokal disebut operator pertukaran lokal kompetitif (CLECs), dan mereka dapat mencakup operator interexchange (perusahaan telepon jarak jauh), operator televisi kabel, perusahaan kecil yang hampir tidak memiliki peralatan (disebut CLEC berbasis non-fasilitas).

Alasan di balik pengembangan CLEC cukup jelas dan dimaksudkan untuk lebih mengakomodasi cara penyampaian layanan telepon. Misalnya, di beberapa wilayah di negara ini, perusahaan televisi kabel lokal telah menawarkan layanan telepon lokal. Karena sebagian besar rumah dan bisnis di Amerika Serikat sudah terhubung dengan televisi kabel, mengizinkan perusahaan kabel untuk menawarkan layanan telepon lokal melalui saluran TV

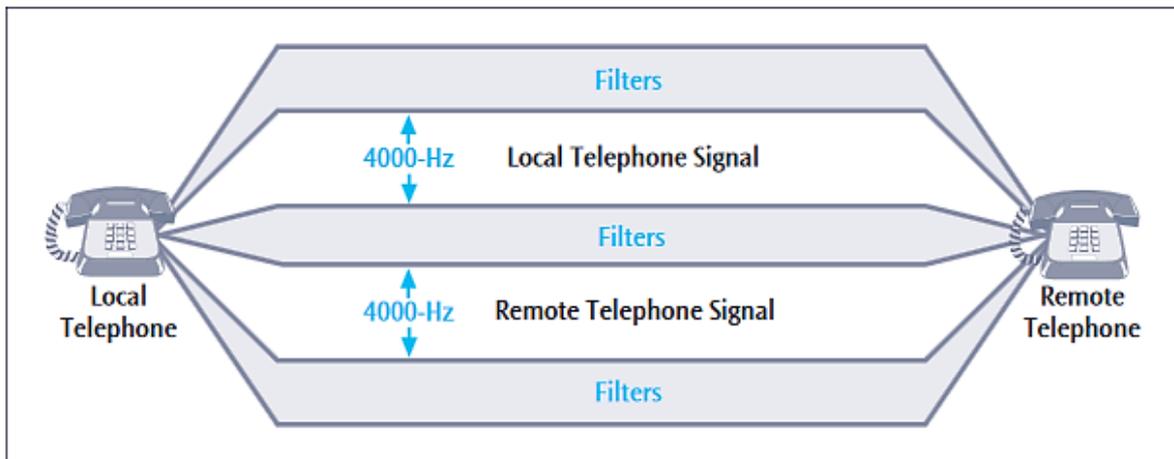
kabel yang sama sepertinya merupakan ide yang masuk akal. Disebut telepon kabel atau telepon kabel, layanan telepon melalui saluran televisi kabel kini ditawarkan oleh sebagian besar perusahaan televisi kabel besar—termasuk Cox Communications dan Comcast, serta banyak perusahaan kabel kecil—di sebagian besar kota besar di seluruh negeri. Laporan National Cable & Telecommunications Association melaporkan bahwa jumlah pelanggan telepon kabel pada Maret 2011 adalah sekitar 24,4 juta. Media yang menyalurkan telepon kabel adalah gabungan kabel fiber dan koaksial yang disebut Hybrid Fiber Coax (HFC). Teknologi ini juga dapat menghadirkan layanan modem kabel ke rumah dan bisnis.

Sayangnya, ada masalah dalam mengizinkan semua penyedia telepon lokal baru ini masuk ke suatu pasar: saluran telepon. Sangat mahal bagi penyedia telepon baru untuk memasang saluran telepon baru di setiap rumah dan bisnis. Perusahaan TV kabel mempunyai keuntungan dalam menggunakan jalur kabel yang sudah terhubung ke rumah pelanggannya, dan perusahaan listrik dapat menggunakan kabel yang menyalurkan layanan listrik, namun perusahaan lain yang mencoba masuk ke pasar telepon lokal tidak mendapatkan keuntungan ini. Untuk mengimbangi tingginya biaya pemasangan ini, Undang-Undang Telekomunikasi tahun 1996 mengamanatkan bahwa perusahaan telepon lokal yang ada, yang sekarang disebut operator pertukaran lokal (ILECs), harus memberikan akses kepada CLEC ke saluran telepon mereka. Selain itu, ILEC harus memberikan pesaing akses terhadap nomor telepon, layanan operator, dan daftar direktori; akses terhadap tiang, saluran, dan jalan raya; dan lokasi fisik peralatan di dalam gedung ILEC—dan mereka harus memberikan layanan ini dengan harga grosir.

Tentu saja, ILEC tidak senang dengan pengaturan ini dan telah menolak penerapannya selama beberapa waktu. Selama beberapa tahun terakhir, FCC telah membuat beberapa perubahan pada Undang-Undang Telekomunikasi tahun 1996 yang mengubah persyaratan ini, memaksa CLEC untuk membayar lebih atau bahkan harga penuh untuk akses ke jalur lokal. Hilangnya harga grosir dan berlanjutnya perlawanan terhadap ILEC telah menyebabkan sebagian besar CLEC yang bergantung pada saluran telepon dan peralatan ILEC meninggalkan layanan mereka. Banyak CLEC yang menawarkan layanan DSL telah menyerah dan menutup tokonya, sehingga ILEC dan perusahaan telepon kabel terus mempunyai pangsa pasar DSL yang lebih besar. Kesimpulannya, kita melihat bahwa Perubahan Keputusan Akhir tahun 1984 membuka pasar telepon jarak jauh terhadap persaingan, sedangkan Undang-Undang Telekomunikasi tahun 1996 dimaksudkan untuk membuka pasar telepon jarak jauh lokal terhadap persaingan.

Keterbatasan sinyal telepon

Sistem telepon pada awalnya dirancang untuk mengirimkan suara manusia. Seperti yang kita lihat di Bab Dua, rata-rata suara manusia memiliki rentang frekuensi sekitar 300 hingga 3400 Hz (bandwidth 3100 Hz). Dengan demikian, jaringan telepon direkayasa untuk mengirimkan sinyal sekitar 3100 Hz. Dalam praktiknya, sistem telepon sebenarnya mengalokasikan 4000 Hz ke suatu saluran, dan menggunakan filter untuk menghilangkan frekuensi yang berada di atas dan di bawah setiap saluran 4000 Hz. Saluran dan frekuensinya digambarkan pada Gambar 11-3.



Gambar 11-3 Dua saluran telepon dan penetapan frekuensinya

Saluran 4000 Hz untuk suara secara signifikan lebih kecil dibandingkan saluran 20.000 Hz yang diperlukan untuk musik berkualitas CD. Oleh karena itu, agar sistem telepon mampu mentransmisikan musik berkualitas CD, setiap salurannya perlu dimodifikasi untuk mendukung sinyal 20.000 Hz. Semua pembicaraan tentang frekuensi dan transmisi suara mengarah pada dua poin penting:

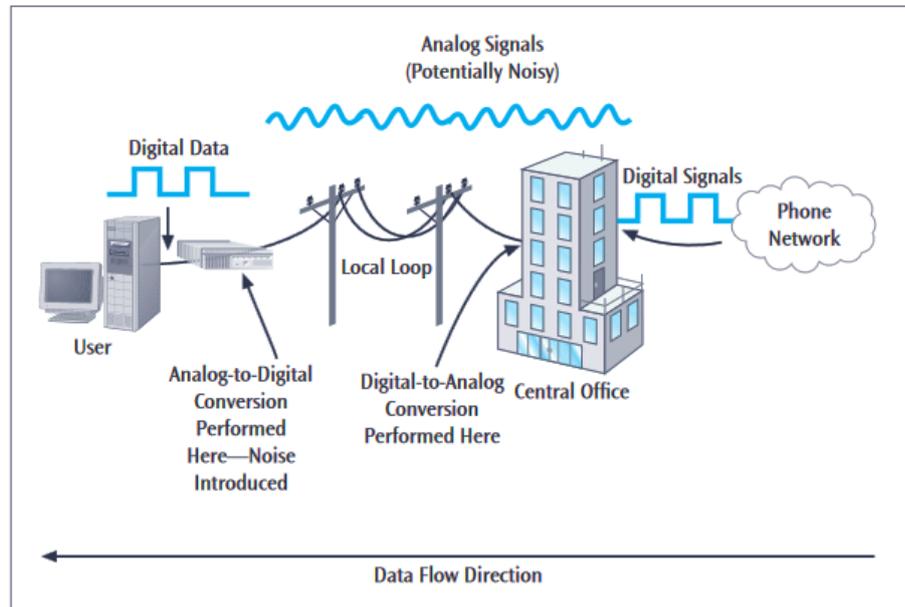
- Semakin banyak informasi yang ingin Anda kirimkan melalui suatu media, semakin tinggi frekuensi sinyal yang Anda perlukan untuk mewakili informasi tersebut. (Lihat Bab Dua untuk pembahasan rinci mengenai hal ini.)
- Jika Anda ingin mengirim data melalui saluran telepon, data tersebut harus dapat dikirimkan dalam satu atau lebih saluran 4000-Hz.

Ketika Anda menggabungkan kedua pernyataan ini, sebuah fakta yang menyakitkan tentang penggunaan jalur komunikasi suara untuk transmisi data muncul: Setiap transmisi data yang dilakukan melalui saluran telepon standar harus sesuai dengan satu atau lebih pita sempit 4000 Hz, yang berarti transmisi data tarif juga akan dibatasi. Ingat rumus Shannon dari Bab Dua, yang menunjukkan bahwa frekuensi, tingkat kebisingan, dan tingkat daya sinyal analog menentukan kecepatan maksimum transmisi data. Dengan teknik modulasi tingkat lanjut seperti multinada diskrit (digunakan dalam DSL) dan multiplexing pembagian frekuensi ortogonal (digunakan dalam televisi digital), dimungkinkan untuk membuat ratusan saluran pada dua pasangan terpilin. Dimungkinkan juga untuk meningkatkan kecepatan transmisi data pada saluran telepon dial-up hingga 56.000 bps teoritis melalui sepasang saluran 4000 Hz, namun kecepatan ini hanya dapat dicapai dalam kondisi ideal. Sebelum kita beralih ke topik lebih lanjut, mari kita lihat lebih dekat bentuk layanan Internet dial-up ini.

Layanan Internet dial-up

Dahulu kala, sebagian besar pengguna komputer mengakses Internet melalui layanan Internet dial-up. Saat ini, diperkirakan kurang dari 10 persen pengguna Internet mengakses Internet melalui dial-up. Modem DSL dan kabel (layanan broadband) pada dasarnya telah mengambil alih pasar dial-up. Layanan dial-up masih dapat ditemukan di daerah pedesaan

yang tidak memiliki DSL atau modem kabel, dan masih populer di kalangan pengguna dengan anggaran terbatas.



Gambar 11-4 Bentuk sambungan telepon analog dan digital antara rumah dan kantor pusat

Modem dial-up tercepat saat ini adalah modem 56k. 56k berarti kecepatan transfer data 56.000 bit per detik; meskipun seperti yang akan segera kita lihat, angka tersebut hampir selalu tidak dapat dicapai. Modem 56k adalah desain hybrid, menggabungkan sinyal analog dan sinyal digital. Koneksi upstream dari modem ke remote end masih menggunakan teknik pensinyalan dan modulasi analog konvensional, sehingga dibatasi pada kecepatan transmisi maksimum 33.600 bps. Namun, jalur hilir menggunakan sinyal digital. Sistem telepon sebenarnya telah menggunakan sinyal digital (untuk mengingatkan cara kerjanya, lihat bagian Bab Dua tentang modulasi kode pulsa) melalui saluran telepon selama bertahun-tahun. Faktanya, sistem telepon dapat mengirimkan sampel 8-bit 8000 kali per detik, yang setara dengan 64.000 bit per detik, atau 64 kbps. Jika perusahaan telepon dapat mengirimkan 64-kbps, apakah ini berarti kita sebagai pengguna dapat menerima sinyal downstream 64-kbps? Sayangnya, jawabannya adalah "Tidak." Ketika perusahaan telepon mengirimkan sinyal telepon digital 64-kbps, sinyal tersebut ditransmisikan secara digital dari satu pusat switching ke pusat switching lainnya. Namun ketika sinyal telepon ditransmisikan ke rumah dan usaha kecil kita, sinyal tersebut harus disesuaikan agar dapat melintasi loop lokal. Loop lokal, seperti yang ditunjukkan pada Gambar 11-1 dan 11-4, adalah bentangan kabel telepon yang menghubungkan rumah (atau usaha kecil) dan kantor pusat perusahaan telepon, dan menggunakan sinyal analog.

Sebelum sinyal telepon ditransmisikan melalui loop lokal, kantor pusat mengubah sinyal digital menjadi sinyal analog (Gambar 11-4). Ketika sinyal analog memasuki rumah Anda, modem 56k komputer Anda mengubah sinyal analog kembali menjadi data digital

karena komputer memanipulasi data digital. Seperti yang mungkin Anda ingat dari Bab Dua, ketika sinyal analog diubah menjadi data digital, kuantisasi noise diperkenalkan. Adanya noise inilah yang menjadi alasan mengapa modem ini tidak disebut sebagai modem 64k melainkan modem 56k. Ternyata tidak mungkin mencapai 56 kbps. Karena gangguan pada kabel tembaga loop lokal, sinyal harus melambat hingga kecepatan data lebih rendah lagi.

Standar pertama yang mendukung modem dial-up 56k adalah standar V.90. Tak lama setelah V.90 diperkenalkan, ITU memperkenalkan standar modem V.92. Standar ini merupakan sedikit peningkatan dibandingkan standar V.90 dalam dua hal. Pertama, link upstream antara pengguna dan perusahaan telepon mampu mendukung koneksi hingga 48 kbps (dibandingkan dengan 33,600 bps pada modem V.90). Tentu saja, tingkat ini hanya mungkin terjadi pada kondisi ideal dengan tingkat kebisingan yang rendah pada saluran telepon. Peningkatan kedua adalah modem V.92 dapat menahan koneksi data jika seseorang menghubungi nomor telepon pengguna (panggilan tunggu). Pengguna kemudian dapat mengangkat telepon dan berbicara saat koneksi data masih aktif namun tertahan. Ketika pengguna mengakhiri panggilan telepon standar, koneksi data dilanjutkan.

Terlepas dari kelebihan yang ditawarkan modem V.90 dan V.92 dibandingkan modem lama 33.600-bps, banyak orang menganggap kecepatan 56-kbps terlalu lambat. Secara khusus, banyak pengguna merasa kecepatan ini terasa lambat saat mengunduh dokumen berukuran besar atau dokumen berisi gambar. Yang kita butuhkan adalah cara alternatif untuk mengirim data melalui sistem telepon dasar. Pada bagian berikut, kita akan memeriksa beberapa alternatif ini.

11.3 SALURAN PELANGGAN DIGITAL

Saluran pelanggan digital (DSL) adalah teknologi yang memungkinkan saluran telepon twisted pair yang ada untuk mengirimkan materi multimedia dan data berkecepatan tinggi. Kecepatan transfer dapat berkisar dari ratusan ribu bit per detik hingga beberapa juta bit per detik. Meskipun beberapa perusahaan telepon lokal yang lebih besar pada awalnya ragu-ragu untuk menawarkan layanan DSL, perusahaan-perusahaan telepon baru (CLEC) sangat bersemangat untuk melakukannya. Tidak lama setelah CLEC mulai menarik pelanggan DSL, perusahaan telepon lokal mulai mengubah rencana mereka; dan sekarang sebagian besar, jika tidak semua, perusahaan telepon menawarkan berbagai tingkat layanan DSL.

Dasar-dasar DSL

Seperti halnya teknologi apa pun yang dapat mengirimkan data multimedia, kecepatan transmisi merupakan isu penting. DSL mampu mencapai berbagai kecepatan. Kecepatan transfer saluran tertentu bergantung pada satu atau lebih faktor berikut: operator yang menyediakan layanan, jarak rumah atau bisnis Anda dari kantor pusat perusahaan telepon lokal, dan apakah layanan DSL bersifat simetris. koneksi atau koneksi asimetris. Faktor pertama, operator, menentukan bentuk tertentu dari teknologi DSL dan format transmisi pendukung, yang dipilih oleh masing-masing operator secara individual. Bentuk DSL dan teknologi yang mendasarinya menentukan kecepatan layanan.

Pengaruh faktor kedua, jarak, terhadap kecepatan transfer suatu saluran relatif mudah: Semakin dekat rumah atau bisnis Anda ke kantor pusat, semakin cepat kemungkinan kecepatan transmisinya. Ketergantungan pada jarak ini disebabkan oleh fakta bahwa twisted pair berbahan dasar tembaga cukup rentan terhadap noise, yang secara signifikan dapat mempengaruhi sinyal transmisi DSL. Semakin panjang kabel tanpa repeater, semakin banyak noise pada saluran, dan semakin lambat kecepatan transmisi. Jarak maksimum sebuah rumah atau bisnis dari kantor pusat tanpa repeater adalah sekitar 5,5 km (3 mil).

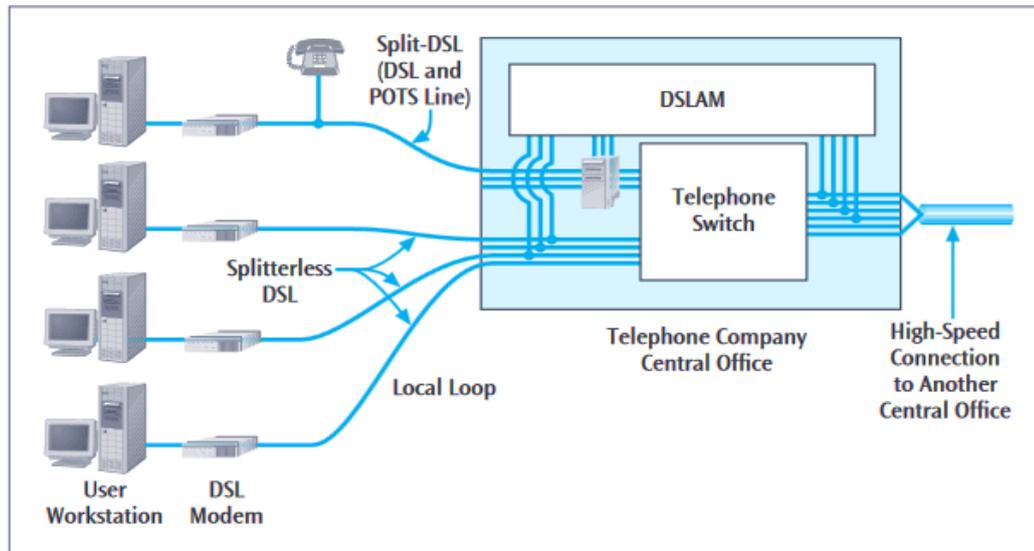
Faktor ketiga yang mempengaruhi kecepatan transfer adalah jenis sambungan: simetris atau asimetris. Sambungan simetris adalah sambungan yang kecepatan perpindahannya pada kedua arah adalah sama. Koneksi asimetris memiliki kecepatan transmisi downstream yang lebih cepat dibandingkan kecepatan upstreamnya. Misalnya, layanan DSL asimetris dapat memberikan kecepatan unduh hingga ratusan ribu bit per detik, sedangkan kecepatan unggah mungkin kurang dari 100.000 bps (100 kbps). Layanan asimetris berguna untuk koneksi Internet di mana sebagian besar lalu lintas (dalam bentuk halaman Web) turun dari Internet ke workstation. Seringkali satu-satunya data yang masuk ke Internet adalah permintaan untuk halaman Web lain, beberapa pesan email yang relatif kecil, atau permintaan FTP untuk mendownload file. Sebagian besar layanan DSL residensial bersifat asimetris. (Meskipun beberapa penyedia DSL mulai mengenakan biaya berdasarkan jumlah data yang diunduh per bulan.)

Karakteristik lain dari DSL adalah koneksinya yang selalu aktif. Pengguna tidak perlu melakukan panggilan dan membuat sambungan. Dengan demikian, stasiun kerja di rumah atau bisnis dapat memiliki koneksi 24 jam sehari ke Internet, atau layanan telekomunikasi lainnya. Selain itu, sambungan ini dikenakan tarif tetap, biasanya bulanan. Pengguna tidak membayar biaya berdasarkan jarak koneksi dan berapa lama koneksi dibuat. (Meskipun beberapa penyedia DSL mulai mengenakan biaya berdasarkan jumlah data yang diunduh per bulan.)

Karena DSL merupakan koneksi yang selalu aktif, DSL menggunakan sirkuit permanen dan bukan sirkuit yang diaktifkan. Sirkuit permanen ini tidak dapat dikonfigurasi secara dinamis, namun harus dibuat oleh penyedia layanan DSL. Karena sebagian besar pengguna DSL rumahan dan bisnis saat ini menggunakan layanan ini untuk menyambungkan komputer mereka ke penyedia layanan Internet, tidak adanya sambungan dinamis bukanlah masalah serius. Namun jika pengguna ingin memindahkan koneksi DSL ke penyedia layanan Internet lain, layanan DSL baru mungkin harus dikontrak.

Apa yang dibutuhkan oleh pengguna bisnis atau rumahan untuk membuat koneksi DSL? Saat ini diperlukan empat komponen. Perusahaan telepon lokal (LEC) harus memasang router khusus yang disebut DSLAM (DSL Access Multiplexer) di kantor pusat perusahaan telepon tersebut. Perangkat ini melewati peralatan switching kantor pusat, dan membuat serta menerjemahkan sinyal DSL yang ditransfer pada loop lokal telepon (Gambar 11-5). Selanjutnya, perusahaan telepon lokal juga dapat memasang pembagi DSL di lokasinya, yang menggabungkan atau memisahkan sirkuit DSL (saluran hulu dan hilir) dengan sirkuit telepon standar POTS. Beberapa sistem DSL mengirimkan melalui saluran telepon yang sama yang

berjalan dari kantor pusat ke rumah atau bisnis. Karena merupakan saluran telepon yang sama, DSL harus berbagi saluran dengan sinyal POTS.



Gambar 11-5 Empat komponen penting koneksi DSL

Jika DSL berbentuk tertentu, seperti DSL Lite (akan dijelaskan secara singkat), maka saluran DSL tidak membawa sirkuit telepon standar. Dengan demikian, tidak perlu memisahkan sinyal DSL dari sinyal telepon baik di sisi pengirim maupun penerima. Jika tidak ada splitter yang digunakan untuk memisahkan sinyal DSL dari sinyal POTS, maka layanan ini disebut DSL splitterless.

Di sisi pengguna, modem DSL diperlukan untuk mengubah sinyal DSL menjadi bentuk yang dapat dipahami oleh stasiun kerja atau jaringan pengguna. Jika rangkaian DSL juga membawa rangkaian telepon POTS, pengguna juga memerlukan splitter untuk memisahkan saluran telepon biasa dari saluran data DSL.

Terakhir, router DSLAM di kantor pusat perusahaan telepon harus terhubung ke penyedia layanan Internet melalui saluran berkecepatan tinggi. Karena jalur berkecepatan tinggi ini akan mendukung permintaan layanan Internet dari banyak pengguna, jalur tersebut memerlukan layanan yang sangat cepat, seperti ATM.

Mari kita pertimbangkan perusahaan telepon dan jenis layanan DSL yang disediakan. Kebanyakan penyedia DSL menawarkan sejumlah jenis layanan berbeda. Layanan pertama, dirancang untuk pengguna rumahan, biasanya menyediakan kecepatan downstream sekitar 700 kbps dan kecepatan upstream 100 kbps dengan biaya sekitar \$25,00 per bulan. Untuk pengguna rumahan yang membutuhkan kecepatan lebih, layanan kedua biasanya menyediakan kecepatan hilir 1,5 hingga 3,0 Mbps dengan biaya sekitar \$50,00 per bulan. Untuk bisnis, yang biasanya membutuhkan kapasitas lebih besar, tersedia layanan DSL yang dapat mengunggah dan mengunduh data dengan kecepatan beberapa juta bit per detik; ini biayanya ratusan dolar per bulan. Kecepatan dan harga yang disebutkan di sini hanyalah contoh kecil dari kecepatan dan harga yang mungkin terjadi di Amerika Serikat.

Format DSL

Jika DSL berbentuk tertentu, seperti DSL Lite (akan dijelaskan secara singkat), maka saluran DSL tidak membawa sirkuit telepon standar. Dengan demikian, tidak perlu memisahkan sinyal DSL dari sinyal telepon baik di sisi pengirim maupun penerima. Jika tidak ada splitter yang digunakan untuk memisahkan sinyal DSL dari sinyal POTS, maka layanan ini disebut DSL splitterless.

Di sisi pengguna, modem DSL diperlukan untuk mengubah sinyal DSL menjadi bentuk yang dapat dipahami oleh stasiun kerja atau jaringan pengguna. Jika rangkaian DSL juga membawa rangkaian telepon POTS, pengguna juga memerlukan splitter untuk memisahkan saluran telepon biasa dari saluran data DSL.

Terakhir, router DSLAM di kantor pusat perusahaan telepon harus terhubung ke penyedia layanan Internet melalui saluran berkecepatan tinggi. Karena jalur berkecepatan tinggi ini akan mendukung permintaan layanan Internet dari banyak pengguna, jalur tersebut memerlukan layanan yang sangat cepat, seperti ATM.

Mari kita pertimbangkan perusahaan telepon dan jenis layanan DSL yang disediakan. Kebanyakan penyedia DSL menawarkan sejumlah jenis layanan berbeda. Layanan pertama, dirancang untuk pengguna rumahan, biasanya menyediakan kecepatan downstream sekitar 700 kbps dan kecepatan upstream 100 kbps dengan biaya sekitar Rp. 2.500.000 per bulan. Untuk pengguna rumahan yang membutuhkan kecepatan lebih, layanan kedua biasanya menyediakan kecepatan hilir 1,5 hingga 3,0 Mbps dengan biaya sekitar Rp. 5.000.000 per bulan. Untuk bisnis, yang biasanya membutuhkan kapasitas lebih besar, tersedia layanan DSL yang dapat mengunggah dan mengunduh data dengan kecepatan beberapa juta bit per detik; ini biayanya ratusan dolar per bulan. Kecepatan dan harga yang disebutkan di sini hanyalah contoh kecil dari kecepatan dan harga yang mungkin terjadi di Amerika Serikat.

Saluran pelanggan digital hadir dalam berbagai format. Meskipun variasi ini memberikan operator dan pengguna beragam pilihan teknologi dan kecepatan, variasi ini juga dapat membagi pengguna menjadi beberapa kelompok, sehingga membuat proses penetapan satu format sebagai standar agak sulit. Sejumlah format ini, tidak diragukan lagi, akan hilang seiring berjalannya waktu, namun tidak ada cara untuk mengetahui berapa lama waktu yang dibutuhkan. Untuk saat ini, pengguna jaringan bisnis yang terinformasi harus mengetahui berbagai format. (Harap dicatat bahwa kecepatan transmisi data yang disediakan akan sering berubah seiring berkembangnya teknologi.) Sering secara kolektif disebut sebagai xDSL, ada empat format DSL yang digunakan saat ini:

- Jalur pelanggan digital asimetris (ADSL)—Format populer yang mentransmisikan data hilir dengan kecepatan lebih cepat dibandingkan kecepatan hulu. Kecepatan data hilir umumnya berkisar antara 600 kbps hingga 1500 kbps, sedangkan kecepatan data hulu berkisar antara 300 kbps hingga 600 kbps.
- DSL Lite—Format yang lebih lambat dibandingkan ADSL; juga dikenal sebagai DSL Universal, G.Lite, dan DSL tanpa splitter. Kecepatan transmisi tipikal berada pada kisaran 200 kbps.

- Kecepatan data sangat tinggi DSL2 (VDSL2)—Format yang sangat cepat (kira-kira 100-Mbps downstream dan upstream) pada jarak yang sangat pendek (kurang dari 300 meter).
- Rate-adaptive DSL (RADSL)—Sebuah format yang kecepatan transfernya dapat bervariasi tergantung pada tingkat kebisingan dalam loop lokal saluran telepon.

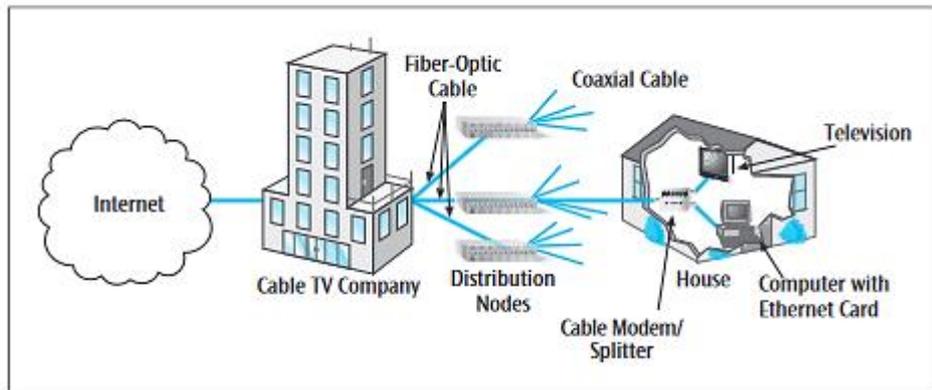
DSL bukan satu-satunya cara pengguna rumahan atau bisnis kecil dapat mengontrak layanan pengiriman data untuk menghubungkan komputernya ke Internet. Mari kita periksa teknologi kedua yang sangat populer: modem kabel.

11.4 MODEM KABEL

Modem kabel adalah layanan komunikasi berkecepatan tinggi yang memungkinkan akses berkecepatan tinggi ke jaringan area luas seperti Internet melalui koneksi televisi kabel. Secara teknis, modem kabel adalah perangkat fisik yang memisahkan data komputer dari sinyal video televisi kabel, namun banyak orang merujuk pada keseluruhan sistem (kabel serat optik, node distribusi lingkungan, kabel koaksial, pembagi modem kabel, dan kartu antarmuka). sebagai layanan modem kabel. Koneksi komponen ini ditunjukkan pada Gambar 11-6.

Kebanyakan modem kabel adalah perangkat eksternal yang terhubung ke komputer pribadi melalui kartu antarmuka jaringan Ethernet umum, yang disediakan oleh perusahaan kabel atau dibeli di sebagian besar toko yang menjual peralatan komputer. Dengan demikian, koneksi ini mampu mentransmisikan data berukuran megabit, dengan kecepatan transmisi berkisar antara 300 kbps hingga beberapa Mbps. Koneksi ini, mirip dengan DSL, biasanya asimetris.

Modem kabel menyediakan koneksi berkecepatan tinggi ke Internet dan permintaan terhadapnya berkembang pesat. Pertumbuhan ini tidak terjadi tanpa adanya kesulitan dalam perusahaan kabel. Seperti sistem telepon, sistem kabel mempunyai semacam loop lokal—yaitu, kabel yang berjalan dari titik distribusi lingkungan ke rumah atau bisnis. Untuk mendukung bandwidth yang sangat tinggi yang diperlukan untuk menyediakan akses Internet berkecepatan tinggi ke banyak pengguna, perusahaan kabel harus mengganti sebagian besar kabel loop lokal mereka yang ada, yang sebagian besar bersifat koaksial, dengan kabel serat optik. Pada titik tertentu, perusahaan kabel (dan juga perusahaan telepon) dapat mengganti kabel tembaga mereka dengan kabel serat optik juga. Faktanya, semakin banyak komunitas di seluruh negeri yang mulai merasakan manfaat dari teknologi baru ini.



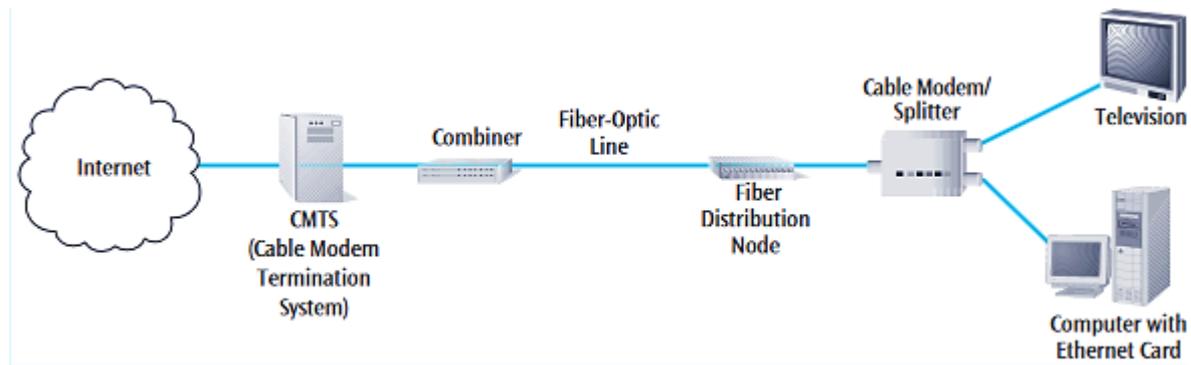
Gambar 11-6 Modem kabel yang menghubungkan komputer pribadi ke Internet melalui sambungan televisi kabel

Kelemahan modem kabel—sangat mungkin satu-satunya kelemahannya—terkait dengan tren berikut: Ketika lalu lintas pada jaringan area lokal berbasis Ethernet meningkat, terjadi penurunan throughput secara keseluruhan—kemampuan untuk mengirim atau menerima pesan lengkap. Dengan demikian, semakin banyak pelanggan dalam wilayah geografis lokal, seperti sejumlah kecil blok lingkungan, yang berlangganan layanan modem kabel, lalu lintas akan meningkat ke titik di mana throughput mungkin menurun.

Pengoperasian Modem Kabel

Perusahaan kabel yang menawarkan layanan modem kabel menggunakan standar yang disebut Spesifikasi Antarmuka Layanan Data Over Cable (DOCSIS). DOCSIS (sekarang DOCSIS versi 3.0) dirancang untuk mencakup semua elemen operasional yang digunakan dalam memberikan layanan data melalui sistem televisi kabel, termasuk penyediaan layanan, keamanan, antarmuka data, dan antarmuka frekuensi radio. Arsitektur dasar sistem modem kabel ditunjukkan pada Gambar 11-7.

Sistem ini terdiri dari enam komponen utama. Komponen pertama, Cable Modem Termination System (CMTS), terletak di fasilitas utama operator kabel dan menerjemahkan paket data halaman Web yang masuk ke frekuensi radio. Frekuensi yang digunakan untuk transfer paket data halaman Web adalah frekuensi yang tidak terpakai dalam rentang 6 MHz. Komponen kedua dari sistem modem kabel adalah penggabung, yang menggabungkan frekuensi paket data halaman Web dengan frekuensi saluran televisi kabel umum. Sinyal-sinyal ini kemudian dikirim melalui jalur serat optik, yang merupakan komponen ketiga dalam sistem, ke simpul distribusi serat, komponen keempat dalam sistem. Node distribusi fiber berada di lingkungan pengguna dan dapat mendistribusikan sinyal ke 500–2000 rumah. Dari node distribusi serat, kabel koaksial membawa sinyal ke rumah-rumah di mana splitter, komponen kelima, memisahkan frekuensi paket data halaman Web dari frekuensi saluran kabel lainnya. Frekuensi saluran kabel lainnya menuju ke pesawat televisi, dan frekuensi paket data halaman Web yang telah dipisahkan menuju ke modem kabel. Modem kabel (komponen keenam dari sistem) mengubah sinyal radio kembali menjadi paket data digital untuk dikirimkan ke komputer Anda.



Gambar 11-7 Arsitektur dasar dan komponen sistem modem kabel

11.5 T-1 LAYANAN LEASED LINE

Sejak tahun 1960an dan 1970an, dunia usaha memerlukan koneksi berkecepatan tinggi antara mereka dan perusahaan telepon, atau antara mereka dan gedung perusahaan lain. Saluran telepon dial-up tidak cukup cepat, dan menghubungi pihak yang dihubungi setiap kali sambungan diperlukan sangatlah merepotkan. Modem DSL dan kabel bisa menjadi solusi yang baik dalam banyak kasus, namun keduanya belum ditemukan. Sebaliknya, perusahaan telepon mulai menawarkan layanan jalur sewaan. Jalur sewaan ini hadir dengan berbagai kecepatan transfer data (dari 56.000 bps hingga 64 Mbps) dan merupakan sirkuit tetap—sirkuit (atau koneksi) dipasang secara permanen di antara dua lokasi. Perusahaan tidak perlu menghubungi nomor telepon karena sirkuit selalu aktif. Perusahaan telepon membebaskan biaya pemasangan dan kemudian biaya sewa bulanan kepada bisnis tersebut. Banyak perusahaan menggunakan saluran sewaan ini untuk memelihara koneksi data yang konstan antara dua lokasi, atau mereka menggunakannya untuk menghubungkan sekelompok saluran telepon ke kantor pusat perusahaan telepon. Saat ini, jalur sewaan seperti ini telah menurun popularitasnya.

Salah satu bentuk layanan sewa jalur yang sangat populer dan masih eksis hingga saat ini adalah T-1. Layanan T-1, seperti yang mungkin Anda ingat dari bab sebelumnya, adalah koneksi serba digital yang dapat mentransfer suara atau data dengan kecepatan hingga 1,544 Mbps (1,544,000 bit per detik). Tergantung pada keinginan pengguna, jalur T-1 dapat mendukung hingga 24 sirkuit telepon individual, 24 jalur data individual dengan kecepatan masing-masing 56.000 bit per detik, atau berbagai kombinasi opsi ini. Jika Anda tidak memerlukan 1,544 Mbps untuk mengirimkan data komputer, Anda dapat meminta seperempat-T-1 atau setengah-T-1, yang sesuai dengan namanya, menyediakan seperempat setengah dari 1,544-Mbps kecepatan data, masing-masing. Jalur seperempat T-1 dan setengah T-1 ini disebut layanan fraksional T-1; mereka tidak ditawarkan oleh semua perusahaan telepon. Di sisi lain, pelanggan yang membutuhkan kecepatan transmisi lebih tinggi dari 1,544 Mbps dapat mempertimbangkan beberapa T-1, atau layanan T-3, yang mentransmisikan data pada 45 Mbps. Sayangnya, perbedaan biaya, seperti perbedaan kecepatan, antara T-1 dan T-3 sangat dramatis.

Seperti semua layanan jalur sewaan, sambungan T-1 adalah layanan point-to-point dan selalu aktif. Jalur IntraLATA T-1 biasanya berharga sekitar Rp. 3.500.000 hingga Rp.

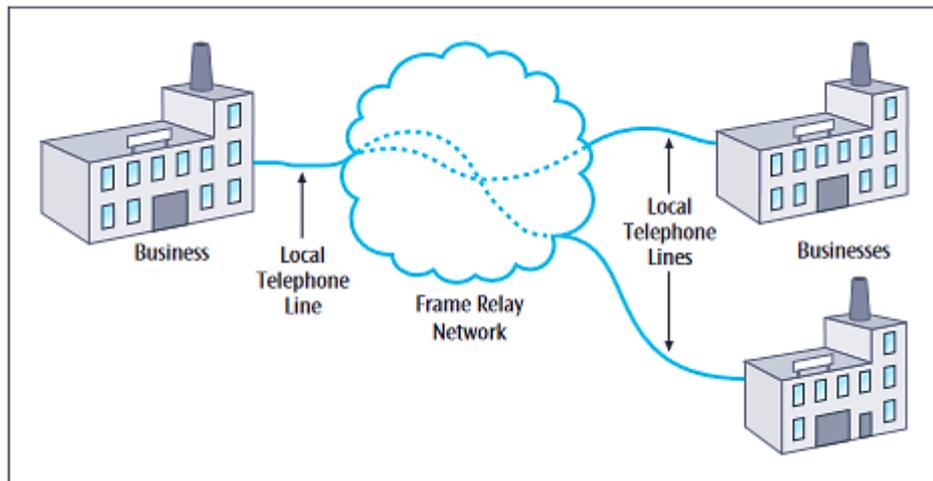
4.000.000 per bulan, sedangkan jalur interLATA T-1 berharga Rp. 1.200.000 per bulan ditambah Rp. 250.000 per mil untuk sambungannya.

Menariknya, layanan T-1, yang diciptakan pada tahun 1963, dirancang hanya untuk mendukung sirkuit telepon yang digunakan perusahaan telepon untuk mengirimkan data antar pusat switching. Ketika dunia usaha mendengar tentang jalur T-1, mereka mulai memintanya sebagai cara untuk menghubungkan kantor mereka ke pusat peralihan perusahaan telepon (kantor pusat). Permintaan terhadap jalur T-1 terus meningkat sejak saat itu. Namun baru-baru ini, jalur T-1 mulai menghadapi persaingan ketat dari layanan baru yang menawarkan kecepatan transmisi yang sama atau lebih cepat dengan label harga yang lebih murah. Kami akan memeriksa beberapa layanan alternatif ini selanjutnya dan melihat perbandingannya dengan T-1.

11.6 FRAME RELAY

Pertimbangkan skenario berikut: Sebuah perusahaan menginginkan koneksi yang cepat dan andal ke situs lain. Lokasi ini dapat berupa gedung lain dalam perusahaan yang sama yang terletak di lokasi yang jauh, atau dapat berupa perusahaan lain yang ingin berbisnis dengan perusahaan pertama. Perusahaan menginginkan koneksi ini untuk mengirimkan data, sehingga sistem yang dipilihnya harus dirancang untuk data dan bukan suara. Terkadang koneksi harus bersifat permanen, dan terkadang diperlukan koneksi sementara atau teralihkan. Terakhir, koneksi harus bersifat pribadi; datanya relatif sensitif dan perusahaan tidak ingin sembarang orang memanfaatkan koneksinya. Apa yang harus digunakan perusahaan ini? Saluran telepon dial-up? Tentu saja tidak. Saluran telepon dial-up tidak dirancang untuk data, tidak cepat, dan akan sangat mahal. Bagaimana dengan jalur T-1? T-1 mungkin berhasil; namun T-1 menjadi sangat mahal untuk jarak jauh dan 1,5 Mbps mungkin tidak cukup cepat. Modem DSL dan kabel tidak akan berfungsi karena biasanya dirancang untuk menghubungkan pengguna rumahan dan bisnis ke Internet. Lalu apa yang bisa digunakan perusahaan untuk menghubungkan kedua lokasinya? Mari kita lihat beberapa kemungkinan solusi untuk masalah ini.

Frame relay adalah jaringan packet-switched yang dirancang untuk mengirimkan data melalui saluran tetap (bukan saluran dial-up). Jika sebuah perusahaan tertarik untuk menyewa rangkaian frame relay, perusahaan tersebut akan menghubungi perusahaan telepon setempat atau penyedia layanan frame relay. Kebanyakan perusahaan telepon jarak jauh menawarkan layanan frame relay di sebagian besar negara. Layanan frame relay dapat berupa layanan lokal atau layanan jarak jauh. Setelah layanan ditetapkan, pelanggan hanya perlu mengirimkan datanya melalui link lokal ke stasiun frame relay terdekat, yang ditunjukkan pada Gambar 11-8 sebagai cloud. Jaringan frame relay kemudian bertanggung jawab untuk mentransmisikan data pengguna melalui jaringan dan mengirimkannya ke situs tujuan yang dituju.



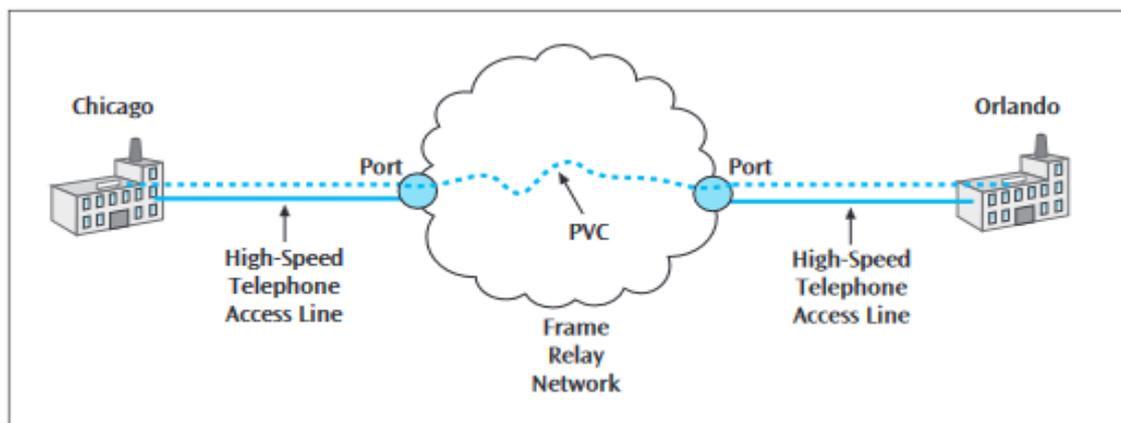
Gambar 11-8 Tiga bisnis terhubung ke frame relay cloud melalui koneksi lokal

Layanan frame relay memberikan banyak alternatif menarik untuk saluran sewaan. Salah satu karakteristik nyata pertama dari jaringan frame relay adalah kecepatan transfer yang sangat tinggi. Kecepatan transfer datanya bisa sangat cepat, hingga 45 Mbps. Seiring dengan kecepatan transfer data yang tinggi, terdapat pula throughput yang tinggi—jaringan secara keseluruhan juga sangat cepat. Dengan menggunakan kabel serat optik, frame relay switch dengan cepat mentransfer data sehingga berpindah dari satu ujung jaringan ke ujung lainnya dalam waktu yang relatif singkat. Jaringan frame relay juga memberikan tingkat keamanan yang wajar, berdasarkan kepemilikan jaringan pribadi bersama dengan transmisi serat optik. (Catatan: Direkomendasikan agar semua koneksi jaringan area luas yang aman harus menggunakan perangkat lunak enkripsi atau perangkat lunak jaringan pribadi virtual untuk memberikan tingkat keamanan yang lebih tinggi.) Selain itu, koneksi frame relay dapat bersifat permanen atau dapat dialihkan. Dengan koneksi permanen, saluran selalu tersedia. Koneksi switch, di sisi lain, memberikan kemampuan dinamis untuk mengalokasikan bandwidth sesuai permintaan.

Keuntungan lain yang terkait dengan jaringan frame relay (dan jaringan area luas berkecepatan tinggi modern lainnya) adalah tingkat kesalahannya selama transmisi rendah. Faktanya, tingkat kesalahan jaringan frame relay sangat rendah sehingga jaringan tidak memiliki pengendalian kesalahan apa pun. Jika terjadi kesalahan, jaringan frame relay akan membuang frame tersebut. Ini adalah tanggung jawab aplikasi, dan bukan jaringan frame relay, untuk melakukan pengendalian kesalahan.

Terakhir, jaringan frame relay memiliki harga yang wajar. Penetapan harga tetap bulanan didasarkan pada tiga biaya: biaya port untuk setiap jalur akses yang menghubungkan bisnis ke jaringan frame relay; biaya untuk setiap koneksi permanen yang berjalan melalui jaringan frame relay antara dua titik akhir (perusahaan yang menggunakan layanan ini); dan biaya untuk jalur akses, yaitu saluran telepon berkecepatan tinggi yang secara fisik menghubungkan bisnis ke port frame relay. Karena port dan jalur akses mampu mendukung beberapa koneksi permanen, pengguna dapat membayar satu biaya port, satu biaya jalur akses, dan beberapa biaya koneksi permanen.

Koneksi permanen yang diperlukan untuk mentransfer data antara dua titik akhir disebut sirkuit virtual permanen (PVC). (Catatan: Meskipun pembahasan saat ini berpusat pada frame relay, sebagian besar rincian berikut juga berlaku untuk layanan pengiriman data lainnya.) Ketika perusahaan ingin membuat koneksi frame relay antara dua kantor, perusahaan akan meminta frame relay penyedia untuk membangun PVC antar kantor (Gambar 11-9). Misalnya, jika sebuah perusahaan memiliki kantor di Chicago dan Orlando, perusahaan tersebut dapat meminta penyedia frame relay untuk membuat PVC antara kantor Chicago dan Orlando. Setiap kantor terhubung ke jaringan frame relay melalui jalur akses telepon berkecepatan tinggi melalui port. Port ini dan saluran telepon berkecepatan tinggi digabungkan untuk menciptakan koneksi fisik. PVC—koneksi logis—berjalan dari kantor Chicago, melalui jaringan frame relay, ke kantor Orlando.



Gambar 11-9 Koneksi frame relay antara Chicago dan Orlando, menunjukkan jalur akses, port, dan PVC

Jika dua kantor di Chicago dan Orlando mempunyai satu aplikasi (seperti berbagi database atau mentransfer catatan perusahaan) yang berjalan di antara keduanya, maka hanya satu PVC yang diperlukan. Namun, jika dua jenis aplikasi berbeda berjalan di antara dua kantor, mungkin perlu dibuat dua PVC. Meskipun terdapat dua PVC, dimungkinkan untuk mendukung kedua PVC tersebut melalui jalur akses dan port yang sama. Mendukung dua PVC melalui jalur akses dan pelabuhan yang sama akan dimungkinkan jika jumlah dari dua kecepatan transmisi PVC tidak lebih besar dari kapasitas pelabuhan dan jalur akses.

Untuk mengilustrasikan konsep ini, mari kita asumsikan bahwa aplikasi Chicago–Orlando memerlukan koneksi 256-kbps. Perusahaan meminta penyedia frame relay untuk PVC 256-kbps. Misalkan perusahaan mempunyai port 512-kbps dan saluran telepon yang mampu mendukung setidaknya 512 kbps (seperti T-1). Penyedia frame relay dapat memasang PVC 256-kbps antara kantornya di Chicago dan Orlando. Sekarang misalkan kedua kantor ingin menambahkan aplikasi baru dan oleh karena itu memerlukan tambahan PVC 256-kbps. Karena jumlah kedua PVC tidak lebih besar dari 512 kbps, perusahaan dapat meminta penyedia frame relay untuk menambahkan PVC tambahan 256 kbps ini.

Frame relay disebut protokol lapisan 2. Mengingat model OSI, penunjukan protokol lapisan 2 berarti bahwa teknologi frame relay hanya merupakan salah satu bagian dari aplikasi jaringan dan berada pada lapisan data link. Saat Anda membuat solusi jaringan untuk aplikasi tertentu, pilihan frame relay hanyalah salah satu bagian dari solusi. Anda tetap harus memilih perangkat lunak lapisan jaringan dan transport, seperti perangkat lunak yang mendukung protokol TCP dan IP, untuk dijalankan di atas jaringan frame relay, serta jenis saluran telepon berkecepatan tinggi pada lapisan fisik. Aplikasi yang dimaksud—misalnya, sistem pengambilan database—kemudian berjalan di atas TCP/IP.

Tingkat informasi yang berkomitmen atau perjanjian tingkat layanan

Ketika pelanggan membuat sirkuit virtual dengan pembawa frame relay, baik pelanggan maupun pembawa menyepakati sejumlah parameter penting yang berkaitan dengan transfer data pelanggan. Dengan layanan frame relay, hal ini disebut dengan commit information rate (CIR). Secara umum, ini disebut perjanjian tingkat layanan (SLA). Sebagian besar layanan pengiriman data memerlukan beberapa bentuk perjanjian tingkat layanan untuk ditandatangani sebelum sirkuit virtual apa pun dibuat. Untuk contoh frame relay kami, jika pelanggan mencari CIR sebesar 512 kbps, operator setuju untuk mentransfer data pelanggan dengan kecepatan ini. Pelanggan setuju bahwa ia tidak akan melebihi tarif ini. Disepakati juga bahwa jika pelanggan melebihi CIR-nya, dan jaringan frame relay menjadi jenuh, operator dapat menghapus frame pelanggan mana pun yang melebihi kecepatan informasi yang berkomitmen. Bagian tambahan dari perjanjian ini adalah tingkat burst, yang memungkinkan pelanggan untuk melebihi tingkat informasi yang berkomitmen dengan jumlah yang tetap untuk waktu yang singkat.

Untuk setiap sirkuit virtual, pelanggan dapat menentukan throughput yang terjamin dan waktu pengiriman data yang terbatas. Memiliki throughput yang terjamin berarti penyedia frame relay menjamin bahwa persentase tertentu dari semua frame akan dikirimkan, dengan asumsi bahwa data tidak ditransfer lebih cepat dari kecepatan informasi yang berkomitmen. Memiliki waktu pengiriman data yang terbatas berarti semua frame data akan dikirimkan dalam jumlah waktu yang disepakati, jika, sekali lagi, pelanggan tidak melebihi CIR. Harga sirkuit virtual kemudian akan berbanding lurus dengan tingkat CIR. Semakin tinggi tingkat CIR, semakin tinggi harga sirkuit virtualnya.

Perhatikan contoh sederhana. Sebuah bisnis di New York memiliki jalur akses berkecepatan tinggi (1,544 Mbps) ke dalam jaringan frame relay. Ia meminta operatornya untuk membuat sirkuit virtual dari New York ke Dallas dengan CIR 512 kbps. Jika bisnis tetap berada dalam CIR-nya, operator menjamin throughput 99,99 persen dan penundaan jaringan tidak lebih dari 20 milidetik. Sekarang, apa yang terjadi jika pelanggan melebihi CIR-nya dengan mengirimkan data pada kecepatan 800 kbps? Sebagian besar operator akan mengizinkan pelanggan untuk melebihi CIR hingga tingkat ledakan tetap hingga dua detik tanpa penalti. Untuk contoh ini, asumsikan pelanggan memiliki burst rate 256 kbps. Artinya pelanggan dapat melakukan transmisi pada kecepatan 512 kbps plus 256 kbps, atau 768 kbps selama dua detik. Jika pelanggan melebihi CIR-nya selama lebih dari dua detik, operator menetapkan bit Discard Eligible (DE) di header frame dari frame pelanggan. Jika kemacetan

jaringan terjadi, frame yang ditandai akan dibuang oleh switch jaringan. Hal ini kemudian menjadi tanggung jawab aplikasi pelanggan untuk mengawasi frame yang dibuang karena jaringan frame relay tidak memberi tahu pengguna bahwa frame tersebut dibuang.

Apa trade-off antara CIR rendah dan CIR tinggi? Jika Anda meminta CIR rendah dan kecepatan data Anda terus-menerus melebihi CIR tersebut, beberapa frame Anda mungkin dibuang. Namun jika jaringan tidak padat, Anda tidak akan kehilangan frame. Jika Anda membayar untuk CIR yang tinggi, dijamin kecepatan datanya lebih tinggi dan Anda tidak akan kehilangan frame, terlepas dari apakah jaringan sedang padat atau tidak. Pertanyaannya adalah seberapa besar Anda seorang penjudi. Anda dapat menghemat uang, menggunakan CIR yang lebih rendah, dan berharap jaringan tidak menjadi padat. Atau Anda dapat membayar untuk CIR yang lebih tinggi dan cukup yakin bahwa tidak ada frame yang akan dibuang. Jika Anda mendukung aplikasi yang tidak boleh kehilangan frame apa pun dalam kondisi apa pun, mungkin ada baiknya Anda membayar CIR yang lebih tinggi. Menariknya, bagaimanapun, banyak pelanggan frame relay memilih untuk membayar biaya terendah dengan memilih opsi Zero CIR yang tidak memberikan jaminan pengiriman.

Sekarang kita akan mengalihkan perhatian kita ke layanan pengiriman data lain yang kuat dan cukup menarik: Mode Transfer Asinkron.

11.7 MODE TRANSFER ASINCHRONOUS

Mode Transfer Asynchronous (ATM), seperti frame relay, adalah layanan packet-switched berkecepatan sangat tinggi yang ditawarkan oleh sejumlah perusahaan komunikasi. Sebuah bisnis yang ingin mengirim data antara dua titik (baik di dalam gedung atau di seluruh negeri) dengan kecepatan transfer yang sangat tinggi mungkin mempertimbangkan untuk menggunakan ATM. Kecepatan transfernya mencapai 622 Mbps, dan bahkan mungkin lebih cepat lagi di beberapa lokasi.

ATM memiliki beberapa fitur unik yang membedakannya dari frame relay dan layanan paket lainnya. Di ATM, semua data dikirim dalam paket kecil berukuran 53 byte yang disebut sel. Ukuran sel dijaga tetap kecil sehingga ketika sel mencapai sebuah node (switch point) dalam jaringan ATM, sel tersebut akan dengan cepat melewati node tersebut dan melanjutkan perjalanannya ke tujuannya. Kemampuan peralihan yang cepat ini membuat ATM memiliki kecepatan transfer yang sangat tinggi. Selain itu, ATM adalah jaringan yang sepenuhnya beralih. Saat sel berpindah dari satu node ke node lain melalui jaringan, masing-masing sel diproses dan diteruskan oleh switch berkecepatan tinggi (untuk penyegaran proses ini, tinjau pembahasan tentang switch di Bab Tujuh).

Jaringan ATM dirancang untuk mendukung suara, video, dan data secara bersamaan. Seperti yang akan Anda pelajari sebentar lagi, ATM dapat menangani berbagai aplikasi, termasuk video langsung, musik, dan suara interaktif. Selain itu, ATM dapat digunakan sebagai teknologi transfer untuk jaringan area lokal, jaringan area metropolitan, dan jaringan area luas. Karena ATM, seperti frame relay, adalah protokol lapisan 2, maka ATM dapat didukung oleh berbagai jenis media lapisan fisik, seperti twisted pair dan kabel serat optik. Terakhir, ATM dapat mendukung kelas lalu lintas yang berbeda untuk memberikan tingkat layanan yang

berbeda (kualitas layanan, atau QoS). Kelas lalu lintas ATM akan dijelaskan secara rinci pada bagian selanjutnya.

Seperti pada frame relay, sebelum ATM dapat mentransfer data apa pun, Anda harus terlebih dahulu membuat sambungan logis yang disebut sambungan saluran virtual (VCC). Berbeda dengan koneksi virtual frame relay, VCC ini harus dibuat melalui koneksi jalur virtual. Koneksi jalur virtual (VPC) adalah kumpulan VCC yang memiliki titik akhir yang sama. VCC dibuat untuk transfer data, namun juga digunakan untuk sinyal kontrol, manajemen jaringan, dan perutean. VCC dapat dibuat antara dua pengguna akhir, dalam hal ini VCC akan mengirimkan data dan sinyal kontrol. VCC juga dapat dibuat antara pengguna akhir dan entitas jaringan, dalam hal ini VCC akan mengirimkan sinyal kontrol pengguna ke jaringan. Ketika VCC mengirimkan sinyal kontrol pengguna-ke-jaringan, koneksinya disebut antarmuka pengguna-jaringan. Akhirnya, VCC dapat dibuat antara dua entitas jaringan, dalam hal ini VCC akan mengirimkan sinyal manajemen jaringan dan routing. Ketika VCC mentransmisikan sinyal manajemen jaringan dan perutean, itu disebut antarmuka jaringan-jaringan.

Kelas layanan ATM

Salah satu fitur ATM yang membedakannya dari sebagian besar sistem transmisi data dan suara lainnya adalah bahwa ATM memberikan pengguna kemampuan untuk menentukan kelas layanan. Kelas layanan adalah definisi jenis lalu lintas dan teknologi yang mendasarinya yang akan mendukung jenis lalu lintas tersebut. Misalnya, kelas layanan interaktif real-time mendefinisikan lalu lintas video langsung. Aplikasi interaktif real-time adalah salah satu aplikasi yang paling menuntut dalam hal kecepatan transmisi data dan throughput jaringan. Mengirimkan aliran video melalui suatu media memerlukan sejumlah besar bandwidth, dan menyediakan layanan real-time memerlukan jaringan yang cukup cepat untuk mengirim dan menerima video sehingga aplikasi langsung dapat didukung.

Jika suatu jaringan tidak menyediakan kelas tingkat layanan yang berbeda-beda, maka semua aplikasi akan membagi bandwidth jaringan secara merata, yang mungkin tidak memberikan distribusi bandwidth yang adil. Sebagai contoh, mari kita periksa Internet, yang menggunakan IPv4 tidak menawarkan fitur layanan kelas. Misalkan Anda dan rekan kerja sedang duduk di depan komputer di bilik yang berdekatan. Anda mengirim email, sementara rekan kerja Anda berpartisipasi dalam konferensi video langsung dengan rekan kerja ketiga di negara bagian lain. Baik aplikasi email maupun konferensi video menggunakan Internet untuk transmisi data. Meskipun aplikasi email Anda sering kali mengirimkan sangat sedikit data dan waktu sama sekali tidak penting, email Anda memiliki prioritas yang persis sama di Internet seperti aplikasi rekan kerja Anda, yang mencoba menjalankan proses yang sangat memakan waktu dan memakan waktu. konferensi video yang memakan data. Meskipun program email Anda mungkin berfungsi dengan baik melalui Internet, konferensi video rekan kerja Anda mungkin berkinerja buruk. Jika Internet dapat mendukung kelas layanan yang berbeda, program email Anda akan meminta layanan kelas rendah, dan program konferensi video rekan kerja Anda akan meminta layanan kelas tinggi. Dengan layanan kelas atas, program konferensi video akan berkinerja jauh lebih baik.

Dengan ATM, pelanggan menentukan kelas layanan yang diinginkan untuk setiap saluran virtual yang diatur. Seperti yang Anda duga, kelas layanan yang diinginkan menentukan harga untuk menggunakan saluran virtual tertentu. ATM telah menetapkan empat kelas layanan yang secara fungsional setara dengan layanan jalur sewa, layanan frame relay, dan layanan Internet. Kelas layanan ini menentukan jenis lalu lintas yang dapat dibawa oleh jaringan ATM:

- Kecepatan bit konstan (CBR)—Mirip dengan saluran sewaan sistem telepon saat ini, CBR adalah kelas layanan yang paling mahal. CBR bertindak sangat mirip dengan layanan telepon multipleks pembagian waktu, tetapi ini bukan sirkuit khusus seperti saluran telepon sewaan. CBR menghadirkan aliran data berkecepatan tinggi dan berkelanjutan yang dapat digunakan dengan aplikasi intensif transmisi.
- Variable bit rate (VBR)—Mirip dengan layanan frame relay, rt-VBR digunakan untuk aplikasi real-time, seperti video interaktif terkompresi, dan nrt-VBR digunakan untuk aplikasi non-real-time, seperti pengiriman e- email dengan lampiran multimedia yang besar. Aplikasi VBR sering mengirimkan data dalam jumlah besar, dan jaringan ATM menjamin bahwa lalu lintas VBR dikirimkan tepat waktu. CBR dan VBR sama-sama dianalogikan seperti terbang kelas satu. Kelas satu memang mahal, namun pelanggan mendapat prioritas utama dengan dijamin mendapat tempat duduk dan mendapat tempat duduk terlebih dahulu.
- Laju bit yang tersedia (ABR)—ABR juga digunakan untuk lalu lintas yang mungkin mengalami semburan data, yang disebut lalu lintas “bursty”, dan rentang bandwidthnya diketahui secara umum, seperti kumpulan saluran sewaan perusahaan. Kisaran transfer rendah dan tinggi ditentukan melalui negosiasi, namun mendapatkan ruang bit untuk mengirimkan data melalui jaringan ATM dengan layanan kelas ini mirip dengan terbang siaga di sebuah maskapai penerbangan. Anda mungkin mendapat kesempatan untuk mengirimkan data Anda, atau Anda mungkin harus menunggu. Namun begitu data Anda ada di jaringan, data itu akan dikirimkan. ABR baik untuk lalu lintas yang tidak harus tiba dalam jangka waktu tertentu. ABR juga memberikan feedback yang mengindikasikan jika ada bagian jaringan ATM yang mengalami kemacetan.
- Kecepatan bit tidak ditentukan (UBR)—UBR juga mampu mengirimkan lalu lintas yang mungkin mengalami semburan data, namun tidak ada jaminan kapan data akan dikirim; dan jika ada masalah kemacetan, tidak ada umpan balik kemacetan (seperti yang diberikan pada ABR). Tidak seperti data yang dikirimkan di kelas layanan lainnya, data yang dikirimkan melalui koneksi UBR mungkin tidak sampai ke tujuan akhir. Jika bandwidth yang diperlukan untuk mengirimkan data Anda diperlukan oleh data yang menggunakan kelas layanan yang lebih tinggi, data Anda mungkin dibuang di tengah sambungan jaringan. Bayangkan Anda sedang terbang dalam keadaan siaga tetapi akan terlempar keluar dari pesawat jika, selama sambungan, tempat duduk Anda dibutuhkan oleh orang lain. Layanan UBR biasanya merupakan layanan yang paling murah.

Dengan menawarkan kelas layanan yang berbeda, penyedia layanan ATM juga dapat menawarkan layanan transmisi yang disesuaikan dengan kebutuhan dan membebaskan biaya yang sesuai kepada pelanggan. Selain itu, pelanggan dapat meminta kelas layanan tertentu yang sesuai untuk aplikasi tertentu.

Komposisi Sel ATM

ATM mentransmisikan semua data dan sinyal kontrol menggunakan sel 53-byte (Gambar 11-10). Sel dibuat tetap kecil sehingga pengalihan sel ke rute tertentu (peralihan sel) dapat dilakukan oleh perangkat keras, yang merupakan cara peralihan sel tercepat. Header ATM selalu berukuran 5 byte, sehingga menyisakan 48 byte sel untuk data. Bidang sel dan fungsinya antara lain:

- Kontrol aliran generik hanya diterapkan pada antarmuka jaringan-pengguna. Kontrol aliran generik mengurangi kondisi kelebihan beban jangka pendek dengan memberi tahu pengguna untuk memperlambat pengiriman data ke jaringan ATM. Kontrol aliran generik saat ini tidak digunakan oleh banyak sistem ATM, jika ada.
- Pengidentifikasi jalur virtual adalah bidang 8-bit (memungkinkan 256 kombinasi) yang mengidentifikasi VPC tertentu.
- Pengidentifikasi saluran virtual adalah nilai 16-bit yang mengidentifikasi VCC unik. Ketika sebuah perusahaan membuat koneksi ATM antara dua lokasi, jalur virtual mendukung satu atau lebih saluran virtual. Agar dapat diidentifikasi dengan benar, jalur dan saluran memiliki nomor ID unik.
- Jenis payload terdiri dari tiga bit. Ketiga bit ini mengidentifikasi jenis payload, baik sebagai data pengguna atau pemeliharaan jaringan, dan melaporkan apakah kemacetan telah terjadi di jaringan.
- Prioritas kehilangan sel adalah satu bit dan diatur oleh pengguna. Nilai 0 berarti sel ini mempunyai prioritas tinggi, sehingga jaringan ATM harus berpikir dua kali untuk membuangnya jika terjadi kemacetan jaringan.
- Kontrol kesalahan header terdiri dari checksum redundansi siklik 8-bit ($x^8 x^2 x^1$). Ini menyediakan pemeriksaan kesalahan untuk empat byte pertama header, tetapi tidak untuk data. Checksum siklik juga dapat memberikan koreksi kesalahan dengan memperbaiki kesalahan bit tunggal di header.

Generic Flow	Virtual Path Identifier	Virtual Channel Identifier	
4 bits	8 bits	16 bits	
Payload Type	Cell Loss Priority	Header Error Control	Data
3 bits	1 bit	8 bits	
Data (continued)			
48 bytes			

Gambar 11-10 Sel ATM 53-byte dengan field individualnya

Kelebihan dan kekurangan ATM

Karena berbagai fiturnya, seperti kecepatan transfer yang tinggi, berbagai kelas layanan, dan kemampuan untuk beroperasi pada berbagai jenis media dan topologi jaringan, ATM memiliki sejumlah keunggulan yang signifikan. ATM dapat mendukung berbagai macam aplikasi dengan bandwidth yang bervariasi, pada rentang kecepatan transmisi yang luas. Peralihan sel, yang dilakukan oleh switch berbasis perangkat keras berkecepatan tinggi yang mengarahkan sel ke jalur yang sesuai, sangat cepat sehingga menghasilkan penundaan singkat dan bandwidth tinggi. Kelas layanan ATM yang berbeda memungkinkan pelanggan untuk memilih jenis layanan dan harga secara individual untuk setiap koneksi data (VCC). Terakhir, ATM sangat serbaguna. Itu dapat membawa suara, paket data, dan video melalui fasilitas yang sama.

Seperti yang Anda duga, ATM juga memiliki sejumlah kelemahan. Seringkali lebih mahal dibandingkan opsi transmisi data lainnya. Biaya peralatan ATM tinggi. Hal ini karena peralatan cell-switching, yang mampu memberikan koneksi secepat itu, memerlukan kebutuhan yang relatif rumit. Karena kompleksitas ATM, terdapat kurva pembelajaran yang tinggi untuk menyiapkan dan mengelola jaringan. Terakhir, perangkat keras dan perangkat lunak yang kompatibel mungkin tidak tersedia secara luas.

ATM kini banyak digunakan oleh operator telekomunikasi besar (AT&T, Sprint, dan sebagainya) untuk menyediakan layanan suara dan Internet. Karena kerumitan dan biayanya, beberapa usaha kecil enggan menggunakan ATM. Namun, teknologi alternatif yang dapat menawarkan kecepatan yang sebanding dengan biaya yang jauh lebih rendah telah menarik banyak perhatian dari usaha kecil. Jaringan Metro Ethernet, seperti yang kita lihat di bab sebelumnya, mengalami pertumbuhan di pasar pengiriman data wilayah metro. Namun bagaimana dengan pengiriman data dalam jarak yang lebih jauh? Ternyata, ada satu jaringan yang menyebabkan kesedihan bagi penyedia frame relay dan ATM: Internet.

11.8 MPLS DAN VPN

Hingga saat ini dalam diskusi, banyak yang telah dibicarakan tentang layanan pengiriman data seperti frame relay dan ATM, namun sedikit yang dibicarakan tentang penggunaan Internet untuk menghubungkan dua kantor bisnis. Mengapa frame relay dan ATM begitu banyak digunakan jika Internet tersedia dan pada dasarnya gratis? Ada dua alasan utama, seperti yang telah kita lihat. Pertama, tidak ada jaminan bahwa Internet akan mengirimkan data secara konsisten dan tepat waktu. Internet tidak dirancang untuk menangani aliran data dengan nilai latensi kecil. Dengan kata lain, ketika paket data berpindah ke router, tidak ada jaminan kapan paket tersebut akan meninggalkan router. Hal ini sebagian disebabkan karena router menangani lalu lintas dalam jumlah besar, dan tabel perutean yang ditemukan di router terus menjadi semakin kompleks setiap saat. Frame relay dan khususnya ATM dirancang untuk memindahkan paket dengan cepat melalui jaringan.

Alasan kedua mengapa frame relay dan ATM dipilih daripada Internet adalah persepsi bahwa frame relay dan ATM lebih aman. Meskipun benar bahwa frame relay dan ATM adalah jaringan pribadi (Anda harus memiliki kontrak dengan penyedia layanan sebelum Anda dapat

mentransfer data melalui jaringan), tidak ada jaminan bahwa semua data di jaringan pribadi aman kecuali ada tindakan pencegahan yang tepat. Hal ini berbeda dengan Internet. Hampir semua orang, dimanapun di dunia dapat terhubung ke Internet. Hal ini mengarah pada situasi di mana orang jahat dapat memangsa pengguna yang tidak menaruh curiga dalam jumlah yang hampir tidak terbatas.

Terlepas dari kekurangan yang tampak ini, semakin banyak bisnis yang beralih dari frame relay dan ATM, dan mengirimkan data mereka melalui Internet. Apa yang berubah? Pengguna internet kini memiliki dua senjata baru di gudang senjata mereka: MPLS dan VPN. Seperti yang kita lihat di bab sebelumnya, MPLS (Multiprotocol Label Switching) dapat digunakan untuk membuat jalur yang lebih cepat melalui Internet. Dan VPN (jaringan pribadi virtual) dapat menciptakan terowongan aman melalui Internet, yang melaluinya bisnis dapat dengan percaya diri mengirimkan data pribadi.

Pada dasarnya ada dua cara bisnis dapat membuat terowongan melalui Internet. Pada teknik pertama, pengguna menginstal perangkat lunak yang diperlukan di setiap ujung terowongan dan mengontrak penyedia layanan Internet untuk membuat dan memelihara terowongan. Ini biasanya dikenakan biaya bulanan dari ISP. Teknik kedua melibatkan pengguna membeli perangkat keras dan perangkat lunak yang diperlukan yang ditempatkan di setiap ujung terowongan. Perangkat keras pada dasarnya adalah gateway (router tingkat lanjut) yang menyediakan VPN dan perangkat lunak keamanan yang diperlukan. Pengguna sering kali membayar harga satu kali untuk perangkat kerasnya, namun masih memerlukan koneksi Internet standar melalui ISP.

Hanya waktu yang akan membuktikan apakah tren terowongan MPLS/VPN yang menggantikan layanan pengiriman data lainnya akan terus berlanjut. Meskipun demikian, frame relay dan ATM tidak akan hilang dalam semalam.

Ringkasan Layanan Pengiriman Data

Untuk memulai ringkasan kami, kami perlu membagi layanan pengiriman data kami menjadi tiga kategori berbeda. Kategori pertama berisi modem DSL dan kabel. Kita sering menganggap DSL dan modem kabel hanya sebagai koneksi lokal, antara pengguna dan ISP. Setelah koneksi dibuat antara pengguna dan ISP, teknologi DSL dan modem kabel berakhir dan teknologi jaringan area luas dimulai. T-1, frame relay, dan ATM termasuk dalam kategori kedua dan dapat digunakan baik untuk sambungan lokal maupun sambungan jarak jauh. Terakhir, MPLS/VPN membuat koneksi lokal dan jarak jauh, tetapi melalui Internet. Mereka tidak dapat bertahan hidup sendirian; untuk terhubung ke Internet melalui MPLS atau VPN, kita perlu menggunakan T-1, DSL, atau modem kabel.

Saat membandingkan modem DSL dan kabel, kami melihat banyak kesamaan (Tabel 11-1). Keduanya menawarkan koneksi Internet ke rumah atau bisnis kecil, bersifat tetap, tidak memberikan kualitas layanan apa pun, dan tersedia secara luas. Kecepatan transmisi datanya agak berbeda; namun jika Anda hanya membandingkan DSL konsumen dengan modem kabel, keduanya cukup mirip. DSL berkecepatan lebih tinggi tersedia dengan perkiraan peningkatan biaya.

Tabel 11-1 Ringkasan berbagai teknologi jaringan pengiriman data berkecepatan tinggi

	Tipe Kecepatan Maksimum	Biaya Perbulan *Rp. X.000	Dapat dialihkan / diperbaiki	QoS
Konsumen DSL	~ 600 Kbps	300	Tetap	Tidak
Bisnis DSL	~ 7 Mbps	1.000	Tetap	Tidak
Modem Kabel	~ 1.5 Mbps	350	Tetap	Tidak
T-1	1.544 Mbps	1.000 (Lokal)	Tetap	Tidak
Relay Bingkay	45 Mbps	1.000 – 10.000	Keduanya	Tidak
ATM	622 Mbps	1.000 – 10.000	Keduanya	Ya
MPLS/VPN		1.000an	Keduanya	Ya

*Tergantung pada koneksi ke Internet

Sekarang mari kita pertimbangkan T-1, frame relay, ATM, dan MPLS/VPN. Perhatikan bahwa ketika kita membandingkan kecepatan transmisi maksimum, ATM adalah salah satu yang tercepat—tetapi harganya lebih mahal. Selain itu, ATM merupakan teknologi yang paling kompleks (yang biasanya berarti pemeliharaan lebih tinggi dan biaya lebih tinggi). Frame relay menawarkan kecepatan yang wajar dengan harga yang wajar. Baik ATM maupun frame relay dapat bersifat tetap atau dapat dialihkan; namun layanan yang dapat dialihkan, jika tersedia, lebih mahal. T-1 ada dimana-mana. Dalam banyak kasus, kecepatan maksimum 1,544 Mbps dapat membatasi, dan T-1 jarak jauh bisa menjadi sangat mahal. T-3 secara signifikan lebih cepat (45 Mbps) dan karenanya lebih mahal.

Terakhir, MPLS/VPN menjadi cukup menarik. Dengan menggunakan Internet, seseorang dapat membuat koneksi yang aman dan relatif cepat antara dua titik akhir mana pun. Biayanya relatif rendah —tetapi jangan lupa bahwa Anda masih harus terhubung ke Internet, yang memerlukan koneksi seperti DSL atau T-1 di kedua ujung koneksi.

Dalam grup ini, hanya ATM dan, pada tingkat lebih rendah, MPLS/VPN yang dapat menawarkan fitur kualitas layanan. Hal ini dapat menjadi keuntungan besar dibandingkan teknologi lain bagi perusahaan yang membutuhkan koneksi berkecepatan tinggi, latensi rendah, dan kecepatan data konstan.

11.9 KONVERGENSI

Kita telah melihat contoh konvergensi di beberapa bab awal buku ini. Mulai dari Bab Satu, kita melihat bagaimana pasar pengguna Internet di seluruh dunia telah berkumpul pada rangkaian protokol TCP/IP. Pada Bab Dua, kita melihat bagaimana modulasi kode pulsa telah menjadi teknik utama untuk mengubah data analog menjadi sinyal digital. Pada Bab Tujuh, kita menemukan bagaimana pasar jaringan area lokal telah menyatu pada Ethernet dan hampir menghapuskan teknologi sebelumnya seperti jaringan token ring dan FDDI. Kita juga telah melihat bagaimana dua atau lebih teknologi menyatu menjadi satu. Misalnya, kita melihat di Bab Tiga bagaimana ponsel pintar dapat digunakan untuk mengambil dan mengirimkan foto, serta melakukan pengoperasian GPS, bermain game, mengirim email, menjalankan fungsi penunjuk tanggal dan kalender, dan bahkan mengunduh acara televisi.

Meskipun konvergensi merupakan tren penting di banyak bidang komunikasi data dan jaringan komputer, konvergensi mempunyai dampak yang nyata pada pasar telekomunikasi. Kita melihat sejumlah perusahaan telepon bergabung menjadi satu kesatuan. Contohnya termasuk penggabungan SBC dengan AT&T, dan Verizon dengan MCI. Tren merger telekomunikasi besar-besaran ini sungguh ironis jika kita mengingat kekhawatiran industri yang menyebabkan pecahnya AT&T. Pada saat itu, memisahkan layanan telekomunikasi agar dapat ditawarkan oleh banyak perusahaan dianggap sebagai hal yang terbaik bagi konsumen karena akan mendorong persaingan, yang akan menghasilkan harga yang lebih rendah. Saat ini pendulum tampaknya berayun ke arah lain—dan industri ini lebih memilih penggabungan berbagai layanan telekomunikasi.

Masalah konvergensi penting lainnya (seperti yang baru saja kita lihat) adalah kenyataan bahwa layanan pengiriman data seperti frame relay dan ATM mulai digantikan oleh layanan lain seperti Ethernet dan MPLS/VPN melalui tulang punggung IP. Ethernet jelas mendominasi arena jaringan area lokal. Dengan perluasan Metro Ethernet ke banyak pasar wilayah metropolitan, beberapa pihak di industri merasa hanya masalah waktu sebelum Ethernet menjadi jaringan area luas yang umum. Jika ini terjadi, Ethernet akan tersedia di jaringan lokal, metropolitan, dan area luas. Banyak perusahaan akan menganggap hal ini menarik karena mereka kemudian dapat mendukung semua kebutuhan jaringan mereka hanya dengan menggunakan satu teknologi: Ethernet. Dengan kata lain, sebuah bisnis akan dapat menyiapkan serangkaian jaringan yang mulus, semuanya menjalankan protokol Ethernet.

MPLS, yang diperkenalkan pada bab sebelumnya, juga menyebabkan jumlah sistem frame relay menurun. Dengan melapisi frame MPLS di atas frame IP, penyedia layanan mampu mengirimkan paket data berkecepatan tinggi melalui tulang punggung Internet.

Sebelum kita meninggalkan bab ini, mari kita lihat dua contoh konvergensi dalam industri telekomunikasi. Yang pertama melibatkan penggabungan jaringan telepon dengan jaringan area lokal untuk menciptakan satu jaringan yang dapat menangani panggilan telepon masuk dengan cara yang sama seperti menerima pesan email. Hal ini dikenal sebagai integrasi komputer-telepon. Yang kedua melibatkan konvergensi berbagai bentuk komunikasi seperti pesan, telepon, dan konferensi video ke dalam antarmuka terpadu yang ramah konsumen. Ini disebut komunikasi terpadu.

Integrasi komputer-telepon

Integrasi komputer-telepon (CTI) adalah bidang yang menggabungkan jaringan suara tradisional dengan jaringan komputer modern. CTI mengintegrasikan saklar telepon PBX dengan layanan komputer untuk menciptakan aplikasi suara dan data modern yang berjalan pada sistem komputer. Ingatlah bahwa PBX adalah sistem telepon internal yang digunakan banyak bisnis untuk mendukung semua operasi telepon mereka, termasuk panggilan in-house, panggilan in-house ke luar, pesan suara, transfer panggilan, dan panggilan konferensi. Secara tradisional, layanan ini memerlukan saklar PBX, satu set telepon, dan kabel telepon standar. Berbeda dengan CTI, yang Anda perlukan hanyalah workstation yang menjalankan perangkat lunak telepon yang sesuai. Karena CTI menggabungkan kekuatan sistem komputer

dengan layanan jaringan telepon, pengguna dapat melakukan pengoperasian telepon biasa dengan mengklik jendela program.

Pertimbangkan skenario berikut: Sebuah bisnis menjual produk dan menyediakan layanan pelanggan untuk mendukung produk tersebut. Untuk mendapatkan layanan pelanggan, pelanggan menghubungi nomor bebas pulsa perusahaan. Karena perusahaan memiliki sistem CTI yang menggabungkan kekuatan jaringan area lokal dengan layanan telepon modern, nomor telepon penelepon muncul di layar monitor komputer perwakilan layanan pelanggan saat telepon berdering (ID penelepon). Bahkan sebelum perwakilan layanan pelanggan menjawab telepon, sistem CTI menggunakan nomor telepon pelanggan sebagai kunci untuk permintaan database, dan ringkasan akun pelanggan juga muncul di layar. Perwakilan layanan pelanggan menjawab telepon dan menampilkan informasi pelanggan di layar ketika pelanggan berkata, "Halo." Saat perwakilan tersebut berbicara kepada pelanggan dan mengetahui masalah pelanggan, dia dapat mengklik ikon di layar komputer untuk mengalihkan panggilan pelanggan ke pihak lain, menunda pelanggan, atau mengambil informasi tambahan dari database komputer. Dengan demikian, perbedaan antara komputer dan sistem telepon menjadi sangat kabur. Komputer dan jaringan area lokal melakukan operasi telepon semudah melakukan operasi data.

CTI juga dapat mengintegrasikan kabel suara dengan kabel data. Sistem CTI awal menciptakan perpaduan yang kuat antara operasi data dan suara namun tetap mempertahankan kabel terpisah: satu set kabel untuk jaringan area lokal dan stasiun kerjanya, dan set lainnya untuk saluran telepon. PBX mungkin telah berkomunikasi langsung dengan jaringan area lokal, mengirimkan data dan perintah telepon bolak-balik, namun data komputer dan data telepon sebenarnya tetap terpisah secara fisik. Sebaliknya, sistem yang dikembangkan baru-baru ini mendukung data komputer dan data suara pada rangkaian kabel yang sama. Inovasi ini dapat menghemat uang perusahaan dalam hal pemasangan kabel—seringkali merupakan salah satu bagian jaringan yang paling mahal. Namun desain ini memiliki kelemahan karena memerlukan sistem pengkabelan tunggal yang lebih besar.

Menggunakan CTI memiliki tiga keuntungan. Pertama, menciptakan aplikasi bisnis suara/data baru yang dapat menghemat waktu perusahaan. Kedua, memanfaatkan sumber daya yang ada secara optimal. Ketiga, menghemat uang. Keuntungan ini berarti bahwa bisnis dapat memperoleh banyak manfaat dari aplikasi CTI. Misalnya:

- *Perpesanan terpadu*—Pengguna menggunakan satu aplikasi desktop untuk mengirim dan menerima e-mail, pesan suara, dan faks.
- *Respons suara interaktif*—Saat pelanggan menelepon suatu perusahaan, nomor teleponnya digunakan untuk mengambil catatan pelanggan dari database perusahaan. Catatan pelanggan ditampilkan di stasiun kerja perwakilan layanan saat perwakilan tersebut menjawab telepon.
- *Pengenalan dan respons suara terintegrasi*—Pengguna yang menelepon ke sistem telepon perusahaan menyediakan beberapa bentuk data dengan berbicara ke telepon, dan permintaan database dilakukan menggunakan informasi lisan ini.

- *Pemrosesan faks dan faks-kembali*—Dalam pemrosesan faks, gambar faks yang disimpan pada hard disk server LAN dapat diunduh melalui jaringan area lokal, dikonversi dengan kartu faks, dan dikirim ke pelanggan melalui trunk. Faks yang masuk dapat dikonversi ke format file dan disimpan di server jaringan area lokal. Dengan faks kembali, pengguna menghubungi server faks, mengambil faks dengan memasukkan nomor, dan mengirimkan faks tersebut ke mana saja.
- *Konversi teks-ke-ucapan dan ucapan-ke-teks*—Saat seseorang berbicara melalui telepon, sistem dapat mendigitalkan suara tersebut dan menyimpannya di hard disk drive sebagai data komputer. Sistem juga dapat melakukan operasi sebaliknya.
- *Kontrol panggilan pihak ketiga*—Pengguna memiliki kemampuan untuk mengontrol panggilan—misalnya, mengatur panggilan konferensi—tanpa menjadi bagian darinya.
- *Antarmuka pengguna grafis PBX*—Ikon berbeda di layar komputer mewakili fungsi umum PBX seperti penahan panggilan, transfer panggilan, dan konferensi panggilan, sehingga membuat sistem lebih mudah digunakan oleh operator.
- *Pemfilteran panggilan*—Pengguna dapat menentukan nomor telepon yang boleh dihubungi. Semua panggilan lainnya akan dialihkan ke petugas atau kotak pesan suara.
- *Sistem menu yang disesuaikan*—Organisasi dapat membuat menu yang disesuaikan untuk sistem penjawab otomatis guna membantu penelepon menemukan informasi, agen, atau departemen yang tepat. Dengan menggunakan fungsionalitas drag-and-drop, sistem menu dapat direvisi setiap hari. Sistem menunya bisa interaktif, memungkinkan penelepon merespons perintah suara dengan menekan nomor yang berbeda. Pesan suara yang berbeda dapat dikaitkan dengan setiap respons, dan pesan suara dapat dibuat secara instan melalui mikrofon PC.

Seperti yang Anda lihat, beberapa aplikasi menarik bermunculan dari konvergensi sistem suara dan data.

Komunikasi terpadu

Sama seperti CTI yang merupakan konvergensi berbagai teknologi dan aplikasi, komunikasi terpadu juga menggabungkan berbagai bentuk komunikasi. Lebih tepatnya, komunikasi terpadu adalah konvergensi layanan komunikasi real-time dan non-real-time seperti telepon, pesan instan, konferensi video, pengenalan suara, pesan suara, email, dan sesuatu yang disebut informasi kehadiran menjadi satu kesatuan. antarmuka. Ini bukan produk tunggal melainkan kombinasi produk yang, ketika bekerja sama, memberikan pengalaman pengguna yang terpadu. Misalnya, pengguna yang bekerja dalam lingkungan komunikasi terpadu akan dapat mengirim email dari komputer dan kemudian menerima balasan sebagai pesan teks atau pesan suara di telepon seluler.

Beberapa produk komunikasi terpadu juga menyediakan perangkat lunak kolaboratif, yang memungkinkan tim pengguna berkomunikasi melalui berbagai platform. Misalnya, rekan kerja, vendor, dan pelanggan dapat berkolaborasi dan berbagi video, teks, telepon, dan gambar baik dari jarak jauh atau di kantor. Program online populer Facebook juga dapat dianggap sebagai bentuk komunikasi terpadu, karena memungkinkan papan pesan, pesan

berbasis teks, ruang obrolan online, email, dan video interaktif semuanya melalui antarmuka yang umum.

Tidak diragukan lagi, konvergensi memainkan peran besar dalam industri komunikasi. Bentuk konvergensi baru apa yang akan muncul dalam hidup Anda? Apakah Anda akan menjadi salah satu penciptanya?

11.10 SISTEM TELEKOMUNIKASI PERUSAHAAN

Better Box Corporation memproduksi kotak karton. Kantor pusat administratifnya berada di Chicago, Illinois, dan memiliki kantor penjualan regional di Seattle, San Francisco, dan Dallas. Better Box sedang memperluas kemampuan jaringan datanya dan meminta bantuan Anda dalam merancang jaringan perusahaan barunya. Ia ingin menghubungkan keempat lokasinya, sehingga kantor pusat di Chicago dapat menerima catatan data dari tiga kantor lainnya. Biasanya, sekitar 20.000 catatan penjualan per bulan akan diunggah dari masing-masing kantor penjualan regional. Setiap catatan penjualan berukuran 400.000 byte. Diperlukan waktu tidak lebih dari 20 detik untuk mengunggah satu catatan penjualan. Meskipun perusahaan mempunyai dana yang cukup untuk mendukung banyak kemungkinan solusi, perusahaan ingin mencari solusi yang paling hemat biaya untuk jangka panjang.

Pilihan

Untuk membuat keputusan yang tepat mengenai jenis layanan transmisi data, kami akan mempertimbangkan harga sejumlah jenis layanan yang berbeda:

- Layanan telepon biasa yang mentransmisikan data dengan kecepatan 56 kbps melalui saluran analog
- T-1 jarak lokal (intraLATA) (tarif bulanan tetap) dan T-1 jarak jauh (antar-LATA) (tarif bulanan tetap ditambah biaya jarak tempuh)
- Serangkaian layanan frame relay, yang mencakup kecepatan port dan kapasitas PVC
- Serangkaian layanan ATM, yang meliputi kecepatan port, biaya jalur, dan biaya saluran
- Menggunakan MPLS dan VPN untuk menciptakan koneksi yang aman dan cepat melalui Internet Mari kita periksa masing-masing hal ini satu per satu.

Membuat pilihan

Untuk memilih layanan pengiriman data yang tepat, Anda harus memilih kecepatan transmisi data yang sesuai untuk setiap layanan, menjaga biaya tetap rendah, dan memenuhi persyaratan Better Box. Untuk setiap layanan jaringan, mari kita periksa total biaya per bulan yang mungkin dibayarkan Better Box Corporation kepada operator telekomunikasi untuk menggunakan layanan tersebut guna menghubungkan keempat situsnya. Ingatlah bahwa biaya frame relay memiliki tiga komponen: (1) biaya jalur akses, (2) biaya port frame relay, dan (3) biaya PVC. Demikian pula, ATM mempunyai empat komponen biaya: (1) biaya jalur akses, (2) biaya port ATM, (3) biaya saluran PVC, dan (4) biaya jalur PVC. Tabel 11-2 mencantumkan biaya untuk komponen-komponen ini serta biaya untuk jenis layanan lainnya.

Tabel 11-2 Harga hipotetis berbagai layanan telekomunikasi

Type of Service	Speed	Per-Month Cost (Approximate)
POTS	~53 kbps	\$20
T-1 (local-distance)	1.544 Mbps	\$350
T-1 (long-distance)	1.544 Mbps	\$1200 + \$2.50 per mile
Frame Relay port	56 kbps	\$220
	128 kbps	\$400
	256 kbps	\$495
	512 kbps	\$920
	768 kbps	\$1240
	1.544 Mbps	\$1620
Frame Relay PVC	56 kbps	\$60
	128 kbps	\$110
	256 kbps	\$230
	512 kbps	\$410
	1024 kbps	\$1010
	1.544 Mbps	\$1410
ATM CBR port	1.544 Mbps	\$2750
	3 Mbps	\$3400
ATM ABR port	1.544 Mbps	\$1750
	3 Mbps	\$2400
ATM PVC path		\$2 per mile
ATM PVC channel		\$250 per channel (no mileage charge)
MPLS/VPN	Depends on link to ISP	\$1000 initial hardware per port plus \$375 per month ISP charge

**harga Paket Lengkap Jawa dan Bali di Lampiran*

Untuk memulai, Anda perlu membaca ulang rencana Better Box dan mengetahui persyaratan transmisi perusahaan. Kami melihat persyaratan bahwa catatan 400.000 byte tidak boleh lebih dari 20 detik untuk diunggah. Berikut beberapa perhitungan sederhana:

$$400.000 \text{ Bytes} \times 8 \text{ Bits/byte} = 3.200.000 \text{ bits}$$

$$n = 3.200.000 \text{ bits}/20 \text{ detik}$$

$$n = 160.000 \text{ bps}$$

Untuk memulai, Anda perlu membaca ulang rencana Better Box dan mengetahui persyaratan transmisi perusahaan. Kami melihat persyaratan bahwa catatan 400.000 byte tidak boleh lebih dari 20 detik untuk diunggah. Berikut beberapa perhitungan sederhana:

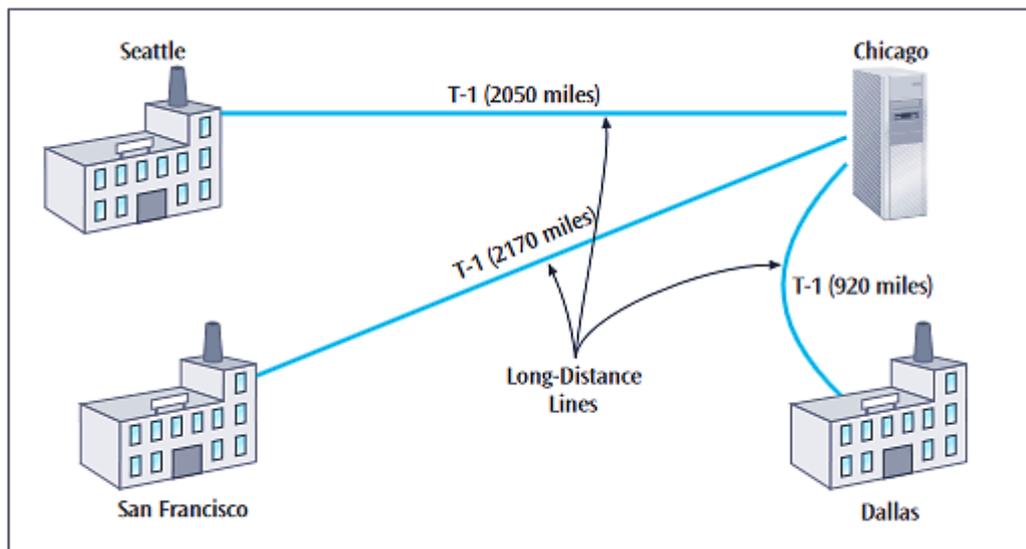
Oleh karena itu, Better Box membutuhkan jalur telekomunikasi yang terhubung ke dunia luar dengan kecepatan transmisi minimal 160 kbps. Layanan apa yang akan memenuhi persyaratan ini?

Untuk mencapai kecepatan transmisi minimal 160 kbps, Better Box perlu menggunakan jalur T-1, layanan frame relay, layanan ATM, atau MPLS/VPN. Jalur POTS tidak akan cukup, karena kecepatan transmisi terbaik yang dapat dicapai menggunakan modem dial-up dengan POTS adalah 53 kbps (sebenarnya, mungkin 53 kbps yang mendorongnya).

Ketika Anda mempertimbangkan skenario T-1 (Gambar 11-11), Anda menyadari bahwa Better Box memerlukan tiga jalur T-1: satu dari Seattle ke Chicago (2.050 mil), satu dari San Francisco ke Chicago (2.170 mil), dan satu dari Dallas ke Chicago (920 mil). Masing-masing jalur ini merupakan jalur jarak jauh, atau interLATA. Dengan menggunakan jarak tempuh antara titik-titik ini, tiga jalur interLATA T-1 akan memakan biaya kira-kira:

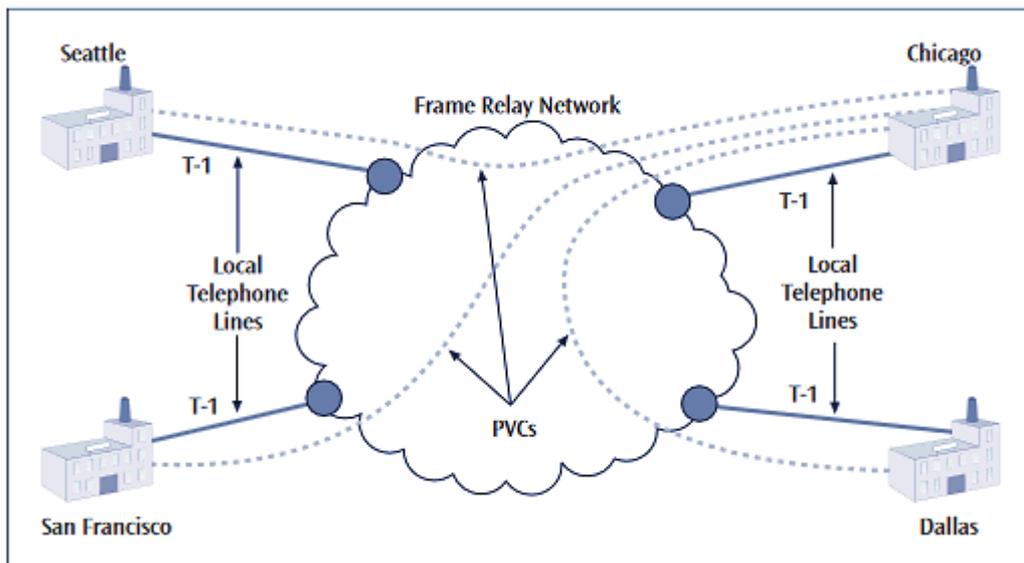
- Rp. 63.250.000 (Rp. 12.000.000 per bulan + Rp250.000 per mil dari Seattle ke Chicago)
- Rp. 66.250.000 (Rp. 12.000.000 + Rp. 250.000 per mil dari San Francisco ke Chicago)
- Rp. 35.000.000 (Rp. 12.000.000 + Rp. 250.000 per mil dari Dallas ke Chicago)

Ini memberi kami total bulanan Rp. 16.450.000. Sayangnya, skenario ini bahkan tidak memungkinkan Seattle untuk berbicara langsung dengan San Francisco, atau Seattle untuk berbicara langsung dengan Dallas, misalnya; itu menyediakan komunikasi hanya antara Chicago dan masing-masing situs regional. Jika Better Box ingin masing-masing dari empat situs berkomunikasi langsung satu sama lain, maka diperlukan enam koneksi. (Administrator jaringan yang cerdas mungkin dapat menemukan cara agar setiap situs dapat berkomunikasi dengan situs lainnya, namun tetap hanya menggunakan empat koneksi. Kita biarkan ini sebagai latihan.)



Gambar 11-11 Tiga jalur T-1 yang menghubungkan tiga kantor regional ke Chicago

Dengan skenario frame relay, Anda tidak perlu khawatir menjalankan jalur terpisah antara setiap pasangan kota. Anda hanya perlu membuat koneksi frame relay ke jaringan frame relay (Gambar 11-12). Jadi, empat koneksi memungkinkan kita mengirim data antara dua kota mana pun. Seperti yang sudah kami hitung, masing-masing koneksi tersebut harus mendukung kecepatan transmisi 160 kbps. Koneksi frame relay 256 kbps adalah ukuran terdekat yang akan mendukung kecepatan yang diinginkan.



Gambar 11-12 Empat kota terhubung ke frame relay cloud

Biaya frame relay akan mencakup:

- Tiga biaya port masing-masing 256 kbps = 3 x Rp. 4.950.000 = Rp. 14.850.000
- Satu port di Chicago dengan kecepatan 512k (untuk mendukung total tiga koneksi yang melewatinya) = Rp. 9.200.000
- Total biaya Port = Rp. 24.050.000
- Tiga muatan PVC untuk tiga sambungan 256-kbps (diwakili oleh garis putus-putus pada Gambar 11-12) = 3 x Rp. 2.300.000 = Rp. 6.900.000
- Empat saluran telepon jarak lokal T-1 untuk menghubungkan empat kota ke jaringan frame relay = 4 x Rp. 3.500.000 = Rp. 14.000.000

Total biaya untuk frame relay adalah Rp. 44.950.000 per bulan, yang jauh lebih murah dibandingkan opsi sebelumnya yang menggunakan tiga jalur interLATA T-1 di antara empat kota.

Solusi ATM akan mirip dengan solusi frame relay di mana Anda hanya perlu menghubungkan keempat kota ke cloud ATM. Setelah ini terhubung, Anda akan membuat tiga jalur dengan satu saluran di setiap jalur. Tata letak ini akan sangat mirip dengan tata letak frame relay. Koneksi ATM ABR 1,544 Mbps adalah ukuran terdekat yang akan mendukung kecepatan yang diinginkan. Biaya ATM akan mencakup:

- Empat biaya pelabuhan di empat kota, masing-masing ABR 1,544-Mbps = 4 x Rp. 17.500.000 = Rp. 70.000.000
- Tiga saluran untuk mendukung tiga koneksi = 3 x Rp. 2.500.000 = Rp. 7.500.000
- Tiga jalur untuk mendukung tiga saluran = Rp. 20.000 per mil x 5.140 mil = Rp. 102.800.000
- Empat T-1 intraLATA untuk menghubungkan empat lokasi ke ATM cloud = 4 x Rp. 3.500.000 = Rp. 14.000.000

Total biaya untuk jaringan ATM ABR adalah Rp. 194.300.000 per bulan.

Solusi terakhir kami adalah pembuatan terowongan MPLS/VPN melalui Internet. Biaya yang terkait dengan terowongan Internet terutama terdiri dari biaya perangkat keras awal (dua gateway, satu di setiap ujung sambungan) ditambah sambungan bulanan antara bisnis dan penyedia layanan Internet. Kami memerlukan dua T-1 intraLATA yang setara, seperti yang kami perlukan untuk menghubungkan frame relay dan ATM ke cloud masing-masing. Selain itu, kami juga harus membayar biaya bulanan ke ISP untuk koneksi Internet berkecepatan tinggi. Itu memberi kita biaya berikut:

- Biaya awal Rp. 10.000.000 per gateway per port = 4 x Rp. 10.000.000 = Rp. 40.000.000
- Biaya bulanan koneksi ISP di setiap port = 4 x Rp. 3.750.000 = Rp. 15.000.000
- Biaya bulanan T-1 jarak lokal di setiap lokasi = 4 x Rp. 3.500.000 = Rp. 14.000.000

Tampaknya setelah biaya awal Rp. 40.000.000, kami akan dikenakan biaya Rp. 29.000.000 per bulan. MPLS/VPN adalah solusi yang paling murah, diikuti oleh solusi frame relay.

RINGKASAN

- Sistem telepon dasar yang mencakup Amerika Serikat disebut layanan telepon biasa, dan merupakan gabungan loop lokal analog dan sirkuit digital. Saluran telepon dirancang untuk membawa sinyal suara dengan sinyal bandwidth 4000 Hz. Saluran telepon adalah kumpulan kabel yang membentang dari kantor pusat ke rumah atau bisnis dan mentransfer sinyal analog; itu disebut loop lokal. Batang telepon membawa beberapa sinyal telepon digital dan biasanya berjalan antara kantor pusat dan pusat switching.
- Divestasi AT&T pada tahun 1984 membuka pasar telepon jarak jauh ke penyedia layanan jarak jauh lainnya, memaksa AT&T untuk menjual perusahaan telepon lokalnya, dan membagi negara menjadi wilayah transportasi akses lokal.
- PBX adalah saklar telepon terkomputerisasi lokal yang menangani semua panggilan telepon internal dan keluar, dan menawarkan sejumlah layanan telepon.
- Centrex menawarkan layanan yang sama seperti PBX, namun peralatannya berada di properti perusahaan telepon, dan bisnis menyewakan layanan tersebut. Saluran pribadi atau saluran sewaan adalah saluran telepon permanen yang menghubungkan dua lokasi dan menyediakan akses konstan tanpa perlu menghubungi nomor telepon.
- Undang-Undang Telekomunikasi tahun 1996 membuka layanan telepon lokal bagi pesaing baru dan mewajibkan perusahaan telepon lokal yang ada untuk memberikan akses ke saluran telepon lokal kepada pesaing tersebut. Perusahaan telepon lokal yang sudah ada dikenal sebagai operator pertukaran lokal yang sudah ada, sementara perusahaan telepon lokal yang baru dikenal sebagai operator pertukaran lokal yang kompetitif.
- Kecepatan data modem dial-up yang menggunakan saluran telepon tingkat suara telah mencapai puncaknya pada kecepatan mendekati 50.000 bit per detik, tergantung pada kondisi saluran.
- Jalur sewa dibuat oleh penyedia layanan komunikasi dan berfungsi sebagai sambungan pribadi permanen antara dua lokasi. Banyak jenis layanan jalur sewaan yang ditawarkan

oleh perusahaan telepon. Layanan jalur sewa paling populer adalah T-1 serba digital 1,544-Mbps.

- Teknologi seperti jalur pelanggan digital dan modem kabel telah meningkatkan kecepatan transfer data yang tersedia antara rumah dan bisnis serta penyedia layanan Internet; kecepatan transfer data ini sekarang mencapai jutaan bit per detik. Saat ini, terdapat berbagai jenis layanan DSL di seluruh negeri, namun sebagian besar dapat diklasifikasikan menjadi splitterless (hanya layanan DSL), splitter (layanan DSL dan layanan telepon POTS pada rangkaian kabel yang sama), asimetris, atau simetris.
- Frame relay adalah layanan yang menyediakan transfer data digital melalui jarak lokal dan jarak jauh dengan kecepatan transfer data tinggi, latensi rendah, dan tingkat kesalahan rendah.
- Untuk menggunakan layanan frame relay, pelanggan menghubungi penyedia frame relay yang membuat sirkuit virtual permanen antara pelanggan dan situs yang ingin dihubungkan dengan pelanggan. Pelanggan membayar PVC, akses ke jaringan frame relay (biaya port), dan saluran telepon yang memberikan pelanggan akses ke pelabuhan.
- Frame relay adalah protokol lapisan 2, yang berarti dapat dijalankan pada berbagai media fisik dan mendukung berbagai jenis aplikasi pada lapisan 3 dan lebih tinggi. Tingkat informasi yang berkomitmen adalah kesepakatan antara pelanggan frame relay dan penyedia layanan. Permintaan pelanggan
- kecepatan transmisi tertentu; dan jika pelanggan tidak melebihi tarif tersebut, penyedia layanan akan menjamin pengiriman bingkai data yang akurat dan tepat waktu.
- Frame relay lebih dapat diandalkan dibandingkan Internet dan memberikan tingkat keamanan yang lebih baik, namun Internet lebih murah dan tersedia di mana saja.
- Mode Transfer Asinkron juga merupakan layanan packet-switched, namun mendukung semua jenis lalu lintas. Karena ATM menggunakan switch yang sangat cepat, maka ATM dapat mentransfer sel ATM dengan kecepatan yang sangat tinggi (lebih dari 600 Mbps). Untuk menawarkan ATM, penyedia layanan ATM membuat koneksi jalur virtual antara dua titik, dan pengguna kemudian membuat satu atau lebih koneksi saluran virtual melalui jalur virtual tersebut. Keuntungan yang kuat dari ATM adalah bahwa ia menyediakan sejumlah kelas layanan yang berbeda untuk mendukung berbagai aplikasi jaringan, beberapa di antaranya mungkin memerlukan kecepatan transmisi dan throughput jaringan yang berbeda-beda. Kerugian dari layanan ini termasuk kompleksitas dan biayanya.
- Frame relay dan ATM mengalami penurunan pangsa pasar karena adanya dua pendatang baru: MPLS dan jaringan pribadi virtual. Keuntungan MPLS dan VPN adalah biaya yang lebih rendah dan kemampuan untuk menggunakan Internet di mana-mana.
- Integrasi komputer-telepon adalah konvergensi jaringan komunikasi data dan sistem suara. Konvergensi ini menyediakan sejumlah aplikasi suara/komputer baru, seperti layanan telepon yang dikendalikan stasiun kerja dan layanan pengambilan data.
- Komunikasi terpadu adalah konvergensi pesan, video, dan audio dalam penyampaian dan kolaborasi operasi bisnis sehari-hari.

PERTANYAAN

1. Apa yang dimaksud dengan layanan telepon lama biasa?
2. Berapakah rentang frekuensi khas suara manusia?
3. Dua entitas apakah yang dihubungkan oleh loop lokal?
4. Apa itu LATA?
5. Apa perbedaan bagasi dengan saluran telepon?
6. Sebutkan hasil terpenting dari Keputusan Akhir AT&T yang Dimodifikasi.
7. Apa perbedaan antara operator bursa lokal dan operator antar bursa?
8. Sebutkan hasil-hasil terpenting dari Undang-Undang Telekomunikasi tahun 1996.
9. Mengapa modem 56-kbps lebih cepat dibandingkan modem lama 33.600-bps?
10. Mengapa modem 56 kbps tidak melakukan transmisi pada kecepatan 56 kbps?
11. Apa saja fitur dasar dan kecepatan transfer DSL?
12. Apa saja fitur dasar dan kecepatan transfer modem kabel?
13. Apa perbedaan layanan jalur sewa dengan POTS?
14. Apa ciri-ciri dasar jalur T-1?
15. Apa saja layanan dasar jalur T-3?
16. Apa karakteristik dasar frame relay?
17. Fitur apa yang membuat frame relay begitu menarik?
18. Bagaimana cara membuat rangkaian virtual permanen frame relay?
19. Apa perbedaan sirkuit virtual yang diaktifkan dengan sirkuit virtual permanen?
20. Apakah mungkin untuk memiliki lebih dari satu PVC dalam satu jalur fisik? Menjelaskan.
21. Apa yang terjadi ketika pelanggan dan layanan frame relay menyetujui tingkat informasi yang berkomitmen?
22. Apa yang terjadi bila pengguna mengirimkan data lebih cepat dari kecepatan informasi yang disepakati?
23. Bagaimana frame relay dibandingkan dengan pengiriman data melalui Internet?
24. Apa saja fitur dasar ATM?
25. Apa hubungan antara koneksi saluran virtual ATM dan koneksi jalur virtual?
26. Apa yang dimaksud dengan ATM yang mempunyai kelas pelayanan?
27. Jelaskan beberapa aplikasi yang menggabungkan integrasi komputer-telepon.
28. Teknologi apa yang mengancam penggunaan frame relay dan ATM?

LATIHAN SOAL

1. Saluran telepon yang menghubungkan rumah atau bisnis Anda ke kantor pusat (local loop) membawa percakapan Anda dan percakapan orang yang Anda ajak bicara. Berapa perkiraan Anda bandwidth loop lokal?
2. Jika Anda memutar CD untuk seorang teman melalui telepon, apakah teman Anda akan mendengarkan musik berkualitas tinggi? Jika tidak, mengapa tidak?

3. Jika Anda melakukan panggilan telepon dan panggilan tersebut meninggalkan LATA Anda dan masuk ke LATA lain, jenis panggilan telepon apa yang telah Anda lakukan? Perusahaan telepon macam apa yang menangani panggilan telepon ini?
4. Untuk setiap skenario berikut, nyatakan apakah saluran telepon atau saluran utama harus digunakan:
 - A. Koneksi dari rumah Anda ke perusahaan telepon lokal
 - B. Hubungan antara PBX perusahaan besar dan perusahaan telepon
 - C. Koneksi antara dua kantor pusat
5. Banyak orang di industri telepon merasa pada akhirnya kita akan kehabisan kode area dan nomor telepon. Berapa banyak kode area berbeda yang tersedia saat ini? Apa yang Anda sarankan untuk menambah jumlah nomor telepon?
6. Nyatakan apakah hal-hal berikut ini merupakan akibat dari Keputusan Akhir yang Dimodifikasi tahun 1984, Undang-Undang Telekomunikasi tahun 1996, atau bukan keduanya:
 - A. FCC dibentuk untuk mengawasi sistem telepon antar negara bagian.
 - B. AT&T harus menjual perusahaan telepon lokalnya.
 - C. LATA telah dibuat.
 - D. Perusahaan televisi kabel dapat menyediakan layanan telepon lokal.
 - E. Pelanggan dapat memilih di antara penyedia telepon jarak jauh yang berbeda.
 - F. AT&T memisahkan divisi teknologinya, yang menjadi Lucent.
7. Anda ingin memulai perusahaan telepon lokal Anda sendiri. Apakah Anda harus memasang saluran telepon sendiri ke setiap rumah dan bisnis? Menjelaskan.
8. Jenis layanan telepon apa yang Anda gunakan untuk menghubungkan PBX ke kantor pusat jika Anda ingin mengizinkan 40 pengguna melakukan panggilan keluar secara bersamaan?
9. Jika Anda memasang modem 56-kbps di komputer Anda dan melakukan panggilan ke jaringan jarak jauh yang hanya memiliki modem 33.600-bps, apakah modem Anda tidak berguna? Pertahankan jawaban Anda.
10. Mengapa Anda ingin menggunakan modem V.92 yang lebih baru daripada V.90 yang lama? Mengapa layanan Internet online mungkin tidak ingin Anda menggunakan modem V.92?
11. Anda masuk ke penyedia layanan Internet Anda menggunakan modem 56k Anda. Setelah terhubung, kecepatan data Anda ditampilkan 42.000 bps. Mengapa tidak 56k bps? Buat daftar semua kemungkinan alasannya.
12. Keesokan harinya, Anda menghubungi penyedia layanan Internet yang berbeda dari yang digunakan pada pertanyaan sebelumnya. Kali ini Anda terhubung pada 24.000 bps. Mungkinkah ada alasan lain yang menyebabkan koneksi lebih lambat ini? Jelaskan tanggapan Anda.
13. Modem kabel, seperti modem 56k, menghasilkan koneksi asimetris. Apa artinya ini, dan mengapa koneksi asimetris ini tidak mempengaruhi rata-rata pengguna Web?
14. Apa fungsi dasar modem kabel?

15. Berikan contoh seseorang ingin menggunakan layanan DSL simetris.
16. Apa keunggulan utama DSL asimetris dibandingkan DSL simetris?
17. Dalam layanan DSL, apa fungsi DSLAM?
18. Anda tinggal di sebuah rumah yang berjarak 10 mil dari kota terdekat. Apakah Anda bisa mendapatkan layanan DSL ke rumah Anda? Jika jawabannya tidak, apa yang dapat dilakukan penyedia layanan DSL untuk menyediakan DSL kepada Anda?
19. Jika Anda sudah memasang layanan frame relay, bisakah Anda langsung mengangkat telepon dan menghubungi nomor pihak yang ingin Anda hubungi? Menjelaskan.
20. Misalkan Anda ingin memiliki koneksi frame relay antara kantor Anda di Chicago dan kantor Anda di New York. Uraikan berbagai biaya yang harus Anda bayar untuk koneksi ini.
21. Anda telah membuat sambungan frame relay dengan kecepatan informasi berkomitmen sebesar 256 kbps dan kecepatan burst sebesar 128 kbps. Beberapa kali sehari, sistem komputer Anda mengirimkan lebih dari 512 kbps. Apa yang akan terjadi pada data Anda?
22. Apa sebenarnya yang dilakukan frame relay jika frame kacau dan menghasilkan kesalahan checksum?
23. Nyatakan apakah frame relay atau Internet merupakan media transmisi yang lebih baik untuk setiap aktivitas berikut:
 - A. Mengirim email
 - B. Mengirim data berkecepatan tinggi
 - C. Mengirimkan komunikasi suara interaktif
 - D. Menerima streaming video langsung
 - E. Berpartisipasi dalam ruang obrolan atau newsgroup
24. Salah satu kelemahan ATM adalah “pajak sel 5-byte.” Jelaskan apa artinya ini.
25. Anda memiliki koneksi ATM yang berpindah dari lokasi Anda ke entitas jaringan, ke entitas jaringan kedua, dan kemudian ke tujuan yang Anda inginkan.
Gambarlah sketsa sederhana yang menunjukkan setiap koneksi saluran virtual.
26. Nyatakan kelas layanan ATM mana yang paling baik mendukung setiap aplikasi berikut:
 - A. Email dengan lampiran gambar
 - B. Video interaktif
 - C. Email teks sederhana
 - D. Percakapan suara
27. Bagaimana jaringan area lokal mendukung pengoperasian telepon menggunakan CTI?
28. Jelaskan aplikasi bisnis atau sekolah yang akan mendapat manfaat dari komunikasi terpadu.

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Sebuah perusahaan ingin menghubungkan dua kantor yang berlokasi di Memphis, Tennessee, dan Laramie, Wyoming. Kantor perlu mentransfer data dengan kecepatan 512 kbps. Solusi mana yang lebih murah: sambungan T-1 atau sambungan frame relay?

Apa yang terjadi jika kantor di Baton Rouge, Louisiana, juga harus terhubung ke Memphis dan Laramie dengan kecepatan 512 kbps? Solusi mana yang lebih murah sekarang? Bagaimana jika mempertimbangkan solusi MPLS melalui IP atau bentuk Ethernet jarak jauh?

2. Anda berkonsultasi dengan rumah sakit yang ingin mengirimkan gambar USG berwarna tiga dimensi, resolusi tinggi, antara rumah sakit utama dan klinik rawat jalan. Seorang pasien akan menerima USG di klinik, sementara dokter di rumah sakit utama mengamati gambar tersebut secara real time dan berbicara dengan teknisi USG dan pasien melalui sambungan telepon. Jenis layanan telekomunikasi apa yang disajikan dalam bab ini yang mungkin mendukung penerapan ini? Identifikasi layanan telekomunikasi, dan pastikan untuk mencantumkan rincian khusus mengenai layanan tersebut. Jelaskan alasan Anda.
3. Perusahaan Anda ingin membuat aplikasi yang memungkinkan karyawan melakukan panggilan masuk dari lokasi yang jauh dan, dengan menggunakan satu koneksi, mengakses pesan suara, email, dan file data mereka. Sistem seperti apa yang memungkinkan hal ini? Jelaskan komponen perangkat keras dan perangkat lunak yang diperlukan.
4. Mari kita pertimbangkan skenario Better Box yang disajikan di akhir bab ini. Bagaimana jika kita mempunyai empat situs namun kita menginginkan interkoneksi penuh antara masing-masing pasangan situs? Selanjutnya, kita tidak ingin memasang enam koneksi, namun tetap menggunakan empat koneksi seperti yang disajikan pada bab ini. Untuk melakukan hal ini, kita perlu menjalankan beberapa PVC melalui Chicago. Bisakah ini dilakukan? Jika ya, berapa kapasitas dan biaya yang diperlukan untuk mewujudkan hal ini?
5. Perangkat keras apa yang diperlukan untuk mendukung koneksi T-1 ke bisnis Anda?
6. Teknologi atau teknologi telekomunikasi baru apa yang dapat menggantikan teknologi yang diperkenalkan dalam bab ini? Berikan penjelasan singkat tentang masing-masing teknologi.
7. Dengan menggunakan contoh Better Box Corporation, langkah-langkah lanjutan apa yang diperlukan, dan berapa biaya yang timbul jika langkah-langkah berikut ini dilakukan?
 - A. Akses email untuk semua lokasi
 - B. Kemampuan server internet untuk lokasi Chicago
8. Untuk mengetahui rincian teknis lebih lanjut tentang DSL, selidiki berbagai teknik modulasi yang digunakan untuk mengirimkan sinyal DSL. Meskipun teknik ini cukup rumit, teknik ini merupakan studi menarik tentang kemajuan teknologi yang diperlukan untuk menyediakan aliran data berkecepatan tinggi melalui kabel pasangan terpilin tembaga biasa. Dengan menggunakan sumber internet atau hard copy (yang, jika diperlukan, harus cukup terkini), carilah empat teknologi berikut. Keempatnya digunakan di suatu tempat di sirkuit DSL:
 - Teknologi multinada diskrit (DMT)

- Modulasi fase amplitudo tanpa pembawa (CAP).
- Beberapa jalur virtual (MVL)
- Pembatalan gema

BAB 12

KEAMANAN JARINGAN

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Kenali bentuk dasar serangan sistem
- Kenali konsep yang mendasari tindakan perlindungan fisik
- Sebutkan teknik yang digunakan untuk mengontrol akses ke komputer dan jaringan
- Diskusikan kelebihan dan kelemahan password
- Buat daftar teknik yang digunakan untuk mengamankan data
- Jelaskan perbedaan antara sandi berbasis substitusi dan sandi berbasis transposisi
- Menguraikan fitur dasar kriptografi kunci publik, Standar Enkripsi Lanjutan, tanda tangan digital, dan infrastruktur kunci publik
- Sebutkan teknik yang digunakan untuk mengamankan komunikasi
- Jelaskan perbedaan antara teknik spektrum sebaran frekuensi hopping dan teknik spektrum sebaran urutan langsung
- Mengenali pentingnya firewall dan mampu menjelaskan tiga tipe dasar perlindungan firewall
- Kenali teknik yang digunakan untuk mengamankan komunikasi nirkabel
- Buat daftar keuntungan bagi bisnis jika memiliki kebijakan keamanan

DALAM BEBERAPA tahun TERAKHIR, pengguna komputer dan jaringan komputer telah dibombardir dengan virus komputer. Salah satu virus yang paling merusak, virus Nimda (admin dieja terbalik), diluncurkan pada bulan September 2001. Pakar keamanan internet memperkirakan bahwa Nimda menginfeksi lebih dari 140.000 komputer di Amerika Serikat saja. Virus memasuki komputer pengguna atau server Web melalui email dan halaman Web, membuat akun tingkat administrator, dan menimpa file. Biaya untuk membersihkan virus Nimda diperkirakan melebihi Rp. 26 Triliyun.

Meskipun tahun 2002 merupakan tahun yang relatif tenang bagi virus, tahun 2003 dimulai dengan penuh ledakan. Pada bulan Januari, empat virus baru diluncurkan: Lirva, SoBig, SQL Slammer, dan Yaha. Tiga dari virus ini dengan mudah melewati program email yang sudah dipatch atau dilindungi dan hampir seketika membanjiri Internet dengan jutaan pesan. Sekali lagi, biaya pembersihan diperkirakan mencapai ratusan juta hingga miliaran dolar.

Virus Netsky dan Bagle menyerang pada bulan Maret 2004, diikuti oleh worm Sasser, yang menyerang sistem Windows dengan keras pada bulan Mei 2004. Sejak tahun 2005, perangkat lunak komputer telah mengalami kemajuan dan serangan virus semacam ini jauh lebih jarang terjadi. Sebaliknya, pada tahun 2006 hingga 2011 terjadi serangan baru dalam bentuk phishing, malware, dan botnet.

Apa yang akan terjadi di masa depan? Ketika perusahaan perangkat lunak mengeluarkan tambalan untuk menutupi lubang dan kerentanan dalam perangkat lunak

mereka, semakin banyak lubang dan kerentanan yang ditemukan. Jika tren ini terus berlanjut, uang dan waktu yang dihabiskan untuk melindungi komputer dan memulihkan dari serangan akan terus meningkat pada tingkat yang mengkhawatirkan.

Jenis keamanan data apa saja yang ada saat ini?

Jenis keamanan komunikasi apa saja yang ada saat ini?

Jika Internet tidak mampu melindungi dirinya sendiri, jika ada, apa yang dapat Anda lakukan untuk melindungi diri Anda sendiri saat Anda menggunakan Internet?

12.1 PENDAHULUAN

Keamanan jaringan komputer telah mencapai titik yang dapat dicirikan oleh dua pernyataan yang tampaknya saling bertentangan: Keamanan jaringan belum pernah lebih baik dari sekarang; dan belum pernah ada jaringan komputer yang lebih rentan dibandingkan saat ini. Bagaimana kedua pernyataan ini bisa benar merupakan sebuah paradoks yang menarik. Keamanan jaringan, serta keamanan sistem operasi, telah berkembang pesat sejak awal mula komputer. Selama tahun 1950-an dan 1960-an, keamanan berarti kepercayaan—seorang pengguna komputer memercayai pengguna komputer lain untuk tidak merusak file datanya. Sejak itu, sistem komputer semakin kompleks, dan sistem modern mendukung banyak pengguna secara bersamaan dengan permintaan yang semakin menuntut, seperti pengambilan basis data dan pengunduhan video dan halaman Web yang intensif grafis. Untuk melindungi pengguna satu sama lain, keamanan sistem komputer juga harus semakin kompleks.

Saat ini, Internet memungkinkan siapa pun di dunia untuk mengakses atau mencoba mengakses sistem komputer mana pun yang terhubung ke Internet. Interkonektivitas antara sistem komputer dan jaringan ini merupakan keuntungan sekaligus kerugian. Hal ini memungkinkan kita untuk mengunduh halaman Web dari Eropa dan Asia dan memesan mainan untuk anak-anak (atau diri kita sendiri) dari toko elektronik, namun hal ini juga membuat semua sistem yang terhubung ke Internet rentan terhadap serangan. Dan kenyataannya adalah ada pengguna Internet tertentu yang mempunyai satu tujuan: mengakses sistem terlarang dan mencuri atau menghancurkan apa pun yang bisa mereka dapatkan.

Sistem internet bukan satu-satunya sistem yang mengalami masalah keamanan. Sistem apa pun dengan kemampuan nirkabel juga rentan terhadap vandalisme, seperti halnya pusat perkantoran atau fasilitas pendidikan perusahaan mana pun yang merupakan target potensial bagi seseorang yang ingin masuk dan mencuri atau menghancurkan file komputer. Bahkan membangun tembok setinggi 30 kaki dan membuat parit di sekitar perusahaan Anda serta memutus semua koneksi ke dunia luar tidak akan menciptakan lingkungan yang aman. Faktanya, banyak penelitian menunjukkan bahwa sebagian besar pencurian bisnis dilakukan oleh karyawan yang bekerja di perusahaan tersebut. Membawa pulang flash drive di saku adalah cara yang sangat nyaman (dan mudah) untuk menghapus file data dari jaringan komputer perusahaan. Di lingkungan saat ini, mengelola keamanan jaringan komputer adalah pekerjaan yang menyeluruh dan tidak pernah berakhir.

Pembahasan bab keamanan jaringan ini dimulai dengan mengkaji serangan sistem standar yang diluncurkan terhadap pengguna komputer dan jaringannya. Kami kemudian akan memeriksa empat bidang dasar keamanan jaringan: penerapan perlindungan fisik jaringan dan peralatan komputer, pengendalian akses ke sistem komputer, pengamanan data, dan pengamanan komunikasi. Bab ini kemudian akan diakhiri dengan prinsip dasar pembuatan kebijakan keamanan jaringan.

12.2 SERANGAN SISTEM STANDAR

Akibat banyaknya serangan terhadap komputer dan jaringan dalam beberapa tahun terakhir, banyak penelitian telah dilakukan untuk mencoba menentukan metode standar serangan sistem. Dua metode serangan populer selama beberapa tahun terakhir telah mengeksploitasi kerentanan yang diketahui dalam sistem operasi dan perangkat lunak aplikasi. Dengan menggunakan Internet dan terkadang kerentanan browser, peretas akan menghabiskan waktu berjam-jam untuk menggali sistem operasi dan perangkat lunak aplikasi populer dalam upaya menemukan celah. Setelah celah ini ditemukan, peretas akan melancarkan serangan yang membahayakan komputer host atau server jaringan. Seringkali, perusahaan yang membuat dan mendukung sistem operasi atau aplikasi yang disusupi akan mengeluarkan patch, yaitu perangkat lunak perbaikan yang dirancang untuk menutup kerentanan. Sayangnya, tidak semua pemilik dan operator komputer menginstal patch tersebut, atau, lebih buruk lagi, patch itu sendiri mungkin memiliki kerentanan tambahan. Menariknya, banyak peretas menunggu hingga perusahaan mengumumkan peluncuran patch. Setelah kerentanan diketahui, peretas membuat kode untuk memanfaatkan kerentanan tersebut, karena mengetahui bahwa banyak perusahaan dan pengguna akan lambat dalam menginstal patch, jika mereka menginstalnya.

Dalam kedua jenis serangan ini, pelaku dapat memperoleh akses ke sistem pengguna melalui beberapa cara. Salah satu teknik yang sangat umum adalah mengirimkan email atau halaman Web yang berisi potongan kode berbahaya yang disebut kode berbahaya seluler atau Trojan horse, karena kode tersebut bersembunyi di dalam potongan kode yang tampak tidak berbahaya. Setelah pengguna membaca email dan membuka lampirannya, kuda Troya dilepaskan, dan kerusakan terjadi. Banyak orang menganggap kuda Troya sebagai salah satu bentuk virus komputer. Virus komputer adalah program kecil yang mengubah cara komputer beroperasi tanpa sepengetahuan pengguna komputer dan sering melakukan berbagai jenis kerusakan dengan menghapus dan merusak data dan file program, atau dengan mengubah komponen sistem operasi, sehingga pengoperasian komputer tidak berjalan dengan baik. terganggu atau bahkan terhenti. Baru-baru ini, program jahat yang mengambil alih operasi pada komputer yang disusupi disebut botnet.

Beberapa jenis virus lainnya antara lain:

- *Virus makro*—Jenis virus umum yang diprogram ke dalam file makro terlampir. Makro sering ditemukan dalam spreadsheet, database, dan dokumen pengolah kata. Virus makro bersembunyi di dalam makro aplikasi dan diaktifkan saat makro dijalankan.

- *Virus boot sector*—Salah satu bentuk virus asli, virus boot sector biasanya disimpan pada beberapa bentuk media yang dapat dipindahkan. Ketika media yang dapat dilepas terhubung ke mesin baru dan digunakan untuk mem-boot mesin, virus berpindah dari media ke sistem host. Versi yang lebih baru tidak perlu di-boot; mereka hanya harus berada di media yang dapat dipindahkan, seperti pada flash drive.
- *Virus polimorfik*—Virus ini bermutasi pada setiap infeksi, sehingga sulit ditemukan lokasinya.
- *Virus infector file*—Virus yang menginfeksi bagian kode yang dapat dieksekusi seperti file .exe atau .com. Ketika program dijalankan, baik dari disk atau melalui jaringan, komputer host terinfeksi.

Bentuk lain dari virus komputer adalah worm. Worm komputer adalah program yang menyalin dirinya dari satu sistem ke sistem lain melalui jaringan, tanpa bantuan manusia. Worm biasanya menyebarkan dirinya dengan cara berpindah dari komputer ke komputer melalui email. Biasanya, virus atau worm diangkut sebagai kuda Trojan—dengan kata lain, bersembunyi di dalam potongan kode yang tampak tidak berbahaya seperti email atau makro aplikasi.

Beberapa serangan sistem bahkan tidak memerlukan pengguna untuk membuka email atau halaman Web sama sekali. Yang harus dilakukan pengguna untuk terinfeksi adalah terhubung ke Internet. Saat terhubung, komputer pengguna selalu rentan terhadap program perangkat lunak berbahaya di Internet yang memindai komputer yang tidak terlindungi (port TCP terbuka) dan mencoba mengeksploitasi kerentanan sistem operasi dan aplikasi yang diketahui. Kecuali jika pengguna menginstal perangkat lunak perlindungan virus terbaru di komputernya, komputer tersebut kemungkinan besar telah disusupi.

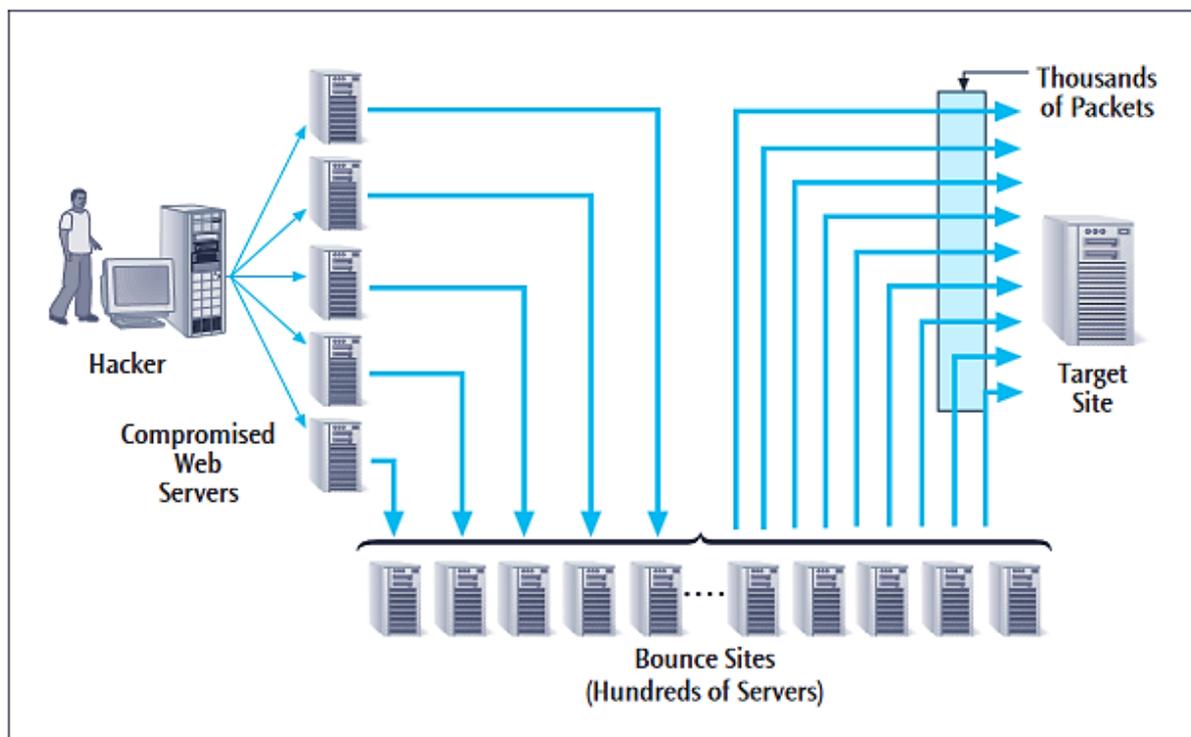
Kategori umum serangan sistem lainnya yang menjadi populer pada akhir abad ke-20 adalah serangan penolakan layanan. Serangan penolakan layanan (atau serangan penolakan layanan terdistribusi) membombardir situs komputer dengan begitu banyak pesan sehingga situs tersebut tidak mampu menjalankan tugas normalnya. Beberapa jenis penolakan layanan yang umum termasuk pemboman email, smurfing, dan badai ping. Dalam pemboman email, pelaku mengirimkan pesan email yang tidak diinginkan dalam jumlah berlebihan kepada seseorang. Jika pesan email ini memiliki alamat pengirim orang lain selain orang yang sebenarnya mengirim email, maka pengirimnya melakukan spoofing.

Smurfing adalah nama program otomatis jahat yang menyerang jaringan dengan memanfaatkan pengalamatan siaran Protokol Internet (IP) dan aspek lain dari operasi Internet. Sederhananya, seorang penyerang mengirimkan sebuah paket ke pihak ketiga yang tidak bersalah—yaitu “penguat”—yang kemudian tanpa sadar mengalikan paket tersebut ratusan atau ribuan kali dan mengirimkan salinannya ke korban yang dituju.

Ping adalah alat Internet umum yang digunakan untuk memverifikasi apakah alamat IP tertentu dari suatu host ada, dan untuk melihat apakah host tertentu saat ini tersedia. Ping paling sering digunakan oleh sistem berbasis Unix, yang banyak digunakan untuk mendukung server Web Internet. Badai ping adalah suatu kondisi di mana program ping Internet digunakan untuk mengirimkan banyak paket ke server sehingga server tidak dapat

dioperasikan. Sebagai contoh spoofing dan badai ping, mari kita perhatikan serangan penolakan layanan yang melanda sejumlah situs web komersial pada awal Februari 2000. Situs yang diserang termasuk situs populer seperti Yahoo!, eBay, Amazon, CNN, dan Dalam satu jenis serangan, seorang hacker entah bagaimana mengambil kendali sejumlah server di Internet dan memerintahkan mereka untuk melakukan kontak dengan server Web tertentu (server yang ingin dinonaktifkan oleh peretas). Server yang disusupi mengirimkan paket TCP/IP SYN (sinkronisasi/inisialisasi) dengan alamat IP sumber palsu (spoofing) ke target yang dituju. Ketika setiap paket SYN tiba, server target mencoba memberikan respons yang sah tetapi tidak bisa karena alamat IP palsu. Sementara server target menunggu respons dari alamat IP palsu, sumber dayanya dikonsumsi karena semakin banyak perintah SYN palsu yang masuk.

Untuk melihat cara kerja serangan penolakan layanan, perhatikan contoh berikut. Peretas menginstruksikan sejumlah server Web yang disusupi (server zombie) untuk mengirim paket ke server kedua (lihat Gambar 12-1). Paket-paket ini berisi alamat tujuan situs Web target. Kumpulan server kedua, yang disebut situs bouncing, menerima beberapa permintaan palsu dan merespons dengan mengirimkan beberapa paket ke situs Web target pada saat yang bersamaan. Situs target kemudian kewalahan dan lumpuh karena membanjirnya paket-paket tidak sah, sehingga tidak ada ruang bagi paket-paket sah.



Gambar 12-1 Contoh serangan penolakan layanan yang dimaksudkan untuk melumpuhkan server Web

Metode serangan populer lainnya adalah menyalahgunakan atau memanfaatkan akun pengguna yang valid dan izin yang terkait dengan akun tersebut. Misalnya, pengguna di

sebuah perusahaan atau perguruan tinggi yang memiliki akun yang valid akan mencoba mengakses dokumen terlarang, mengunggah file dan kumpulan data yang tidak sah, menggunakan jaringan perusahaan sebagai situs untuk serangan Web dan email ilegal, atau sekadar mencoba mengelilingi fitur keamanan sistem dalam upaya mengakses layanan terlarang.

Satu lagi metode serangan yang umum adalah mencoba menebak atau mencegat ID dan kata sandi yang valid dari pengguna yang berwenang. Peretas akan mencoba mencuri kata sandi dengan menebak kombinasi sederhana atau menguping transmisi yang mengirimkan kata sandi. Beberapa peretas bahkan sampai membuat aplikasi yang tampak sah dan meminta ID dan kata sandi kepada pengguna. Begitu seseorang memasukkan ID dan kata sandinya, perangkat lunak akan menampilkan pesan yang memberikan kesan kegagalan sistem. Pengguna melanjutkan, tanpa mengetahui bahwa ID dan kata sandinya baru saja diteruskan ke program palsu. Dalam beberapa tahun terakhir, ada sejumlah upaya untuk mencuri ID dan kata sandi. Dalam beberapa kasus, peretas membuat email yang tampaknya merupakan permintaan sah yang berasal dari perusahaan terkenal. Email tersebut bahkan menyertakan logo dan lambang perusahaan yang tampak resmi. Dalam email tersebut, pengguna yang tidak menaruh curiga diminta untuk memberikan informasi pribadi seperti nomor Jaminan Sosial atau nomor kartu kredit. Peretas akan mengumpulkan informasi pribadi ini dan menggunakannya secara ilegal untuk membeli barang atau, lebih buruk lagi, melakukan pencurian identitas. Jenis serangan ini disebut phishing.

Jenis serangan lain yang melibatkan penipuan pengguna agar memberikan informasi rahasia disebut pharming. Dalam serangan ini, pengguna Web yang ingin mengunjungi situs Web perusahaan tertentu tanpa sadar diarahkan ke situs Web palsu yang terlihat persis seperti situs Web resmi perusahaan tersebut. Tanpa mengetahui bahwa ia mengunjungi situs Web palsu, pengguna dapat memasukkan informasi rahasia untuk mendaftar suatu layanan atau melakukan pembelian, yang kemudian dapat dicuri.

Dua alat lagi yang digunakan oleh pengguna jahat adalah rootkit dan keylogger. Rootkit adalah sebuah program atau program yang telah terinstal (biasanya tanpa disadari) di sistem operasi pengguna. Mereka dipasang jauh di dalam sistem operasi sehingga perangkat lunak perlindungan normal bahkan tidak memperhatikan rootkit, sehingga menjadikannya bentuk serangan yang sangat manipulatif. Dengan adanya rootkit, komputer pengguna pada dasarnya dapat diambil alih oleh pengguna jarak jauh. Meskipun beberapa rootkit sebenarnya berguna dan dapat membantu mengatasi masalah komputer, sebagian besar rootkit dimaksudkan untuk bersifat merusak. Keylogger adalah sistem perangkat lunak yang berjalan di komputer, dan menangkap serta mencatat semua penekanan tombol yang dilakukan pada keyboard. Ini bisa menjadi program yang berguna bagi seseorang yang ingin memantau kemajuan pengguna komputer dalam suatu tugas tertentu. Sayangnya, ini juga dapat digunakan untuk menangkap ID pengguna dan kata sandi seseorang, atau informasi pribadi lainnya. Beberapa perusahaan juga menggunakan keylogger untuk memantau produktivitas atau kebiasaan karyawannya. Penggunaan semacam ini bisa baik atau buruk tergantung pada kerangka acuan Anda.

Profesional yang mendukung jaringan komputer, serta pengguna komputer individu yang memiliki komputer di rumah atau kantor, perlu menyadari serangan umum ini sehingga mereka dapat memutuskan cara terbaik untuk melindungi sistem mereka dari vandalisme dan intrusi.

Sekarang setelah kita memahami beberapa serangan sistem yang lebih umum, mari kita selidiki apa yang dapat kita lakukan untuk mencegahnya. Kita akan mulai dengan memeriksa apa yang dapat kita lakukan untuk melindungi peralatan dan data kita secara fisik.

12.3 PERLINDUNGAN FISIK

Perlindungan fisik suatu sistem komputer atau jaringan komputer terdiri dari perlindungan peralatan dari kerusakan fisik. Penyebab kerusakan fisik antara lain kebakaran, banjir, gempa bumi, lonjakan listrik, dan vandalisme. Dalam banyak kasus, teknik untuk mencegah kerusakan merupakan hal yang masuk akal. Misalnya, ruangan yang berisi peralatan komputer harus selalu dikunci, dan orang yang tidak berwenang tidak boleh memasukinya. Jika memungkinkan, kabel dan perangkat yang dihubungkan dengan kabel tidak boleh dibiarkan terbuka.

Tentu saja, beberapa peralatan harus ditempatkan di tempat terbuka agar dapat diakses publik. Dalam hal ini, peralatan harus dikunci. Ada banyak jenis perangkat anti maling untuk mengunci lemari, mengunci kabel ke lemari, dan mengunci keyboard serta perangkat periferal lainnya. Misalnya, salah satu perangkat tersebut mengirimkan sinyal nirkabel ke pager setiap kali lemari komputer dibuka. Dengan cara ini, orang yang membawa pager akan segera mengetahui kapan lemari dibuka, dan lemari mana yang dibuka; dia kemudian dapat mengarahkan personel keamanan ke lokasi yang sesuai.

Hal lain yang masuk akal adalah bahwa sistem komputer yang mahal tidak boleh ditempatkan di ruang bawah tanah gedung. Ruang bawah tanah bisa banjir dan sering kali merupakan lokasi dengan kelembapan tinggi. Kamar dengan banyak jendela luar juga tidak disarankan. Jendela dapat membiarkan sinar matahari masuk, yang dapat meningkatkan suhu ruangan. Peralatan komputer sendiri diketahui dapat memanaskan ruangan. Dengan bertambahnya sinar matahari, peningkatan suhu dapat membebani kapasitas sistem pendingin udara (jika ada). Ketika suhu meningkat, harapan hidup sirkuit komputer menurun. Ruang dengan banyak jendela eksternal juga harus dihindari karena lebih rentan terhadap pembobolan—dan juga vandalisme atau pencurian.

Untuk mencegah kerusakan listrik pada peralatan komputasi, pelindung lonjakan arus berkualitas tinggi harus digunakan pada semua perangkat yang memerlukan arus listrik. Sirkuit listrik yang menyediakan daya ke perangkat harus cukup besar untuk menopang perangkat tersebut tanpa memberikan beban pada sistem kelistrikan. Selain itu, perangkat komputer tidak boleh berada pada sirkuit yang sama dengan perangkat listrik yang dayanya naik turun dan menyebabkan fluktuasi daya, seperti motor besar. Terakhir, perangkat yang rentan terhadap kerusakan akibat pelepasan listrik statis, seperti kartu memori dan papan sirkuit tercetak, harus diarde dengan benar. Pengawasan juga dapat dianggap sebagai bentuk perlindungan fisik.

Meskipun banyak karyawan merasa pengawasan merupakan gangguan terhadap privasi mereka, banyak administrator jaringan menganggapnya sebagai pencegahan yang baik terhadap vandalisme dan pencurian komputer. Penempatan kamera video di lokasi-lokasi penting dapat mencegah penjahat dan digunakan untuk mengidentifikasi penjahat jika terjadi vandalisme atau pencurian.

Bentuk pengawasan lain dapat digunakan selain pengambilan video langsung dengan kamera. Misalnya, perusahaan yang menerima pesanan barang dagangan melalui telepon sering kali memantau setiap panggilan telepon. Perusahaan mengklaim bentuk pengawasan ini dapat meningkatkan kualitas layanan pelanggan dan membantu menyelesaikan perselisihan di masa depan. Contoh lain, beberapa perusahaan menggunakan bentuk pengawasan yang disebut deteksi intrusi, atau sistem deteksi intrusi, yang melibatkan pemantauan aliran data dan permintaan sistem yang masuk dan keluar dari sistem mereka secara elektronik. Jika terdapat aktivitas yang tidak biasa, tindakan perlindungan dapat segera diambil. Deteksi intrusi adalah bidang studi yang berkembang dalam keamanan jaringan. Deteksi intrusi dan pengawasan merupakan bidang perlindungan fisik yang penting.

Selain pengawasan video dan deteksi intrusi, ada teknik pengawasan menarik yang dibangun berdasarkan konsep honeypot. Dalam terminologi komputer, honeypot adalah jebakan yang dipasang oleh personel jaringan untuk mendeteksi penggunaan sumber daya jaringan yang tidak sah. Biasanya, honeypot adalah lokasi jaringan yang tampaknya menjadi bagian dari sumber daya perusahaan dan berisi data yang mungkin menarik atau berharga bagi peretas. Faktanya, data ini palsu dan dimaksudkan untuk menggoda peretas agar melakukan pembobolan. Perusahaan yang menerapkan teknik ini biasanya menjaga pengawasan terhadap honeypot, sehingga dapat mengamati tindakan calon peretas. Pada dasarnya, honeypot dapat berfungsi sebagai alat peringatan dini, namun perusahaan harus menyadari bahwa penggunaan honeypot untuk tujuan lain (seperti memikat calon peretas untuk melakukan kejahatan) seringkali dipertanyakan etis dan bahkan mungkin ilegal.

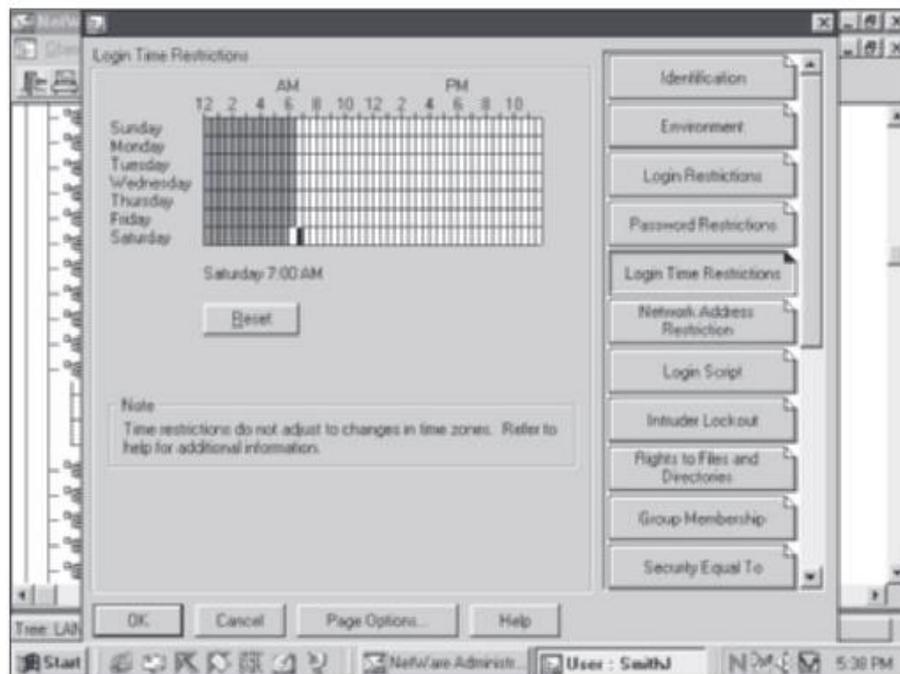
12.4 MENGONTROL AKSES

Mengontrol akses ke jaringan komputer melibatkan pengambilan keputusan dan kemudian membatasi siapa yang dapat menggunakan sistem dan kapan sistem dapat digunakan. Bayangkan sebuah perusahaan besar yang mempunyai banyak tingkatan karyawan dengan deskripsi pekerjaan yang berbeda-beda. Karyawan yang tidak perlu melakukan kontak dengan data sensitif tidak boleh memiliki akses ke tingkat data tersebut. Misalnya, jika seorang karyawan hanya melakukan operasi entri data, dia mungkin tidak boleh mengakses informasi penggajian. Demikian pula, karyawan yang bekerja di bidang penggajian memerlukan akses ke database penggajian, namun kemungkinan besar, mereka tidak memerlukan akses terhadap informasi mengenai program penelitian perusahaan. Seorang manajer di suatu area mungkin memiliki akses terhadap banyak informasi di departemennya, namun akses manajer terhadap informasi di departemen lain mungkin harus dibatasi. Terakhir, eksekutif tingkat atas sering kali memiliki akses terhadap berbagai informasi dalam

suatu perusahaan. Namun ada banyak perusahaan yang dengan bijak membatasi kemampuan akses informasi bahkan manajemen tingkat atas sekalipun.

Jaringan area lokal dan sistem basis data memberikan banyak fleksibilitas dalam pemberian hak akses kepada individu atau kelompok individu, seperti yang akan Anda lihat segera. Hak akses menentukan sumber daya jaringan yang dapat diakses oleh pengguna atau sekelompok pengguna. Spesialis jaringan komputer suatu perusahaan, bersama dengan administrator basis data dan seseorang di tingkat manajemen tertinggi, seperti chief information officer (CIO), sering bekerja sama untuk memutuskan bagaimana perusahaan harus dipecah menjadi kelompok akses informasi. Kemudian mereka menyelesaikan hak akses masing-masing kelompok dan menentukan siapa yang harus berada di setiap kelompok. Seperti yang mungkin Anda ingat dari Bab Delapan, sistem operasi jaringan, seperti Windows Server, bisa sangat berguna dalam tugas membuat kelompok kerja dan menetapkan hak akses.

Dimungkinkan juga untuk membatasi akses ke sistem berdasarkan waktu atau hari dalam seminggu. Jika aktivitas utama di salah satu bagian bisnis Anda adalah mengakses catatan personalia, dan aktivitas ini hanya dilakukan selama jam kerja oleh karyawan di departemen personalia atau sumber daya manusia, maka masuk akal untuk menonaktifkan akses ke catatan personalia setelah jam kerja. —misalnya, mulai pukul 17.30. sampai jam 7 pagi keesokan harinya. Administrator jaringan juga dapat menolak akses ke sistem ini pada akhir pekan. Gambar 12-2 menunjukkan contoh kotak dialog sistem operasi jaringan yang digunakan administrator untuk menetapkan batas akses pengguna dalam jaringan.



Gambar 12-2 Contoh kotak dialog dari sistem operasi jaringan untuk menetapkan batasan waktu

Mungkin juga bijaksana untuk membatasi akses jarak jauh ke suatu sistem pada waktu-waktu tertentu dalam sehari atau seminggu. Salah satu alasannya adalah untuk mencegah seseorang menelepon pada pukul 02.30 untuk melakukan aktivitas ilegal, seperti mentransfer dana dari satu rekening ke rekening lainnya. Mengingat kemungkinan-kemungkinan tersebut, adalah wajar bagi perusahaan untuk melindungi diri mereka sendiri dengan memutuskan bahwa transfer dana perusahaan hanya dapat dilakukan selama jam kerja tertentu dan membatasi aktivitas panggilan masuk pada jam-jam tersebut.

Salah satu cara paling umum untuk mengontrol akses ke suatu sistem adalah dengan meminta ID pengguna dan kata sandi, meskipun teknik ini memiliki sejumlah kelemahan. Mari kita periksa kata sandi dan sistem ID lainnya secara lebih rinci.

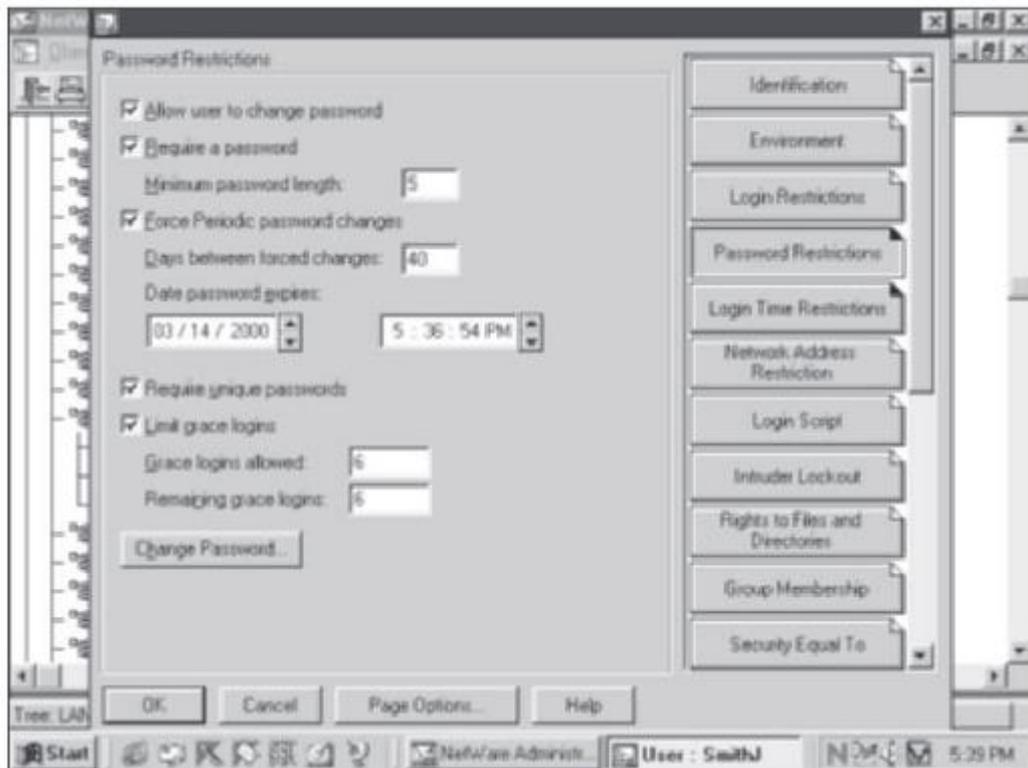
Kata sandi dan sistem ID

Saat ini, hampir setiap sistem yang menyimpan data sensitif atau rahasia memerlukan pengguna yang berwenang untuk memasukkan kata sandi, nomor identifikasi pribadi (PIN), atau bentuk ID lainnya sebelum mendapatkan akses ke sistem. Biasanya, kata sandi atau ID ini berupa rangkaian karakter yang harus diingat pengguna atau fitur fisik pengguna, seperti sidik jari. Teknologi di bidang manajemen identitas berkembang pesat seiring dengan upaya perusahaan untuk menerapkan sistem yang tidak terlalu rentan terhadap penipuan.

Mungkin bentuk perlindungan yang paling umum terhadap penggunaan sistem komputer yang tidak sah adalah kata sandi. Siapa pun yang mengakses sistem komputer, sistem perbankan, atau sistem pesan suara/email wajib memasukkan kata sandi atau PIN. Meskipun kata sandi adalah bentuk identifikasi yang paling umum, kata sandi juga merupakan salah satu bentuk perlindungan terlemah. Seringkali, kata sandi diketahui, atau “salah tempat”, dan jatuh ke tangan yang salah. Kadang-kadang, kata sandi ditulis di atas kertas, dan kertas tersebut ditemukan oleh orang yang salah. Namun, seringkali kata sandinya terlalu sederhana dan penyusup dapat menebaknya. Aturan standar yang harus dipatuhi seseorang saat membuat atau mengubah kata sandi meliputi:

- Ubah kata sandi Anda sesering mungkin.
- Pilih kata sandi yang baik dengan menggunakan setidaknya delapan karakter, campur huruf besar dan kecil jika sistem komputer peka terhadap huruf besar-kecil, dan campur huruf dengan angka.
- Jangan memilih kata sandi yang mirip dengan nama depan atau belakang, nama hewan peliharaan, nama mobil, atau pilihan lain yang mudah ditebak.
- Jangan membagikan kata sandi Anda kepada orang lain; melakukan hal itu akan mengundang masalah dan penyalahgunaan.

Gambar 12-3 menunjukkan bagaimana sistem operasi jaringan pada umumnya memungkinkan administrator jaringan untuk meminta pengguna menggunakan kata sandi, memberikan pengguna kemampuan untuk mengubah kata sandinya sendiri, dan mengharuskan pengguna untuk memilih kata sandi dengan ukuran tertentu.



Gambar 12-3 Mengontrol kata sandi pengguna dengan sistem operasi jaringan pada umumnya

Beberapa sistem komputer menghasilkan kata sandi acak yang sangat sulit ditebak, namun juga sulit untuk diingat. Seringkali, pengguna yang diberi kata sandi yang dibuat secara acak akan mengubahnya menjadi sesuatu yang lebih sederhana, yang membuat kata sandi lebih mudah ditebak, atau menuliskan kata sandi di selembar kertas, yang menggagalkan seluruh tujuan memiliki kata sandi rahasia. Beberapa sistem tidak mengizinkan kata sandi yang jelas atau kata sandi yang sudah digunakan, sehingga mengharuskan pengguna untuk kreatif dan memilih kata sandi yang sulit ditebak.

Kekeliruan umum di kalangan pengguna sistem komputer adalah bahwa file sistem operasi internal yang menyimpan ID login dan kata sandi rentan terhadap intrusi. Menariknya, banyak sistem komputer menyimpan kata sandi dalam bentuk terenkripsi yang tidak diketahui dekripsinya. Lalu bagaimana sistem mengetahui jika Anda telah memasukkan kata sandi yang benar? Ketika pengguna memasukkan ID login dan kata sandinya, kata sandi tersebut dienkripsi dan dibandingkan dengan entri dalam file kata sandi terenkripsi. Jika kedua kata sandi terenkripsi cocok, login diperbolehkan. Siapa pun yang mendapat akses ke file kata sandi terenkripsi ini hanya akan menemukan teks yang tidak dapat dibaca. Teknik enkripsi ini menjadi alasan mengapa, ketika Anda lupa kata sandi, operator komputer tidak bisa begitu saja membaca file dan memberi tahu Anda apa file tersebut. Operator komputer hanya dapat mereset kata sandi ke sesuatu yang baru.

Karena banyaknya kelemahan pada kata sandi, maka muncullah bentuk identifikasi lain. Teknik biometrik yang mengamati dan merekam beberapa aspek pengguna, seperti sidik

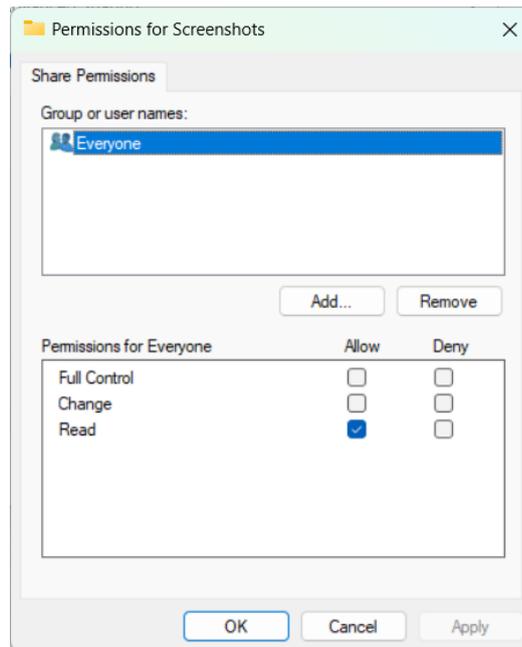
jari, sidik jari, sidik mata, dan sidik wajah, tampaknya semakin populer. Misalnya, Inggris memiliki database sidik jari yang besar. Penelitian menunjukkan bahwa tidak ada dua telinga yang sama; oleh karena itu, sidik jari berguna dalam membantu mengidentifikasi seseorang. Tentu saja, sidik jari telah lama digunakan untuk membedakan seseorang dengan orang lain. Kini, beberapa komputer laptop memiliki pemindai sidik jari internal yang dapat memindai sidik jari pengguna dan membolehkan atau melarang pengguna mengakses sistem komputer. Tersedia juga sistem yang dapat merekam dan mendigitalkan suara Anda. Pola suara digital dibandingkan dengan sampel yang disimpan, dan perangkat lunak menentukan apakah kecocokannya cukup dekat untuk validasi. Pemindaian retina (retina adalah bagian dalam lapisan belakang mata) umumnya ditampilkan dalam film dan memang ada di dunia nyata sebagai teknik keamanan, meskipun pada tingkat kecil karena kerumitan dan biayanya. Hambatan lainnya adalah orang-orang merasa mual ketika diberi tahu bahwa laser akan memindai bagian dalam bola mata mereka. Bagian lain dari mata yang unik di antara semua individu adalah iris, atau bagian mata yang berwarna. Beberapa perangkat keamanan menggunakan iris untuk mengidentifikasi orang yang diizinkan mengakses sistem tertentu. Karena teknologi yang dibutuhkan untuk melakukan pemindaian iris mata lebih murah dibandingkan teknologi pemindaian retina, kemungkinan besar kita akan melihat pemindaian iris mata dilakukan dalam waktu dekat.

Penelitian lain di bidang teknik biometrik ditujukan untuk mendigitalkan fitur seluruh wajah dan membandingkan representasi digital ini dengan gambar yang disimpan. Perusahaan-perusahaan yang memproduksi anjungan tunai mandiri (ATM) 24 jam tertarik untuk mengganti kartu ATM seukuran kartu kredit beserta PIN yang bersangkutan dengan sesuatu yang tidak mudah dicuri, seperti sidik jari, sidik wajah, atau sidik mata. Untuk meningkatkan keamanannya, banyak perusahaan memerlukan kombinasi bentuk identifikasi, seperti kata sandi dan sidik jari.

Hak akses

Sistem komputer modern dan jaringan komputer memungkinkan banyak pengguna mengakses sumber daya seperti file, kaset, printer, dan perangkat periferal lainnya. Namun sering kali, berbagai sumber daya dalam sebuah organisasi tidak seharusnya dibagikan, atau sumber daya tersebut hanya boleh dibagikan kepada kelompok tertentu saja. Jika pembagian sumber daya dibatasi, maka pengguna atau administrator jaringan harus menetapkan hak akses yang sesuai untuk sumber daya tertentu. Kebanyakan hak akses mempunyai dua parameter dasar: siapa dan bagaimana. Parameter *who* mencantumkan siapa yang memiliki hak akses ke sumber daya. Contoh umum yang mencakup pemilik, sekelompok pengguna tertentu, dan seluruh populasi pengguna. Parameter *bagaimana* dapat menentukan bagaimana pengguna dapat mengakses sumber daya, dan hak terdaftar sebagai RWX, untuk membaca, menulis, dan mengeksekusi. Lebih tepatnya, R mencakup hak baca dan cetak; W mencakup hak menulis, mengedit, menambahkan, dan menghapus; dan X berarti mengeksekusi, atau menjalankan. Saat pengguna membuat file, default sistem yang biasa mungkin memberi pengguna akses baca, tulis, dan eksekusi penuh (atau SEMUA), sehingga dia dapat mengubah atau menghapus file kapan saja. Pengguna atau pemilik ini dapat

mengizinkan pengguna lain untuk mengakses file, namun dapat membatasi mereka untuk memiliki hak akses baca saja. Gambar 12-4 menunjukkan contoh bagaimana sistem operasi jaringan memberikan hak akses ke suatu sumber daya. Seperti yang Anda lihat pada gambar, administrator jaringan dapat menggunakan aplikasi ini untuk menetapkan pengawas, membaca, menulis, membuat, menghapus, memodifikasi, memindai file, dan hak kontrol akses kepada pengguna tertentu.



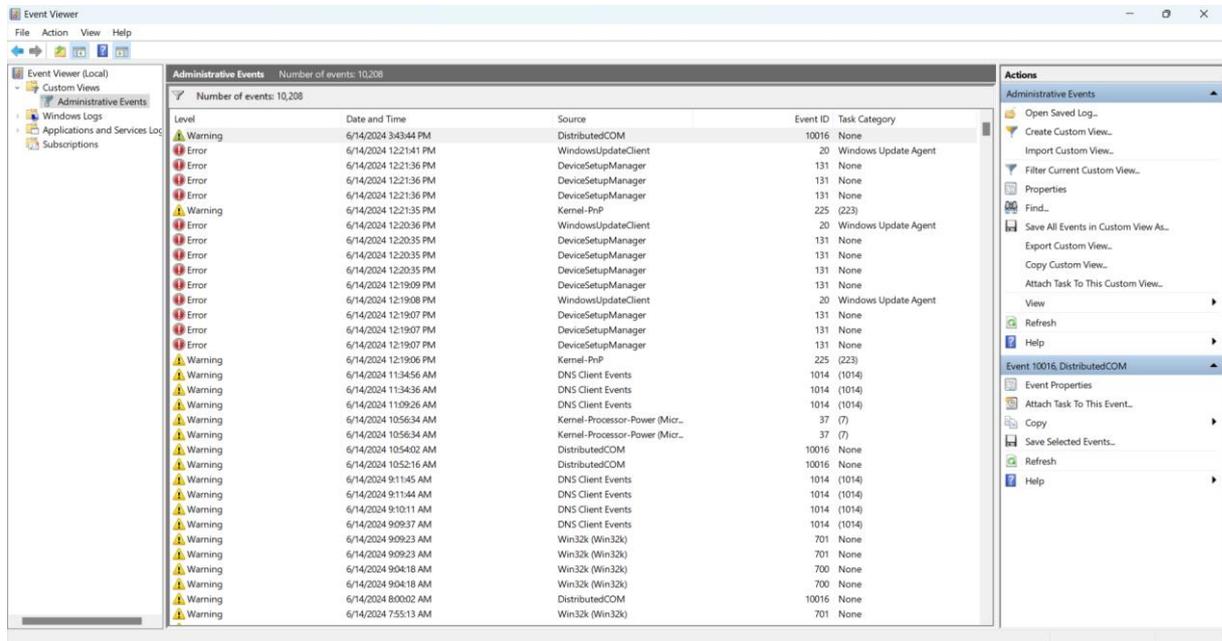
Gambar 12-4 Sistem operasi jaringan yang memberikan hak akses ke sumber daya

Sistem operasi jaringan modern memungkinkan administrator jaringan membuat kelompok kerja. Kelompok kerja ini ditentukan oleh administrator jaringan dan dapat berisi segala bentuk pengelompokan pengguna yang diinginkan. Misalnya, satu kelompok kerja mungkin terdiri dari seluruh karyawan bagian pemasaran dan teknik yang sedang mengerjakan proyek tertentu. Setelah kelompok kerja ditentukan, maka dimungkinkan untuk menetapkan seperangkat hak akses yang unik kepada kelompok kerja ini.

Audit

Mengaudit sistem komputer seringkali merupakan cara yang baik untuk mencegah kejahatan dan juga berguna dalam menangkap penjahat setelah kejahatan dilakukan. Audit komputer biasanya melibatkan program perangkat lunak yang memantau setiap transaksi dalam suatu sistem. Setiap transaksi terjadi, dicatat ke dalam log elektronik beserta tanggal, waktu, dan “pemilik” transaksi tersebut. Jika suatu transaksi dicurigai tidak pantas, log elektronik dipindai dan informasi ini diambil. Dalam kasus klasik kejahatan komputer yang dapat digagalkan melalui audit, seorang warga New York menemukan bahwa ketika tagihan dengan jumlah di bawah \$500 dikirim ke lembaga pemerintah setempat, tagihan tersebut akan dibayar secara rutin tanpa permintaan rincian lebih lanjut. Berbekal pengetahuan ini, dia membuat fakturnya sendiri dan mengirimkannya ke lembaga-lembaga pemerintah tersebut. Sesuai dengan bentuknya, agen-agen tersebut membayar tagihannya, dan rekening

tabungannya bertambah. Namun beberapa bulan kemudian, seorang pengacara yang memeriksa jejak audit komputer atas pembayaran tersebut memperhatikan bahwa ada pola cek (semuanya di bawah Rp. 5.000.000) yang dikirim ke individu yang sama.



Gambar 12-5 Contoh Windows Event Viewer

Gambar 12-5 menunjukkan contoh log audit dari jendela Peraga Peristiwa sistem operasi Windows. Perhatikan bahwa untuk setiap transaksi (atau peristiwa), tanggal, waktu, dan sumber peristiwa dicatat. Peristiwa yang direkam secara umum mencakup kegagalan memuat driver atau komponen sistem lainnya saat startup sistem, kemungkinan pelanggaran keamanan, dan program apa pun yang mungkin mencatat kesalahan saat mencoba melakukan operasi file.

Tersedia banyak program komputer bagus yang dapat mengaudit semua transaksi yang terjadi pada sistem komputer. Uang yang dikeluarkan untuk membeli, memasang, dan mendukung program audit mungkin merupakan investasi yang baik jika program tersebut membantu menangkap seseorang yang melakukan transaksi tidak sah.

12.5 MENGAMANKAN DATA

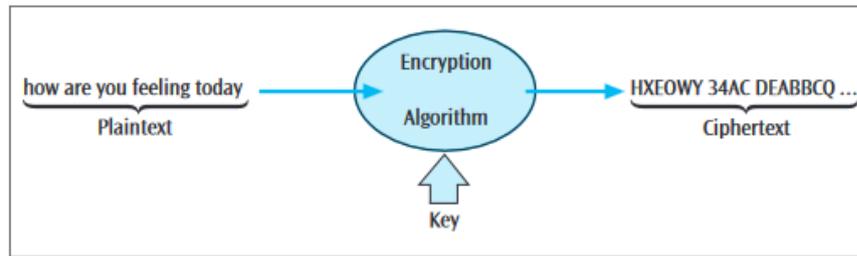
Sistem komputer menyimpan dan memanipulasi data, sedangkan sistem komunikasi mentransfer data. Tindakan pencegahan apa yang dapat kita ambil untuk memastikan bahwa data ini tidak dirusak atau disadap oleh orang yang salah? Mari kita periksa beberapa teknik yang dapat digunakan untuk membuat data lebih aman. Kami akan mulai dengan memperkenalkan teknik dasar yang digunakan untuk mengenkripsi dan mendekripsi data. Kemudian kita akan melihat beberapa teknik terkini yang digunakan untuk mengamankan data, seperti Standar Enkripsi Lanjutan, tanda tangan digital, infrastruktur kunci publik, dan steganografi.

Teknik enkripsi dan dekripsi dasar

Ketika pengguna mentransfer data dari satu titik ke titik lain dalam jaringan komputer, sering kali perlu untuk memastikan bahwa transmisi tersebut aman dari siapa pun yang mungkin menguping saluran tersebut. Istilah “aman” berarti dua hal. Pertama, tidak boleh ada orang yang mencegat dan menyalin transmisi yang sudah ada. Kedua, tidak boleh ada orang yang memasukkan informasi palsu ke dalam transmisi yang sudah ada. Transaksi keuangan dan komunikasi militer adalah dua contoh data yang baik yang harus diamankan selama transmisi.

Kabel serat optik menunjukkan peningkatan besar dalam kemampuan media transmisi untuk mengamankan data sensitif. Seperti yang mungkin Anda ingat dari Bab Tiga, media logam seperti kabel twisted pair dan kabel koaksial dapat menghantarkan sinyal listrik sehingga relatif mudah untuk disadap, namun kabel serat optik jauh lebih sulit untuk disadap karena kabel tersebut mengirimkan pulsa cahaya, yaitu bukan elektromagnetik. Untuk menyadap sistem serat optik secara ilegal, Anda harus memutus kabel serat optik secara fisik—sebuah gangguan yang akan segera diketahui—atau Anda harus mendapatkan akses ke kotak sambungan serat optik, yang biasanya berada di lokasi terkunci.

Terlepas dari seberapa aman media komputer tertentu, data dalam sistem tetap rentan karena suatu saat dalam masa pakainya, data tersebut mungkin akan dipindahkan melalui komputer lain (yang kurang aman), disimpan di hard disk drive yang tidak dikenal/tidak terlindungi, dan/atau ditransmisikan melalui sistem telepon standar—dengan kata lain, data dapat disadap atau dicuri dari sistem lain. Mengingat risiko-risiko ini, data sensitif memerlukan langkah-langkah keamanan tambahan. Salah satu tindakan tambahan tersebut adalah dengan menggunakan perangkat lunak enkripsi untuk mengenkripsi data sebelum dikirimkan, mengirimkan data terenkripsi melalui media aman, dan kemudian mendekripsi data yang diterima untuk mendapatkan informasi asli. Kriptografi adalah studi tentang pembuatan dan penggunaan teknik enkripsi dan dekripsi. Banyak volume yang dapat diisi tentang teknik kriptografi, namun pengenalan prinsip dasar akan memberi Anda pemahaman yang memadai tentang teknik enkripsi yang digunakan saat ini. Menggali topik kriptografi mengharuskan Anda memahami beberapa istilah dasar. Plaintext (yang akan selalu ditampilkan dalam karakter huruf kecil pada contoh berikut) adalah data sebelum enkripsi dilakukan (Gambar 12-6). Algoritma enkripsi adalah program komputer yang mengubah teks biasa menjadi bentuk terenkripsi. Ciphertext (ditampilkan dalam karakter huruf besar) adalah data setelah algoritma enkripsi diterapkan. Kunci adalah informasi unik yang digunakan untuk membuat ciphertext dan kemudian mendekripsi ciphertext kembali menjadi plaintext. Setelah ciphertext dibuat, ia dikirim ke penerima, di mana data ciphertext didekripsi.



Gambar 12-6 Prosedur dasar enkripsi dan dekripsi

Algoritma kriptografi awal menggunakan kunci yang sama untuk enkripsi dan dekripsi. Penggunaan satu kunci sangat mengkhawatirkan banyak ahli. Untuk memungkinkan lokasi lokal dan terpencil mengirim dan menerima data terenkripsi, kunci harus diberikan kepada pihak lokal dan jarak jauh. Jika kunci ini dicegat dan jatuh ke tangan yang salah, data terenkripsi tidak hanya dapat didekripsi, tetapi data palsu juga dapat dienkripsi dan dikirim ke salah satu pihak. Teknik yang lebih baru, seperti yang akan segera Anda lihat, menyelesaikan masalah ini dengan mengizinkan penggunaan dua kunci yang berbeda, namun terkait secara matematis. Kunci pertama untuk mengenkripsi data, dan kunci kedua untuk mendekripsi data. Mari kita mulai diskusi kita tentang teknik enkripsi dengan melihat salah satu yang paling sederhana: sandi berbasis substitusi monoalfabetik.

Sandi Berbasis Substitusi Monoalfabetik

Meskipun namanya menakutkan, sandi berbasis substitusi monoalfabetik sebenarnya merupakan teknik enkripsi yang cukup sederhana. Sandi berbasis substitusi monoalfabetik menggantikan suatu karakter atau sekelompok karakter dengan karakter atau kelompok karakter yang berbeda. Perhatikan contoh sederhana berikut ini. Setiap huruf pada baris teks biasa dipetakan ke huruf di bawahnya pada baris teks sandi.

```

Plaintext : a b c d e f g h i j k l m n o p q r s t u v w x y z
Chipertext : P O I U Y T R E W Q L K J H G F D S A M N Z V C X B
  
```

Teks sandi ini hanya sesuai dengan huruf-huruf pada keyboard, memindai dari kanan ke kiri, dari atas ke bawah. Untuk mengirim pesan menggunakan skema pengkodean ini, setiap huruf teks biasa dari pesan tersebut diganti dengan karakter teks tersandi tepat di bawahnya. Demikian pesannya

```

how about lunch at noon
  
```

akan dikodekan ke

```

EGVPO GNMKN HIEPM HGGH
  
```

Sebuah spasi ditempatkan setelah setiap lima karakter ciphertext untuk membantu menyamakan pola yang jelas. Contoh ini bersifat monoalfabetik karena satu string alfabet

digunakan untuk menyandikan teks biasa. Ini adalah sandi berbasis substitusi karena satu karakter teks tersandi diganti dengan satu karakter teks biasa.

Sandi Berbasis Substitusi Polialfabetik

Sandi berbasis substitusi polialfabetik mirip dengan sandi monoalfabetik, namun menggunakan beberapa string alfabet untuk menyandikan teks biasa, bukan satu string alfabet. Mungkin contoh paling awal dari sandi polialfabetik adalah sandi Vigenère, yang dirancang oleh Blaise de Vigenère pada tahun 1586. Untuk sandi Vigenère, matriks karakter berukuran 26 × 26 dibuat, seperti yang ditunjukkan pada Tabel 12-1.

Tabel 12-1 Contoh matriks karakter ciphertext Vigenère 26 × 26

Karakter Kunci	Huruf Plaintext																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
...	.																									
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Untuk melakukan sandi ini, Anda memilih kunci, seperti ILMU KOMPUTER, yang Anda tempatkan berulang kali di atas pesan teks biasa. Misalnya:

Kunci : COMPUTERSCIENCECOMPUTERSCIENCECOMPUTERSCIENCECO
 Plaintext : thisclassondatacommunicationsisthebestclassever

Untuk mengkodekan pesan, Anda melihat huruf pertama dari teks biasa, t, dan karakter kunci yang sesuai tepat di atasnya, C. C memberitahu Anda untuk menggunakan baris C dari matriks 26 × 26 untuk melakukan substitusi alfabet untuk teks biasa karakter t. Anda kemudian pergi ke kolom T di baris C dan menemukan karakter ciphertext V. Proses ini diulangi untuk setiap karakter plaintext. Kuncinya, COMPUTERSCIENCE, harus dirahasiakan antara encoder dan decoder.

Untuk mempersulit penyusup, standarnya adalah 26 × 26 matriks dengan baris A, baris B, baris C, dan seterusnya tidak harus digunakan. Sebaliknya, pengkodean dan decoding dapat dilakukan dengan menggunakan matriks unik. Dalam hal ini, matriks dan kuncinya harus tetap dirahasiakan.

Cipher Berbasis Transposisi

Sandi berbasis transposisi berbeda dengan sandi berbasis substitusi karena urutan teks biasa tidak dipertahankan. Menata ulang urutan karakter teks biasa membuat pola umum menjadi tidak jelas dan kode menjadi lebih sulit dipecahkan. Mari kita perhatikan contoh sederhana dari sandi transposisi. Pilih kata kunci yang tidak mengandung huruf rangkap, misalnya KOMPUTER. Di setiap huruf dalam kata kunci, tuliskan nomor yang sesuai dengan

urutan kemunculan huruf tersebut dalam alfabet jika dibandingkan dengan huruf lain dalam kata kunci. Untuk kata kunci KOMPUTER, C muncul pertama dalam alfabet, E kedua, M ketiga, O keempat, dan seterusnya.

```
14358726
KOMPUTER
```

Ambil pesan teks biasa seperti “ini adalah kelas terbaik yang pernah saya ambil” dan tuliskan di bawah kata kunci dalam baris berurutan dari kiri ke kanan.

```
14358726
KOMPUTER
iniadala
hkelaste
rbaikyan
gpernahs
ayaambil
```

Untuk mengkodekan pesan, bacalah setiap kolom dimulai dengan kolom bernomor 1 dan berlanjut ke kolom bernomor 8. Kolom bacaan 1 memberi kita TESV, dan kolom 2 memberi kita TLEE. Pengkodean kedelapan kolom memberi kita pesan berikut:

```
TESVTLEEIEIRHBSESSHSTAENSCVKITAA
```

Dua pengamatan menarik dapat dilakukan mengenai contoh ini. Pertama, pemilihan kata kunci sekali lagi sangat penting, dan kehati-hatian harus diberikan untuk memastikan kata kunci tidak jatuh ke tangan yang salah. Kedua, Anda dapat mempersulit enkripsi dengan melakukan sandi berbasis substitusi tambahan pada hasil sandi transposisi. Sebenarnya, mengapa berhenti di situ? Anda dapat membuat kode yang sangat sulit jika Anda mengulangi berbagai pola sandi berbasis substitusi dan transposisi, satu demi satu.

Kriptografi Kunci Publik

Semua teknik pengkodean dan decoding yang ditunjukkan sejauh ini bergantung pada perlindungan kunci dan menjaganya agar tidak jatuh ke tangan penyusup. Mengingat betapa pentingnya kerahasiaan kunci, sungguh mengejutkan betapa seringnya keamanan kata kunci atau kata sandi lemah atau bahkan tidak ada sama sekali. Perhatikan episode Stanley Mark Rifkin dan Security Pacific National Bank. Pada tahun 1978, Rifkin menyamar sebagai pegawai bank, memperoleh akses ke ruang transfer dana kawat, menemukan kata sandi untuk mentransfer dana elektronik yang ditempel di dinding di atas terminal komputer, dan mentransfer \$12 juta ke rekening pribadinya. Ketika dia ditangkap, dia sedang membual tentang prestasinya di bar.

Salah satu teknik untuk melindungi kunci dari penyusup sering terlihat dalam film mata-mata hitam-putih larut malam: Pecahkan kunci menjadi beberapa bagian dan serahkan

setiap bagian ke individu yang berbeda. Dalam kehidupan nyata, alih-alih hanya memberikan satu atau dua karakter pada setiap orang, kriptografer menggunakan teknik matematika, seperti persamaan linear simultan, untuk membagi kunci. Teknik lain yang memerlukan manipulasi kunci, atau menutupi kunci sehingga tidak terlihat jelas, bisa membosankan dan terkadang tidak menambah keamanan nyata pada kunci tersebut.

Salah satu masalah yang melekat dalam melindungi satu kunci adalah bahwa hanya satu kunci yang digunakan untuk menyandikan dan mendekode pesan. Semakin banyak orang yang memiliki kunci tersebut, semakin besar kemungkinan seseorang menjadi ceroboh dan membiarkan kunci tersebut diketahui oleh orang yang tidak berwenang. Namun bagaimana jika ada dua kunci yang terlibat—satu kunci publik dan satu kunci privat? Data yang dienkripsi dengan kunci publik hanya dapat didekodekan dengan kunci privat, dan data yang dienkripsi dengan kunci privat hanya dapat didekodekan dengan kunci publik. Konsep dua kunci, publik dan privat, disebut kriptografi kunci publik. Ini juga disebut enkripsi asimetris. (Kebalikan dari enkripsi asimetris adalah enkripsi simetris, yang mana satu kunci digunakan untuk mengenkripsi dan mendekripsi.) Ketika satu kunci mengenkripsi teks biasa dan kunci lainnya mendekripsi teks tersandi, hal ini hampir tidak mungkin dilakukan—meskipun Anda memiliki akses ke salah satu kunci tersebut. —Untuk menyimpulkan kunci kedua dari kunci pertama. Selain itu, data terenkripsi juga sangat sulit untuk didekodekan tanpa kunci pribadi—bahkan bagi para ahli.

Bagaimana cara kerja kriptografi kunci publik? Pertimbangkan sebuah bisnis yang berkantor pusat di New York. Sebuah kantor cabang di Atlanta ingin mengirimkan data aman ke kantor New York. Kantor di New York mengirimkan kunci publik ke Atlanta dan menyimpan kunci pribadi dengan aman di New York. Kantor Atlanta menggunakan kunci publik untuk mengenkripsi data dan mengirimkan data terenkripsi ke New York. Hanya kantor di New York yang dapat memecahkan kode data karena hanya kantor tersebut yang memiliki kunci pribadi. Sekalipun pihak lain mencegat transmisi kunci publik ke Atlanta, tidak ada keuntungan apa pun karena tidak mungkin menyimpulkan kunci privat dari kunci publik. Demikian pula, intersepsi data terenkripsi tidak akan menghasilkan apa-apa karena data hanya dapat didekodekan dengan kunci privat.

Sebagai contoh yang lebih umum, pertimbangkan situasi di mana seseorang menjelajahi Web ingin mengirimkan informasi aman (seperti nomor kartu kredit) ke server Web. Pengguna di stasiun kerja mengklik halaman Web yang aman dan mengirimkan permintaan yang sesuai ke server. Server mengembalikan “sertifikat”, yang mencakup kunci publik server, dan sejumlah algoritma kriptografi pilihan. Stasiun kerja pengguna memilih salah satu algoritme, menghasilkan sekumpulan kunci publik dan privat, menyimpan kunci privat, dan mengirimkan kunci publik kembali ke server. Sekarang kedua belah pihak memiliki kunci privat masing-masing, dan keduanya memiliki kunci publik masing-masing. Data sekarang dapat dikirim antara dua titik akhir dengan cara yang aman.

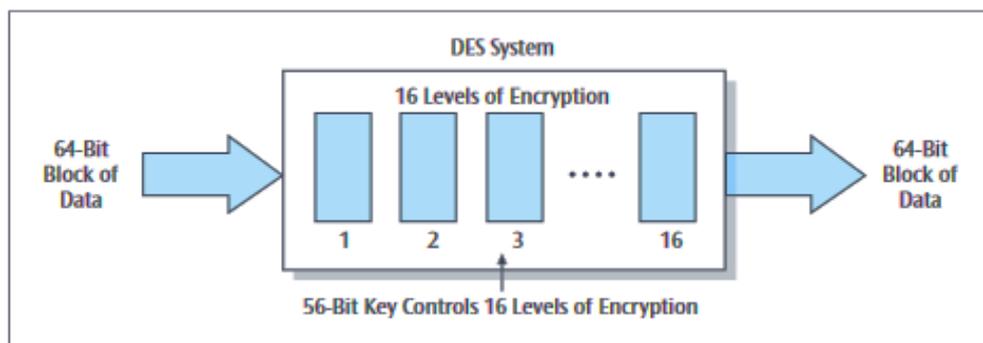
Teknik ini merupakan bagian dari Secure Sockets Layer dan dapat digunakan oleh sebagian besar browser Web dan server ketika diperlukan untuk mengirimkan data yang aman.

Secure Sockets Layer (SSL) adalah lapisan perangkat lunak tambahan yang ditambahkan antara lapisan aplikasi dan lapisan transport (TCP) yang menciptakan koneksi aman antara pengirim dan penerima. Karena sistem operasi Unix membuat koneksi antar titik akhir dalam jaringan melalui soket, perangkat lunak tersebut diberi nama Secure Sockets Layer. Penerus SSL adalah Transport Layer Security (TLS), yang didasarkan pada SSL versi 3 dan berisi beberapa perbaikan teknis dibandingkan SSL. Teknik kedua yang mirip dengan SSL adalah Secure-HTTP atau S-HTTP, namun teknik ini belum mengalami kesuksesan SSL secara luas. SSL dan S-HTTP pada akhirnya akan digantikan oleh IPsec, standar keamanan baru yang dibuat oleh Internet Engineering Task Force.

IPsec (keamanan IP) adalah seperangkat protokol yang dibuat untuk mendukung transfer data yang aman pada lapisan IP. Salah satu aplikasi IPsec yang populer adalah dalam mendukung jaringan pribadi virtual. Ingatlah bahwa jaringan pribadi virtual membuat “terowongan” antara pengguna dan tujuan jarak jauh melalui Internet. IPsec menggunakan enkripsi untuk melindungi paket saat dikirimkan melalui terowongan ini. Lebih tepatnya, titik akhir terowongan menukar pasangan kunci publik/kunci pribadi.

Standar Enkripsi Data dan Standar Enkripsi Lanjutan

Standar Enkripsi Data (DES) adalah metode enkripsi yang umum digunakan oleh bisnis untuk mengirim dan menerima transaksi aman. Standar ini mulai berlaku pada tahun 1977 dan disetujui kembali pada tahun 1983, 1988, dan 1993. Algoritma dasar di balik standar ini ditunjukkan pada Gambar 12-7. Algoritma DES bekerja dengan blok data 64-bit, dan menempatkan setiap blok pada 16 level, atau putaran, enkripsi. Teknik enkripsi didasarkan pada sandi berbasis substitusi dan transposisi. Masing-masing dari 16 tingkat enkripsi dapat melakukan operasi berbeda berdasarkan konten kunci 56-bit. Kunci 56-bit diterapkan pada algoritma DES, blok data 64-bit dienkripsi dengan cara yang unik, dan data terenkripsi dikirimkan ke penerima yang dituju. Merupakan tanggung jawab pihak-pihak yang terlibat untuk menjaga rahasia kunci 56-bit ini dan mencegahnya jatuh ke tangan pihak lain.



Gambar 12-7 Operasi dasar Standar Enkripsi Data

Meskipun kunci 56-bit menyediakan lebih dari 72 kuadriliun kemungkinan kunci, Standar Enkripsi Data dikritik sejak awal karena terlalu lemah. Dunia usaha dan peneliti merasa diperlukan kunci yang jauh lebih besar agar enkripsi tidak mungkin dibobol. Namun, pemerintah merasa bahwa 56 bit sudah cukup dan tidak seorang pun akan menghabiskan

waktu atau sumber daya yang diperlukan untuk mencoba memecahkan kunci tersebut. Mengapa pemerintah enggan mendukung kekhawatiran dunia usaha mengenai keamanan data mereka? Barangkali kekhawatiran pemerintah adalah bahwa penjahat yang memiliki kunci lebih besar dari 56 bit dapat mengirimkan materi terenkripsi yang tidak dapat didekripsi oleh siapa pun, termasuk pemerintah sendiri, sehingga akan menimbulkan kerugian yang dapat membahayakan keamanan nasional. Pada bulan Juli 1998, perdebatan pihak pemerintah mengalami kemunduran ketika sebuah kelompok bernama Electronic Frontier Foundation mengklaim bahwa mereka telah memecahkan kunci 56-bit dalam 56 jam, menggunakan satu komputer pribadi khusus yang disebut DES Cracker.

Upaya untuk merancang teknik enkripsi yang lebih kuat mengarah pada terciptanya triple-DES. Dengan triple-DES, data dienkripsi menggunakan DES sebanyak tiga kali—pertama kali dengan kunci pertama, kedua kali dengan kunci kedua, dan ketiga kali dengan kunci pertama lagi. Meskipun teknik ini menciptakan sistem enkripsi yang hampir tidak dapat dipecahkan, teknik ini membutuhkan banyak CPU; Artinya, penggunaan enkripsi triple-DES memerlukan waktu pemrosesan yang besar. Proses intensif CPU tidak diinginkan pada perangkat kecil seperti ponsel, kartu pintar, dan asisten digital pribadi. Oleh karena itu, yang dibutuhkan adalah teknik enkripsi yang sekuat triple-DES namun juga cepat dan ringkas.

Standar Enkripsi Tingkat Lanjut menjawab kebutuhan ini. Standar Enkripsi Lanjutan (AES) dipilih oleh pemerintah AS untuk menggantikan DES. Lebih tepatnya, Institut Standar dan Teknologi Nasional memilih algoritma Rijndael (diucapkan boneka hujan) pada bulan Oktober 2000 sebagai dasar untuk AES. Algoritma Rijndael melibatkan rumus matematika yang sangat elegan, hanya membutuhkan satu kali lintasan (bukan tiga kali lintasan seperti triple-DES), menghitung dengan sangat cepat, hampir tidak dapat dipecahkan, dan beroperasi bahkan pada perangkat komputasi terkecil sekalipun. Dengan AES, seseorang mempunyai kemampuan untuk memilih ukuran kunci 128, 192, atau 256 bit.

Tanda Tangan Digital

Teknik enkripsi dan dekripsi dasar telah berkembang pesat sejak awal. Meskipun teknik yang ada saat ini sering kali menggunakan metode enkripsi dan dekripsi yang canggih, banyak dari metode ini yang memiliki dasar berdasarkan teknik dasar sebelumnya. Mari kita periksa sejumlah kemajuan terkini dalam kriptografi yang dimulai dengan konsep tanda tangan digital.

Saat berpartisipasi dalam transaksi keuangan atau hukum, orang sering kali mengidentifikasi dirinya melalui tanda tangan tulisan tangan atau dengan memasukkan PIN. Misalnya, ketika Anda menggunakan kartu debit untuk membeli sesuatu, Anda harus memasukkan PIN Anda ke papan tombol elektronik dan PIN Anda dibandingkan dengan yang disimpan di sistem. Dengan asumsi kartu dan PIN Anda belum dicuri dan tidak ada orang yang menyamar sebagai Anda, sistem ini cukup aman. Namun apa jadinya jika Anda ingin “menandatangani” sebuah dokumen elektronik agar nantinya bisa membuktikan bahwa itu adalah dokumen Anda dan bukan milik orang lain? Untuk mengautentikasi dokumen elektronik sebagai milik Anda, Anda perlu membuat tanda tangan digital. Tanda tangan digital

adalah prosedur keamanan yang menggunakan kriptografi kunci publik untuk menetapkan kode pada dokumen yang hanya Anda yang memiliki kuncinya.

Menandatangani dokumen elektronik secara digital melibatkan pengiriman dokumen melalui perhitungan matematis kompleks yang menghasilkan bilangan prima besar yang disebut hash. Dokumen asli dan hash saling terkait erat. Jika dokumen atau hash diubah, keduanya tidak akan cocok, dan dokumen tidak dapat didekode.

Saat pengguna menandatangani dokumen secara digital, hash (hash asli) dihasilkan dari dokumen tersebut dan kemudian dikodekan dengan kunci pribadi pengguna. Hash yang dikodekan ini menjadi tanda tangan digital dan disimpan bersama dokumen atau dikirimkan bersama dokumen. Nanti, jika seseorang ingin memverifikasi bahwa dokumen ini milik pengguna ini, hash baru akan dibuat dari dokumen tersebut. Hash asli, yang telah dienkripsi dengan kunci pribadi pemilik, didekripsi dengan kunci publik pemilik, dan kedua hash tersebut dibandingkan. Jika kedua hash tersebut cocok, maka data tidak diubah, dan tanda tangan digital pengguna valid. Seseorang dapat berargumen bahwa dia tidak melihat pengguna "menandatangani" dokumen asli, dan oleh karena itu tidak benar-benar mengetahui bahwa dokumen tersebut sah. Argumen ini diselesaikan dengan fakta bahwa hanya satu pengguna ini yang boleh memiliki kunci privat ini. Jadi, pengguna ini adalah satu-satunya orang yang dapat membuat dokumen berkode khusus ini.

Salah satu kelemahan sistem ini adalah jika seseorang menemukan kunci pribadi pengguna, tanda tangan digital dapat dipalsukan. Membuat sistem yang menetapkan hash dan kunci serta merahasiakannya memerlukan infrastruktur kunci publik, topik yang akan segera kita diskusikan.

Pada tahun 2000, pemerintah AS menyetujui Undang-Undang Tanda Tangan Elektronik dalam Perdagangan Global dan Nasional. Undang-undang ini memberikan tanda tangan digital pada dokumen elektronik dengan kedudukan hukum yang sama dengan tanda tangan tulisan tangan pada selembar kertas. Namun penting untuk dicatat bahwa tidak semua dokumen dapat ditandatangani secara sah dengan tanda tangan digital. Misalnya, meskipun pinjaman rumah dan hipotek mungkin ditandatangani secara digital, dokumen seperti perjanjian perceraian, surat wasiat, dan kontrak adopsi masih memerlukan tanda tangan pena dan kertas yang lazim.

Pretty Good Privacy (PGP)

Dalam upaya menciptakan skema enkripsi yang dapat digunakan oleh kebanyakan orang, seorang pengusaha bernama Philip Zimmermann menciptakan perangkat lunak enkripsi bernama Pretty Good Privacy (PGP). PGP adalah perangkat lunak enkripsi berkualitas tinggi yang menjadi sangat populer untuk membuat pesan email yang aman dan mengenkripsi jenis file data lainnya. PGP menggunakan beberapa teknik enkripsi terbaru, termasuk kriptografi kunci publik dan tanda tangan digital, dan tersedia bagi siapa saja di Amerika Serikat secara gratis. Situs web, situs FTP, dan papan buletin menawarkan salinan gratis untuk penggunaan individu, dan versi komersial dapat dibeli untuk instalasi komersial. Namun, Anda harus menyadari bahwa meskipun penggunaan PGP dan perangkat lunak enkripsi lainnya legal di Amerika Serikat, hal tersebut mungkin tidak legal di negara lain. Selain itu, mengirim PGP

dari Amerika Serikat ke negara lain adalah ilegal. Zimmermann sendiri mengalami banyak masalah hukum karena dia mengizinkan perangkat lunak PGP miliknya meninggalkan Amerika Serikat, yang melanggar undang-undang ekspor federal yang melarang pengangkutan perangkat lunak enkripsi secara eksternal.

Jika Anda ingin mengirim transmisi yang aman, Anda dapat menerapkan PGP pada dokumen Anda, baik itu halaman Web atau pesan email. Namun perlu diingat bahwa karena PGP didasarkan pada teknik enkripsi kunci publik dan oleh karena itu kunci publik dan privat diperlukan, stasiun kerja penerima harus memiliki perangkat lunak PGP yang sama dengan stasiun kerja pengirim untuk mendekripsi pesan Anda. Karena terdapat banyak versi PGP yang berbeda dan berbagai batasan dalam penggunaannya, Anda harus berkonsultasi dengan satu atau lebih situs Web populer yang ditujukan untuk mendukung PGP untuk mempelajari rincian yang lebih spesifik.

Kerbero

Kerberos adalah protokol otentikasi yang dirancang untuk bekerja pada jaringan klien/server yang menggunakan kriptografi rahasia atau simetris. Berbeda dengan kriptografi kunci publik, yang menggunakan dua kunci—kunci publik dan kunci privat—Kerberos menggunakan satu kunci untuk enkripsi dan dekripsi.

Salah satu fungsi utama Kerberos adalah untuk mengautentikasi pengguna. Misalnya, jika stasiun kerja klien meminta layanan dari server Web, dan server Web menginginkan jaminan bahwa klien tersebut sesuai dengan klaimnya, Kerberos dapat menyediakan otentikasi. Untuk memastikan tingkat otentikasi ini, klien menunjukkan tiket yang awalnya dikeluarkan oleh server otentikasi Kerberos. Dalam tiket ini terdapat kata sandi yang dipilih oleh klien sebelumnya. Server menerima tiket beserta permintaan transaksi, memeriksa tiket, dan memverifikasi bahwa pengguna adalah siapa yang dia klaim. Banyak paket aplikasi yang ditemukan pada sistem klien/server mendukung penggunaan Kerberos.

Sekarang kita telah mempelajari teknik dasar untuk menjaga keamanan data, mari kita lihat teknologi yang menggabungkan semua teknik ini.

Infrastruktur Kunci Publik

Misalkan Anda bekerja untuk sebuah perusahaan yang ingin membuka jaringan area lokal internalnya ke Internet, sehingga memungkinkan karyawannya mengakses sumber daya komputasi perusahaan—seperti email dan database perusahaan—dari lokasi yang jauh; untuk mengizinkan pelanggan korporat atau pemasok mengakses catatan perusahaan; atau untuk memungkinkan pelanggan ritel melakukan pemesanan atau menanyakan tentang pesanan sebelumnya. Dalam setiap transaksi tersebut, perusahaan ingin memastikan bahwa orang yang melakukan transaksi tersebut adalah karyawan atau pelanggan yang sah, bukan peretas yang mencoba menyusupi sistemnya. Teknologi yang membantu perusahaan mencapai tujuan ini adalah infrastruktur kunci publik.

Infrastruktur kunci publik (PKI) adalah kombinasi teknik enkripsi, perangkat lunak, dan layanan yang melibatkan semua bagian yang diperlukan untuk mendukung sertifikat digital, otoritas sertifikat, serta pembuatan, penyimpanan, dan pengelolaan kunci publik. Sebuah perusahaan yang mematuhi prinsip-prinsip PKI menerbitkan sertifikat digital kepada

pengguna dan server jaringan yang sah, menyediakan perangkat lunak pendaftaran kepada pengguna akhir, dan menyediakan server jaringan dengan alat yang diperlukan untuk mengelola, memperbarui, dan mencabut sertifikat.

Sertifikat digital, atau sekadar sertifikat, adalah dokumen elektronik, mirip dengan paspor, yang menetapkan kredensial Anda saat Anda melakukan transaksi di World Wide Web. Sertifikat tersebut dapat berisi nama Anda, nomor seri, tanggal kedaluwarsa, salinan kunci publik Anda, dan tanda tangan digital dari otoritas penerbit sertifikat (untuk memungkinkan Anda memverifikasi bahwa sertifikat tersebut sah). Sertifikat biasanya disimpan dalam registri sehingga pengguna lain dapat mencari informasi kunci publik pengguna tertentu.

Banyak sertifikat yang sesuai dengan standar X.509. Dibuat dan didukung oleh International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), standar X.509 mendefinisikan informasi apa yang dapat dimasukkan ke dalam sertifikat. Semua sertifikat X.509 berisi informasi berikut:

- *Versi*—Mengidentifikasi versi standar X.509 yang berlaku untuk sertifikat ini
- *Nomor seri*—Nilai unik yang mengidentifikasi sertifikat tertentu; ketika sertifikat dicabut, nomor serinya ditempatkan dalam daftar pencabutan sertifikat (CRL)
- *Pengidentifikasi algoritme tanda tangan*—Mengidentifikasi algoritme yang digunakan oleh otoritas sertifikat (entitas yang akan segera ditentukan) untuk menandatangani sertifikat
- *Nama penerbit*—Nama entitas, biasanya otoritas sertifikat, yang menandatangani sertifikat (dalam beberapa kasus, penerbit menandatangani namanya sendiri)
- *Masa berlaku*—Jumlah waktu terbatas yang berlaku untuk setiap sertifikat (jangka waktu yang bisa beberapa detik atau selama satu abad), ditandai dengan tanggal dan waktu mulai serta tanggal dan waktu berakhir
- *Nama subjek*—Nama entitas yang kunci publiknya diidentifikasi oleh sertifikat ini
- *Informasi kunci publik subjek*—Kunci publik dari entitas yang diberi nama, bersama dengan pengidentifikasi algoritme yang menentukan sistem enkripsi kunci publik mana yang dimiliki kunci tersebut
- *Tanda tangan digital*—Tanda tangan otoritas sertifikat yang akan digunakan untuk memverifikasi sertifikat yang sah

Semua sertifikat diterbitkan oleh otoritas sertifikat. Otoritas sertifikat (CA) adalah perangkat lunak khusus di jaringan atau organisasi atau bisnis pihak ketiga tepercaya yang menerbitkan dan mengelola sertifikat. Salah satu bisnis pihak ketiga tersebut adalah VeriSign, yang merupakan penyedia layanan PKI terintegrasi penuh yang dirancang untuk memberikan sertifikat kepada perusahaan yang ingin menggabungkan PKI namun tidak ingin berurusan dengan perangkat keras dan perangkat lunak rumit yang diperlukan untuk membuat dan mengelola sertifikatnya sendiri.

Pertimbangkan skenario di mana pengguna ingin memesan beberapa produk dari situs Web. Ketika pengguna siap untuk melakukan pemesanan, situs Web mencoba memastikan bahwa pengguna tersebut benar-benar seperti yang dia klaim dengan meminta pengguna

menandatangani pesanan dengan kunci pribadinya. Kunci pribadi ini seharusnya sudah diberikan kepada pengguna oleh otoritas sertifikat, seperti VeriSign. Paket yang terdiri dari pesanan pengguna dan tanda tangan digital dikirim ke server. Server kemudian meminta sertifikat pengguna dan sertifikat VeriSign. Server memvalidasi sertifikat pengguna dengan memverifikasi tanda tangan VeriSign, lalu menggunakan sertifikat pengguna untuk memvalidasi tanda tangan pada pesanan. Jika semua tanda tangan cocok, mengonfirmasi bahwa pengguna adalah siapa yang diklaimnya, maka pesanan akan diproses. Biasanya semua ini terjadi tanpa sepengetahuan pengguna. Meskipun sebagian besar pengecer Web tidak menggunakan PKI untuk memverifikasi pelanggan mereka—dan malah mengandalkan Lapisan Soket Aman—terdapat indikasi bahwa lebih banyak pengecer akan melakukan hal yang sama dalam waktu dekat.

Daftar pencabutan sertifikat (CRL) adalah daftar sertifikat yang telah dicabut sebelum tanggal kedaluwarsa yang dijadwalkan semula. Mengapa sertifikat bisa dicabut? Sertifikat akan dicabut jika kunci yang ditentukan dalam sertifikat telah disusupi dan tidak berlaku lagi, atau pengguna yang ditentukan dalam sertifikat tidak lagi memiliki wewenang untuk menggunakan kunci tersebut. Misalnya, jika seorang karyawan telah diberi sertifikat oleh sebuah perusahaan dan kemudian berhenti atau dipecat, otoritas sertifikat akan mencabut sertifikat tersebut dan menempatkan ID sertifikat pada CRL. Karyawan tidak lagi dapat mengirim dokumen aman menggunakan sertifikat ini. Sebenarnya, hal ini hanya berlaku jika perangkat lunak meluangkan waktu untuk memeriksa setiap sertifikat terhadap CRL. Keputusan apakah meluangkan waktu untuk melakukan pemeriksaan ini sepadan dengan usaha yang dilakukan mungkin bergantung pada pentingnya dokumen yang ditandatangani.

Perusahaan yang perlu melakukan transaksi yang aman sering kali akan berinvestasi pada sistem PKI mereka sendiri. Karena sistem PKI bersifat khusus dan relatif terlibat, maka biayanya biasanya sangat mahal. Sebelum membeli sistem PKI, perusahaan perlu mempertimbangkan apakah transaksi yang perlu diamankan tetap bersifat internal (di dalam jaringan), atau apakah transaksi tersebut perlu melintasi jaringan eksternal. Transaksi eksternal, seperti transaksi perdagangan elektronik, memerlukan sistem yang dapat berinteroperasi dengan sistem perusahaan lain. Faktor lain yang perlu dipertimbangkan perusahaan ketika memilih sistem PKI adalah ukuran aplikasi yang memerlukan transaksi aman. Jika Anda memiliki jumlah karyawan yang sedikit (kira-kira kurang dari 100 orang), mungkin akan lebih ekonomis untuk membeli sistem PKI yang tertanam dalam aplikasi. Jika jumlah karyawan lebih besar (lebih dari 100), maka sistem PKI yang mendukung sistem penyimpanan dan pengelolaan kunci dan sertifikat yang lengkap mungkin akan lebih berguna.

Jenis aplikasi atau transaksi apa yang dapat memperoleh manfaat dari infrastruktur kunci publik? Berikut ini contoh singkatnya:

- Akses World Wide Web—Memesan produk melalui Internet adalah aktivitas umum yang mendapat manfaat dari PKI.
- Jaringan pribadi virtual—Sistem PKI dapat membantu menciptakan terowongan VPN yang aman (dijelaskan dalam Bab Sepuluh) melalui Internet yang tidak aman.

- Surat elektronik—PKI dapat digunakan untuk mengamankan pesan ketika pengguna ingin mengirim email aman melalui jaringan tidak aman seperti Internet.
- Aplikasi klien/server—Sistem klien/server, seperti sistem database interaktif, sering kali melibatkan transfer data yang aman. PKI dapat digunakan untuk memastikan bahwa data tetap aman saat berpindah dari klien ke server dan sebaliknya.
- Transaksi perbankan—Transaksi perbankan yang melintasi jaringan eksternal harus aman. PKI umumnya digunakan dalam sistem perbankan untuk membuat pasangan kunci publik/pribadi dan tanda tangan digital.

Ringkasnya, meskipun terdengar bagus, PKI mempunyai permasalahannya sendiri. Saat ini, seperti disebutkan sebelumnya, harganya mahal. Sistem PKI pada umumnya memerlukan biaya puluhan ribu hingga ratusan ribu dolar untuk usaha skala menengah. Selain itu, banyak sistem PKI yang merupakan hak milik dan tidak berinteraksi dengan baik dengan sistem PKI lainnya. Sisi positifnya, harga teknologi PKI, seperti kebanyakan teknologi lainnya, terus menurun. Selain itu, Satuan Tugas Rekayasa Internet terus berupaya membuat standar yang dapat dipatuhi oleh sistem PKI di masa depan. Standar-standar baru ini diharapkan akan meningkatkan kemungkinan interoperabilitas sistem PKI.

Steganografi

Steganografi adalah seni dan ilmu menyembunyikan informasi di dalam pesan atau dokumen lain yang tampaknya biasa saja. Berbeda dengan pengiriman pesan terenkripsi, steganografi melibatkan pesan tersembunyi; dengan demikian, Anda dapat mengetahui kapan pesan terenkripsi telah dikirim, namun Anda tidak dapat mengetahui kapan steganografi menyembunyikan pesan rahasia di dalam dokumen. Meskipun ada banyak cabang steganografi, yang melibatkan cara penyembunyian seperti tinta tak kasat mata dan titik mikro, cabang steganografi yang paling menarik perhatian akhir-akhir ini adalah penyembunyian pesan rahasia di dalam gambar digital.

Ketika disimpan di komputer, gambar digital pada dasarnya adalah kumpulan angka yang besar. Setiap angka mewakili keberadaan piksel, titik berwarna atau hitam-putih. Umumnya memiliki piksel 8-bit yang mewakili 256 warna berbeda, dan ukuran gambar umumnya adalah 640×480 piksel, atau 2.457.600 bit ($640 \times 480 \times 8$). Ide di balik steganografi adalah bahwa pesan rahasia dapat disembunyikan di dalam lebih dari 2,4 juta bit ini. Saat ini, ada tiga cara untuk menyembunyikan bit pesan rahasia dalam gambar digital: dengan menempatkannya dalam bit paling tidak signifikan (bit paling kanan) dari berbagai piksel; dengan menandai gambar dengan proses (disebut masking dan filtering) yang mirip dengan membuat watermark di atas kertas; dan dengan menggunakan algoritma dan transformasi. Pembaca yang tertarik dengan bentuk unik pengamanan data ini didorong untuk mencari informasi lebih lanjut di Web.

Sekarang kita telah membahas berbagai teknologi enkripsi, mari kita periksa jenis sistem pertahanan lain yang dapat digunakan untuk menjaga keamanan sumber daya.

12.6 MENGAMBIL KOMUNIKASI

Sejauh ini dalam bab ini, kita telah mempelajari beberapa teknik serangan yang paling umum digunakan oleh peretas, berbagai cara untuk membuat peralatan komputer dan jaringan aman secara fisik, teknik untuk mengendalikan akses, dan teknik untuk mengamankan data. Sekarang mari kita mengalihkan perhatian kita untuk mencari cara untuk membuat komunikasi lebih aman. Kita akan mulai dengan membahas cara-cara melindungi transmisi sinyal aman dalam jarak pendek menggunakan teknologi spektrum tersebar.

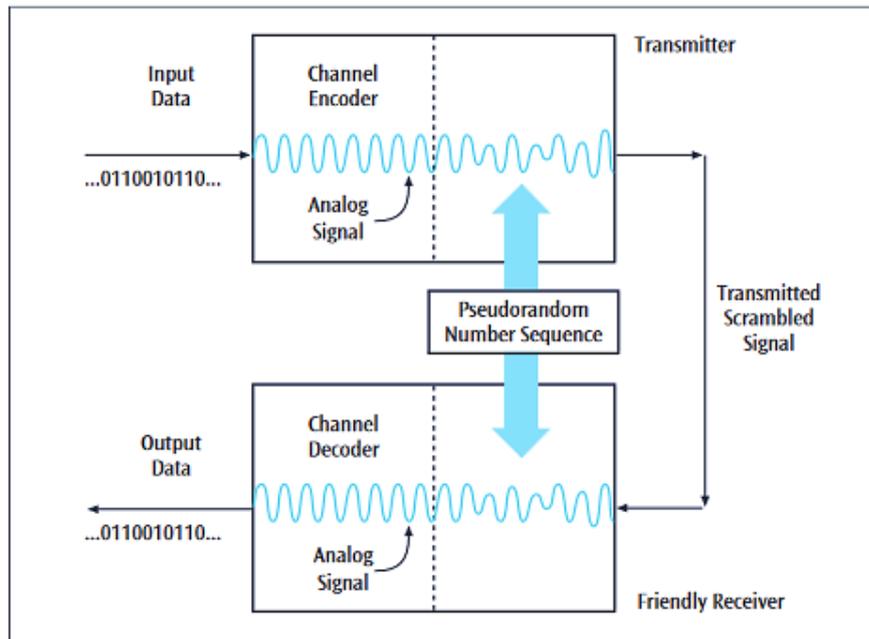
Teknologi spektrum tersebar

Jika Anda ingin mendengarkan stasiun tertentu (AM atau FM) di radio, Anda harus menyetel radio Anda (penerima) ke frekuensi yang sama dengan frekuensi pemancar stasiun tersebut (pengirim). Siapa pun yang berada dalam jangkauan pendengaran pemancar dapat menyetel ke frekuensi yang sama dan mendengarkan. Hal ini berfungsi dengan baik untuk radio komersial, namun selalu menjadi masalah serius bagi militer. Ketika satu pihak mengirimkan informasi militer, biasanya pihak tersebut tidak ingin musuh dapat mendengarnya. Dalam kasus seperti ini, transmisi informasi harus dibuat aman. Julius Caesar mungkin adalah salah satu pemimpin militer pertama yang menggunakan teknik pengkodean di mana surat-surat pesan diacak sedemikian rupa sehingga, jika kurir pesan ditangkap, musuh tetap tidak dapat membaca perintah Caesar. Ketika radio menjadi perangkat telekomunikasi yang umum bagi militer, diperlukan suatu bentuk enkripsi agar transmisi yang aman dapat dikirim dan diterima.

Tak lama setelah Perang Dunia II, teknologi seperti itu tersedia—disebut teknologi spektrum tersebar. Teknologi spektrum tersebar pada dasarnya mengambil data untuk dikirim dan bukannya mentransmisikannya dalam bandwidth tetap, melainkan menyebarkannya melalui bandwidth yang lebih luas. Dengan menyebarkan data, tingkat keamanan ditingkatkan, sehingga membuat sinyal akhirnya lebih tahan terhadap penyadapan atau penyadapan kabel. Salah satu aplikasi komersial yang lebih umum dari teknologi spektrum tersebar adalah komunikasi nirkabel, seperti yang ditemukan pada telepon nirkabel. Telepon nirkabel yang dilengkapi teknologi spektrum tersebar tahan terhadap penyadapan penyusup. Dua teknik dasar spektrum penyebaran yang umum digunakan dalam industri komunikasi saat ini: spektrum penyebaran frekuensi hopping dan spektrum penyebaran urutan langsung. Ide di balik transmisi spektrum penyebaran frekuensi hopping adalah untuk memantulkan sinyal pada frekuensi acak daripada mengirimkannya pada satu frekuensi tetap. Siapa pun yang mencoba menguping tidak akan dapat mendengarkan karena frekuensi transmisi terus berubah. Bagaimana penerima yang dituju mengikuti frekuensi yang memantul secara acak ini? Ternyata sinyalnya tidak memantul pada frekuensi acak; sepertinya hanya itu yang terjadi. Pemancar sebenarnya mengikuti urutan frekuensi pseudorandom, dan penerima yang dituju memiliki pengetahuan perangkat keras dan perangkat lunak untuk mengikuti urutan frekuensi pseudorandom ini.

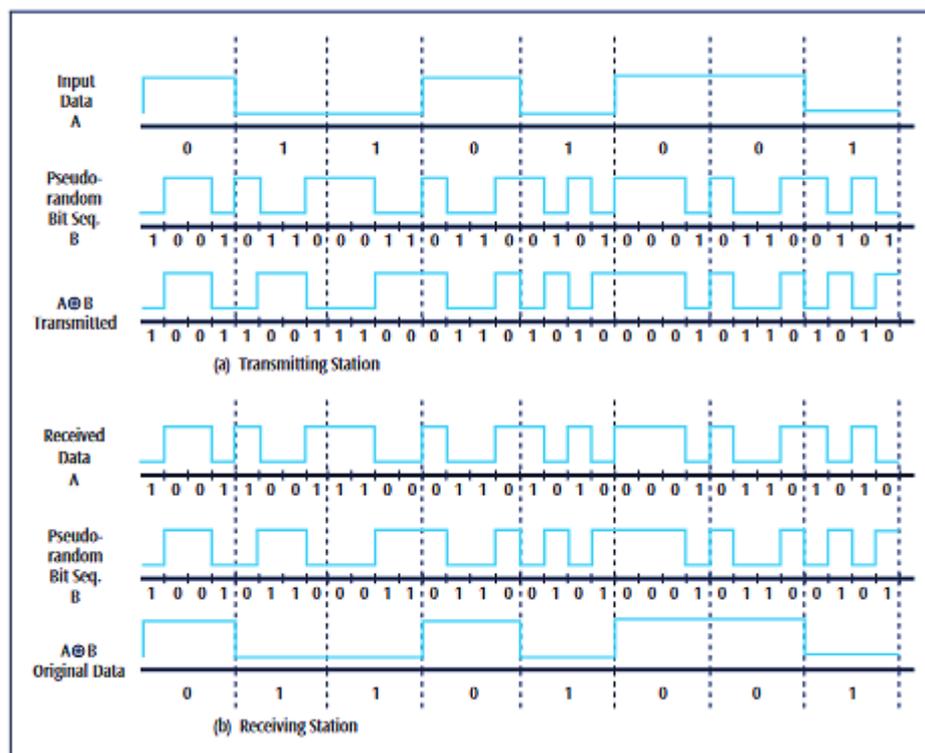
Gambar 12-8 menunjukkan operasi dasar sistem penerima dan pemancar spektrum penyebaran frekuensi hopping. Data masukan masuk ke channel encoder, yaitu perangkat yang menghasilkan sinyal analog dengan lebar pita sempit yang berpusat pada frekuensi

tertentu. Sinyal analog ini kemudian dimodulasi ke dalam pola frekuensi yang tampaknya acak, menggunakan urutan bilangan pseudorandom sebagai panduannya. Sinyal yang dimodulasi secara pseudorandom kemudian ditransmisikan ke penerima yang ramah. Operasi pertama yang dilakukan oleh penerima ramah adalah “menguraikan” sinyal termodulasi, menggunakan urutan pseudorandom yang sama dengan yang digunakan pemancar untuk mengkodekan sinyal. Sinyal yang tidak termodulasi kemudian dikirim ke decoder saluran, yang melakukan operasi kebalikan dari encoder saluran. Hasilnya adalah data asli.



Gambar 12-8 Pengoperasian dasar sistem penerima dan pemancar spektrum penyebaran frekuensi hopping

Teknik kedua untuk menciptakan sinyal spektrum tersebar untuk mengamankan komunikasi adalah spektrum penyebaran urutan langsung. Spektrum penyebaran urutan langsung menyebarkan transmisi sinyal pada rentang frekuensi yang luas menggunakan nilai matematika. Gambar 12-9 menunjukkan bahwa ketika data asli dimasukkan ke modulator urutan langsung, data tersebut di-OR secara eksklusif dengan aliran bit pseudorandom. (Eksklusif-OR adalah operasi logis yang menggabungkan dua bit dan menghasilkan satu bit sebagai hasilnya. Lebih tepatnya, jika Anda eksklusif-OR a 0 dan a 0, hasilnya adalah 0; 0 eksklusif-OR 1 sama dengan 1, dan 1 eksklusif-OR 0 sama dengan 1; bila Anda eksklusif-OR a 1 dan a 1, hasilnya lagi-lagi 0.) Jadi, keluaran modulator barisan langsung adalah hasil OR eksklusif antara data masukan dan bit pseudorandom urutan. Ketika data tiba di penerima yang dituju, sinyal spektrum penyebaran kembali di-OR secara eksklusif dengan aliran bit pseudorandom yang sama yang digunakan selama transmisi sinyal. Hasil dari OR eksklusif di pihak penerima ini adalah data asli. Code Division Multiple Access (CDMA), yang biasa digunakan pada telepon seluler modern, merupakan salah satu bentuk teknologi spektrum penyebaran urutan langsung.



Gambar 12-9 Contoh data biner yang diubah menjadi spektrum sebaran urutan langsung dan sebaliknya

Kesimpulannya, teknologi spektrum tersebar menawarkan cara yang efektif untuk mengamankan transmisi data antara pengirim dan penerima. Mari kita sekarang mengalihkan perhatian kita ke cara lain untuk mengamankan komunikasi. Secara khusus, mari kita periksa bagaimana komunikasi yang aman dapat dibuat antara komputer pengguna dan Internet.

Menjaga dari virus

Sebagaimana dinyatakan dalam pendahuluan bab ini, meskipun tingkat keamanan komputer saat ini lebih tinggi, pengguna belum pernah sedemikian rentan terhadap niat jahat dari pengguna komputer lain. Salah satu bentuk invasi paling umum yang disampaikan melalui saluran komunikasi adalah virus komputer. Karena virus adalah program komputer, ia mempunyai pola biner yang dapat dikenali. Model awal pemindai virus, dari tahun 1980an, mencari pola bit unik dari sebuah virus. Pemindai virus yang lebih baru mengawasi tindakan virus, seperti perubahan file atau aktivitas direktori yang tidak biasa. Untuk melindungi dari virus, Anda dapat membeli perangkat lunak antivirus yang memeriksa semua file Anda secara berkala dan menghapus virus apa pun yang ditemukan. Saat Anda mengunduh file dan email serta membuka aplikasi dengan perangkat lunak ini, Anda mungkin mendapat pesan yang memperingatkan Anda tentang virus baru. Untuk melindungi komputer Anda secara lebih efektif terhadap serangan virus, Anda perlu menggunakan perangkat lunak antivirus yang mencakup pemindaian berbasis tanda tangan, pemantauan penghentian dan tetap tinggal, dan pemeriksaan integritas.

Pemindaian berbasis tanda tangan bekerja dengan mengenali pola unik suatu virus. Semua virus mempunyai pola bit yang unik, seperti halnya untaian DNA yang memiliki urutan

unik. Pengembang produk antivirus dan peneliti virus membuat katalog virus yang dikenal dan tanda tangannya. Pemindaian berbasis tanda tangan kemudian menggunakan daftar katalog ini untuk mencari virus yang dikenal di sistem komputer pengguna. Karena virus baru dibuat setiap hari, pengguna perlu sering memperbarui katalog virus yang dikenal. Pembaruan ini biasanya dilakukan dengan mengunduh informasi virus baru dari Internet.

Untuk memberikan komputer mereka tingkat perlindungan yang konstan dari virus, sebagian besar pengguna menggunakan perangkat lunak antivirus yang terus mengawasi virus—teknik yang dikenal sebagai pemantauan penghentian dan tetap tinggal. Perangkat lunak antivirus dengan pemantauan penghentian dan tetap tinggal berjalan di latar belakang sementara aplikasi yang dijalankan pengguna berjalan di latar depan. Program terminasi dan tetap tinggal dapat memberikan kombinasi layanan perlindungan, termasuk pemantauan disk drive dan file secara real-time, analisis cerdas terhadap perilaku mirip virus, dan deteksi virus polimorfik. Keuntungan perangkat lunak antivirus dengan pemantauan penghentian dan tetap tinggal adalah sifatnya yang otomatis—pengguna tidak perlu mengaktifkan perangkat lunak setiap kali file baru dibuka atau diunduh. Salah satu kelemahan perangkat lunak ini adalah karena pemeriksa virus selalu berjalan, ia menghabiskan memori dan sumber daya pemrosesan. Kerugian lainnya adalah perangkat lunak antivirus jenis ini dapat menimbulkan alarm palsu. Setelah diganggu oleh sejumlah alarm palsu, pengguna sering kali menonaktifkan perangkat lunak antivirus sepenuhnya, sehingga sistem mereka rentan terhadap serangan.

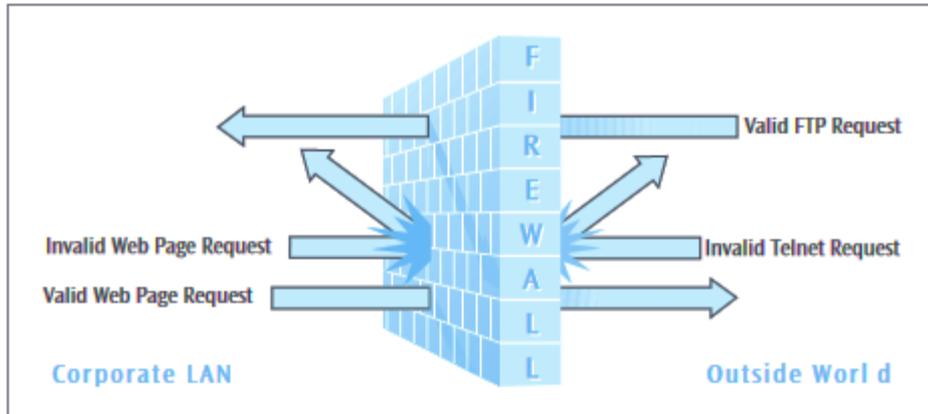
Teknik antivirus yang digunakan bersama dengan pemindaian berbasis tanda tangan dan pemantauan penghentian dan tetap tinggal adalah pemeriksaan integritas. Teknik ini merupakan kombinasi teknik antivirus seperti analisis checksum cerdas dan analisis virus sistem pakar. Analisis checksum cerdas menghitung dan menerapkan checksum ke file dan kumpulan data pada dua waktu utama dalam masa hidup file—di awal, ketika file masih baru (atau dalam kondisi aman), dan di lain waktu, setelah file telah ada selama beberapa waktu. Seperti pada cyclic checksum, checksum dari file saat masih baru dibandingkan dengan checksum selanjutnya untuk menentukan apakah file telah berubah karena tindakan virus. Analisis virus sistem pakar melibatkan serangkaian algoritma kepemilikan yang melakukan jutaan pengujian pada perangkat lunak Anda dan memeriksa aliran kode program dan fungsi perangkat lunak lainnya. Berdasarkan hasil pengujian tersebut, teknik antivirus ini memberikan sejumlah poin pada perangkat lunak yang bersangkutan dan menunjukkan adanya virus jika skor poin mencapai level tertentu.

Pengguna dapat menyederhanakan kerja perangkat lunak antivirus dengan tidak membiarkan serangan virus atau email yang terinfeksi memasuki sistem mereka. Mereka dapat melakukan hal ini dengan firewall, yang jika dipasang dengan benar, dapat berfungsi untuk mencegah orang jahat memasuki komputer mereka. Mari kita periksa firewall lebih dekat, dan lihat bagaimana firewall dapat memberikan tingkat perlindungan yang lebih tinggi kepada pengguna.

Firewall

Firewall adalah suatu sistem atau kombinasi sistem yang mendukung kebijakan kontrol akses antara dua jaringan. Kedua jaringan tersebut biasanya merupakan jaringan internal

perusahaan dan jaringan eksternal, seperti Internet. Firewall dapat membatasi pengguna di Internet untuk mengakses bagian tertentu dari jaringan perusahaan dan dapat membatasi pengguna internal untuk mengakses berbagai bagian Internet. Gambar 12-10 menunjukkan bagaimana firewall memblokir permintaan internal dan eksternal.



Gambar 12-10 Firewall saat menghentikan internal dan eksternal tertentu

Dalam lingkungan perusahaan di mana jaringan area lokal terhubung ke Internet, perusahaan mungkin ingin mengizinkan pesan email eksternal memasuki jaringan tetapi mungkin tidak ingin mengizinkan login jarak jauh ke jaringan perusahaan, karena penyusup yang mempelajari caranya untuk masuk ke aplikasi perusahaan dapat merusak sistem. Alternatifnya, perusahaan mungkin ingin melarang transfer file keluar dari jaringan perusahaan karena takut kehilangan data perusahaan atau rahasia dagang. Bagaimanapun, firewall, seperti yang akan Anda lihat, melibatkan lebih dari sekedar memprogram perangkat untuk menerima atau menolak jenis transaksi tertentu.

Fungsi Firewall

Jenis transaksi apa yang akan dihentikan oleh firewall, dan jenis transaksi apa yang tidak akan dihentikan? Sistem firewall mungkin saja menghentikan login jarak jauh serta email masuk atau keluar dan transfer file. Firewall juga dapat membatasi permintaan halaman Web yang masuk atau keluar. Ketika sebuah perusahaan telah membuat kebijakan keamanan—yang berarti telah memutuskan jenis transaksi mana yang harus dibatasi dan mana yang diperbolehkan—perusahaan dapat membuat sistem firewall yang mengizinkan atau melarang sejumlah besar transaksi tersebut.

Nomor port TCP menunjukkan layanan aplikasi mana yang diinginkan. Ketika suatu transaksi yang ditujukan untuk aplikasi tertentu memasuki suatu sistem, nomor port yang sesuai disertakan sebagai bagian dari transaksi. Beberapa penetapan nomor port yang umum adalah:

- Telnet, atau layanan login jarak jauh, biasanya menggunakan port 23.
- Finger, layanan untuk menemukan ID pengguna, sering kali menggunakan port 79.
- Usenet, layanan newsgroup, sering kali menggunakan port 119.
- Email biasanya port 25.

- Penjelajahan web yang menggunakan HTTP adalah port 80.

Jika sebuah perusahaan ingin memblokir orang luar yang mencoba melakukan Telnet ke dalam jaringannya, perusahaan tersebut dapat mengkonfigurasi firewalnya untuk menghentikan semua transaksi masuk yang meminta port 23. Atau perusahaan dapat menghentikan karyawannya menghabiskan waktu di Usenet dengan mengkonfigurasi firewall untuk memblokir semua transaksi keluar dengan nomor port 119.

Sayangnya, firewall tidak melindungi jaringan dari segala bentuk serangan yang mungkin terjadi. Karena virus dapat bersembunyi di dalam dokumen, kemungkinan besar virus tersebut tidak akan terdeteksi oleh firewall jika dokumen hostnya diizinkan masuk ke dalam sistem. Namun, beberapa sistem firewall membanggakan bahwa mereka dapat mendeteksi virus di dalam dokumen. Namun sistem ini jarang terjadi dan mungkin tidak mendeteksi semua virus yang ada saat ini.

Firewall juga tidak akan melindungi komputer atau jaringan dengan baik jika ada kemungkinan penyusup menghindari firewall dan memasuki sistem melalui rute alternatif. Misalnya, jika sistem jaringan mempunyai satu atau lebih modem dial-up yang bukan bagian dari sistem firewall, pelaku dapat melewati firewall dan mendapatkan akses ilegal. Mesin faks adalah cara lain yang melaluinya informasi sensitif dapat keluar dari perusahaan. Sistem firewall terbaik di dunia tidak akan menghentikan karyawan yang gigih untuk mengirimkan dokumen rahasia melalui faks melalui saluran telepon standar ke penerima luar. Agar sistem firewall dapat berfungsi, kebijakan keamanan komprehensif harus dibuat, diinstal, dan ditegakkan. Kebijakan keamanan ini harus mencakup pengelolaan semua kemungkinan masuk dan keluar dari lingkungan perusahaan, mulai dari komputer, telepon, dan sistem faks hingga orang yang membawa media secara fisik ke dalam dan ke luar gedung.

Tipe Firewall Dasar

Ada tiga tipe dasar firewall:

- Filter paket
- Server proksi
- Lapisan aplikasi

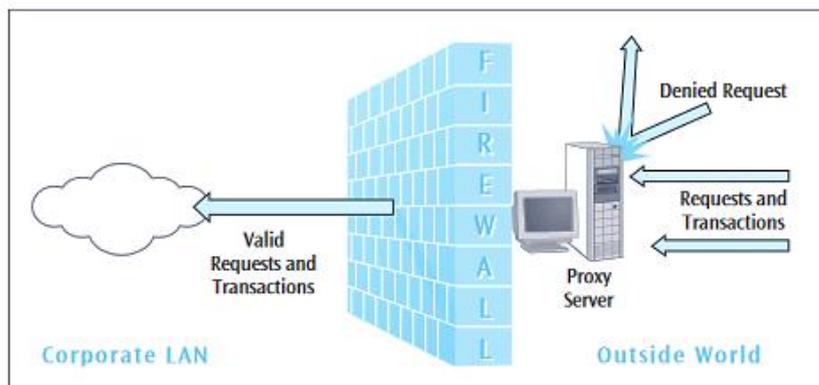
Firewall generasi pertama—filter paket—pada dasarnya adalah router yang telah diprogram untuk menyaring alamat IP atau nomor port TCP tertentu. Router jenis ini melakukan pemeriksaan statis terhadap alamat IP dan nomor port TCP, kemudian menolak transaksi atau mengizinkannya lewat berdasarkan informasi yang disimpan dalam tabel mereka. Router jenis ini memiliki desain yang relatif sederhana. Selain itu, mereka bertindak sangat cepat, namun agak terlalu sederhana untuk memberikan tingkat keamanan yang tinggi. Misalnya, relatif mudah bagi pengguna eksternal yang bertekad menyebabkan masalah jaringan internal untuk memalsukan filter paket statis dengan mengira dia adalah agen yang ramah.

Router (dan firewall) menjadi semakin cerdas selama bertahun-tahun, dan model modern bahkan dapat mengikuti alur percakapan antara entitas internal dan entitas eksternal. Kemampuan ini memungkinkan router modern mendeteksi spoofing. Router modern juga mulai memindai virus pada transaksi masuk.

Server proxy adalah perangkat firewall yang lebih kompleks. Server proxy adalah komputer yang menjalankan perangkat lunak server proxy, yang fungsinya mirip dengan pustakawan yang mengontrol akses ke buku di ruang buku langka di perpustakaan. Untuk menjaga agar buku-buku mahal tidak rusak akibat vandalisme atau penanganan yang ceroboh, banyak perpustakaan tidak mengizinkan pengunjung memasuki ruang buku langka mereka. Sebaliknya, seorang pelindung mengisi slip permintaan informasi dan menyerahkannya kepada pustakawan. Pustakawan memasuki ruang buku langka dan mengambil volume yang diminta. Pustakawan kemudian memfotokopi informasi yang diminta dari buku tersebut dan memberikan fotokopinya kepada pemustaka. Dengan demikian, pelindungnya tidak pernah bersentuhan dengan buku langka yang sebenarnya. Demikian pula, transaksi yang meminta firewall server proxy perusahaan tidak pernah bersentuhan dengan jaringan perusahaan. Setiap transaksi eksternal yang meminta sesuatu dari jaringan perusahaan harus terlebih dahulu mendekati server proxy. Server proxy membuat aplikasi yang disebut proxy yang masuk ke jaringan perusahaan untuk mengambil informasi yang diminta. Karena semua transaksi eksternal harus melalui server proxy, ini menyediakan cara yang sangat baik untuk membuat log audit.

Server proxy yang mendukung permintaan FTP memberikan contoh realistis. Ingat dari Bab Sepuluh bahwa FTP menggunakan dua koneksi jaringan—satu untuk mengontrol informasi dan satu lagi untuk transfer data. Ketika permintaan FTP masuk, proxy FTP memeriksa koneksi kontrol pada lapisan aplikasi, memutuskan perintah mana yang diperbolehkan atau ditolak, dan kemudian mencatat perintah individual. Ketika proxy menemukan perintah yang meminta koneksi kedua—koneksi transfer data—proxy menggunakan informasi kebijakan keamanan yang diprogram perusahaan untuk memutuskan apakah akan memfilter paket data.

Karena server proxy berada di luar jaringan perusahaan dan berbagai hambatan keamanannya, server proxy itu sendiri rentan terhadap vandalisme (Gambar 12-11). Untuk melindungi server proxy, perusahaan harus memastikan server proxy-nya adalah versi komputer jaringan yang disederhanakan. Oleh karena itu, seorang perusak tidak akan berbuat banyak untuk merugikan server proxy. Meskipun server proxy memberikan tingkat keamanan yang lebih tinggi, namun lebih lambat dibandingkan filter paket karena proxy harus dibuat untuk setiap jenis transaksi yang mungkin meminta data dari dalam jaringan perusahaan.



Gambar 12-11 Server proxy berada di luar perlindungan

Bentuk firewall terbaru adalah firewall lapisan aplikasi. Firewall ini memeriksa semua paket yang masuk atau keluar dari koneksi menggunakan lapisan aplikasi rangkaian protokol TCP/IP. Dengan kata lain, firewall lapisan aplikasi melampaui alamat IP dan nomor port TCP dan memeriksa setiap paket untuk melihat apakah paket tersebut milik suatu aplikasi. Manfaat tambahan dari menggali lebih dalam paket ini meningkatkan waktu pemrosesan firewall lapisan aplikasi. Di pasar saat ini, sangat umum untuk menemukan firewall yang beroperasi sebagai filter paket dan filter lapisan aplikasi.

Keamanan nirkabel

Jaringan area lokal telah ada selama bertahun-tahun. Selama tahun-tahun ini, kita telah melihat mereka berevolusi dari sistem server tunggal berbasis bus sederhana menjadi jaringan kompleks dengan switch lapisan dua dan lapisan tiga, sistem operasi jaringan canggih, dan banyak server. Meskipun jaringan area lokal tampaknya telah melewati masa-masa sulitnya, kita kini mengalami masalah yang sama dengan teknologi yang relatif lebih baru: jaringan area lokal nirkabel. Salah satu masalah terbesar yang dihadapi jaringan area lokal nirkabel adalah keamanan. Karena hampir semua orang dapat memiliki laptop nirkabel atau perangkat nirkabel lainnya, hampir tidak mungkin untuk mengontrol siapa yang dapat terhubung ke jaringan area lokal nirkabel dan dari mana. Oleh karena itu, keamanan nirkabel merupakan hal yang penting namun juga rumit.

Protokol keamanan pertama untuk LAN nirkabel adalah Wired Equivalency Protocol (WEP). Meskipun WEP merupakan langkah ke arah yang benar, WEP mempunyai dua kelemahan serius. Pertama, WEP menggunakan kunci enkripsi lemah yang panjangnya hanya 40 bit. Kedua, kuncinya bersifat statis, bukan dinamis. Kunci statis lebih mudah dipecahkan karena tidak mungkin diubah. Banyak administrator berpikir WEP sangat tidak memadai dan sulit untuk digunakan sehingga mereka memilih untuk tidak mempunyai mekanisme keamanan. Untungnya, WEP telah digantikan oleh standar baru, Wi-Fi Protected Access (WPA). WPA mempertahankan kunci enkripsi WEP berukuran 40-bit tetapi memiliki satu peningkatan signifikan: penyertaan fitur Temporal Key Integrity Protocol (TKIP) dan IEEE 802.1x, yang bersama-sama menyediakan enkripsi kunci dinamis dan otentikasi timbal balik untuk klien nirkabel. Jadi, meskipun kunci 40-bit masih belum terlalu kuat, kunci tersebut kini ditetapkan secara dinamis, dan klien nirkabel harus membuktikan bahwa mereka adalah pengguna yang sah sebelum dapat terhubung.

Bagaimanapun, WPA adalah standar sementara yang digunakan hingga standar keamanan yang lebih kuat disetujui dan diterapkan: IEEE 802.11i. IEEE 802.11i (juga disebut WPA2) mengatasi kelemahan WEP dengan mengizinkan kunci, algoritme enkripsi, dan negosiasi ditetapkan secara dinamis, dan dengan mengadopsi enkripsi AES berdasarkan algoritme Rijndael dengan 128-, 192-, atau 256-bit kunci. IEEE 802.11i didasarkan pada WPA dan jaringan keamanan yang kuat (RSN), perangkat lunak yang melakukan negosiasi kuat terhadap algoritma enkripsi dan otentikasi yang digunakan antara titik akses dan agen nirkabel.

12.7 MASALAH DESAIN KEBIJAKAN KEAMANAN

Ketika sebuah perusahaan merancang sistem firewall dan kebijakan keamanan terkait, sejumlah pertanyaan harus dijawab. Pertanyaan pertama menyangkut tingkat keamanan yang diharapkan oleh perusahaan. Apakah perusahaan mencoba mengizinkan akses hanya pada layanan yang dianggap penting bagi bisnisnya? Atau apakah perusahaan ingin mengizinkan semua atau sebagian besar jenis transaksi, sehingga memerlukan sistem firewall hanya untuk mengaudit transaksi dan membuat permintaan transaksi yang teratur? Mengizinkan akses hanya pada layanan yang dianggap penting memerlukan sistem firewall yang lebih rumit sehingga memerlukan lebih banyak pekerjaan dan biaya. Mengizinkan sebagian besar jenis transaksi berlangsung memerlukan sistem firewall sederhana yang hanya melakukan operasi manajemen antrian dan membuat jejak audit. Untuk menentukan tingkat keamanan yang sesuai yang dibutuhkan, perusahaan harus menilai sifat datanya. Lebih tepatnya, perusahaan harus menentukan seberapa aman datanya. Selain itu, ia harus memutuskan apakah semua data ini atau hanya bagian tertentu saja yang harus diamankan. Langkah pemeriksaan data dan menetapkan tingkat keamanan bagi perusahaan dan operasinya biasanya memakan waktu dan biaya.

Keputusan mengenai tingkat keamanan mengarah pada pertanyaan kedua: Berapa banyak uang yang bersedia diinvestasikan perusahaan dalam sistem firewall? Sistem firewall yang dibeli secara komersial bisa jadi kuat, rumit, dan mahal. Namun, dimungkinkan untuk membangun sistem firewall internal yang memanfaatkan kemampuan sumber daya yang ada, seperti sistem operasi jaringan dan router. Seperti yang kita pelajari sebelumnya, sistem operasi jaringan dapat digunakan untuk membatasi akses ke suatu sistem berdasarkan waktu, hari, dan lokasi. Dimungkinkan juga untuk menggunakan perangkat lunak yang ada untuk membuat jejak audit atas semua transaksi masuk dan keluar. Tergantung pada tingkat detail audit yang diperlukan, perusahaan dapat membeli dan menginstal perangkat lunak tambahan yang akan bekerja bersama dengan perangkat lunak sistem operasi jaringan untuk menyediakan tingkat audit yang diinginkan.

Seperti sistem operasi jaringan, banyak router dapat diprogram untuk membatasi akses ke jenis lalu lintas tertentu. Router dapat diprogram untuk menerima dan menolak permintaan dengan alamat IP tertentu atau rentang alamat IP. Router juga dapat diprogram untuk menolak akses ke alamat port tertentu di tingkat TCP.

Pertanyaan ketiga yang harus dijawab oleh perusahaan berkaitan dengan komitmennya terhadap keamanan. Apakah perusahaan cukup serius dalam membatasi akses ke jaringan perusahaan sehingga tidak hanya mengamankan pintu masuk ke jaringan yang berhubungan dengan Internet, namun juga mendukung keamanan setiap dan semua tautan lain ke lingkungan jaringan perusahaan? Dengan kata lain, ketika mengambil keputusan keamanan, perusahaan juga harus mempertimbangkan akses ke modem dial-up, jaringan nirkabel, dan link telekomunikasi lainnya. Mesin faks, baik yang berdiri sendiri maupun berbasis komputer, serta media disk yang dapat dipindahkan, adalah dua contoh cara data masuk atau keluar dari suatu perusahaan. Kebijakan keamanan harus mempertimbangkan titik masuk dan keluar ini, serta Internet.

Memiliki kebijakan keamanan yang dirancang dengan baik akan membuat pekerjaan staf pendukung jaringan menjadi lebih jelas. Kebijakan keamanan yang dirancang dengan baik akan membuat penegakan hukum menjadi lebih mudah, dan akan memungkinkan staf untuk bereaksi dengan baik terhadap permintaan keamanan tertentu. Staf karyawan akan mengetahui apa yang dapat dan tidak dapat diakses oleh pengguna jaringan, dan ke mana mereka dapat dan tidak dapat pergi. Kebijakan tersebut juga akan memperjelas tujuan dan tugas karyawan jaringan ketika mereka harus menegakkan keamanan sehubungan dengan permintaan dari luar.

Jika ada kebijakan keamanan yang baik, maka pengguna korporat sendiri akan memiliki pemahaman yang lebih baik tentang apa yang bisa dan tidak bisa mereka lakukan. Pemahaman ini diharapkan dapat membantu anggota staf jaringan dalam melakukan pekerjaan mereka dan memungkinkan perusahaan menjaga keamanan di dunia yang semakin tidak aman.

Mungkin karena banyak perusahaan mempunyai kebijakan keamanan yang dirancang dengan baik, banyak orang yang menggunakan Internet untuk membeli barang secara online cukup yakin bahwa ketika mereka mentransfer informasi kartu kredit selama sesi aman, data mereka aman dari peretas dan pihak lain. penyadap. (Hal ini terjadi meskipun penyimpanan informasi kartu kredit dalam database perusahaan telah menjadi perhatian serius, dengan sejumlah pembobolan database yang dipublikasikan secara luas.) Namun, rasa aman ini dapat berubah, seiring dengan dibentuknya Satuan Tugas Rekayasa Internet. sedang mempertimbangkan proposal yang memungkinkan pembuatan pintu belakang masuk ke semua lalu lintas Internet. Entri pintu belakang ini akan memungkinkan orang yang berwenang untuk mencegat lalu lintas data apa pun di Internet. Karena penggunaan backdoor jelas merupakan pelanggaran privasi, mengapa ada orang yang mau mengusulkan hal seperti itu? Inti argumennya adalah fakta bahwa sistem telepon standar saat ini memungkinkan lembaga-lembaga pemerintah AS untuk menyadap komunikasi.

Penyadapan telepon ini terjadi di kantor pusat telepon dan dibangun pada saklar telepon kantor pusat. Undang-undang yang memperbolehkan penyadapan, yaitu Undang-Undang Bantuan Komunikasi untuk Penegakan Hukum, telah ada sejak tahun 1994. Para pendukung usulan masuk pintu belakang beralasan bahwa, saat ini Internet mulai menyalurkan lalu lintas suara, maka pemerintah mempunyai wewenang untuk melakukan penyadapan. transaksi suara penyadapan telepon harus meluas ke Internet. Namun seperti yang diperingatkan oleh para pengkritik proposal tersebut, jika pemerintah dapat memanfaatkan suara, maka pemerintah juga dapat memanfaatkan data. Kritikus juga menunjukkan bahwa jika perancang Internet menciptakan pintu belakang seperti itu, akses pintu belakang ini bisa jatuh ke tangan yang salah dan digunakan untuk tujuan kriminal.

Masalah ini semakin diperumit oleh kenyataan bahwa banyak bisnis saat ini mengenkripsi semua data yang keluar dari jaringan perusahaan mereka. Kebanyakan teknik enkripsi yang digunakan oleh dunia usaha sangat efektif sehingga hampir tidak ada seorang pun, termasuk pemerintah, yang dapat memecahkannya. Dalam kasus di mana enkripsi ini dilakukan oleh jaringan tepat sebelum data meninggalkan batas perusahaan, personel

pendukung jaringan perusahaan bertanggung jawab untuk memberikan data yang tidak terenkripsi kepada pemerintah AS, jika diminta. Sebaliknya, jika enkripsi diterapkan pada stasiun kerja pengguna sebelum data dimasukkan ke dalam jaringan perusahaan, tidak jelas siapa yang harus memasok data yang tidak terenkripsi kepada pemerintah. Jelasnya, isu ini akan hangat diperdebatkan dalam beberapa waktu ke depan.

Meskipun perusahaan mungkin sudah mempunyai kebijakan keamanan yang dirancang dengan baik, kejadian eksternal selalu menjadikan hal ini semakin kompleks.

12.8 MEMBUAT KEAMANAN LAN NIRKABEL

Terakhir kali kita melihat Hannah adalah di Bab Delapan, ketika dia sedang memeriksa kandidat yang mungkin untuk memilih sistem operasi jaringan untuk perusahaannya. Kini perusahaan Hannah sedang mempertimbangkan untuk menawarkan layanan jaringan area lokal nirkabel kepada karyawan dan staf administrasinya. Pertanyaannya adalah: Bagaimana jaringan area lokal nirkabel dibuat aman dari pengguna yang tidak berwenang? Ini adalah masalah yang juga dihadapi oleh universitas, dunia usaha, dan bahkan pemilik rumah. Lebih tepatnya, masalahnya adalah: Bagaimana Anda menjaga keamanan jaringan nirkabel Anda dari driver perang? War driver adalah pengguna yang tidak sah, yang menggunakan perangkat nirkabel mereka, mencoba menyambung ke jaringan nirkabel seseorang untuk mendapatkan akses gratis ke Internet atau untuk mencuri dan merusak file.

Seperti yang telah kita lihat, WEP terlalu lemah untuk menjadi protokol keamanan nirkabel yang serius. Hal ini didasarkan pada algoritma yang disebut RC4, yang tampaknya cukup mudah untuk dipecahkan. Meskipun WEP ditingkatkan dari penggunaan kunci 40-bit menjadi kunci 128-bit, individu dapat memecahkan kunci yang lebih besar dengan perangkat lunak dan ketekunan. Kerugian tambahan dari WEP adalah kuncinya bersifat statis, artinya ketika perangkat nirkabel terhubung dengan titik akses nirkabel, kuncinya tidak pernah berubah, sehingga lebih mudah untuk disadap dan didekode.

Hannah dapat mempertimbangkan untuk menggunakan LEAP (Lightweight Extensible Authentication Protocol) Cisco sebagai protokol nirkabel. Sayangnya, LEAP bukanlah perangkat lunak standar, melainkan perangkat lunak berpemilik, dan memiliki masalah interoperabilitas dengan perangkat lain. Hannah pasti ingin menggunakan perangkat lunak yang telah diterima oleh organisasi pembuat standar. WPA dibuat oleh Wi-Fi Alliance. Penerimaan WPA telah dipercepat oleh fakta bahwa Wi-Fi Alliance telah menuntut agar mekanisme keamanan WPA diwajibkan untuk semua sertifikasi Wi-Fi baru.

Meskipun WPA menggunakan enkripsi RC4 yang sama dengan WEP, WPA menyertakan TKIP, yang memutar kunci sehingga memperkuat proses enkripsi. Namun WPA bukannya tanpa masalah. Hannah mendapati bahwa sistem tersebut mungkin tidak kompatibel dengan sistem operasi jaringan lama—yang sebenarnya bukan masalah baginya, karena dia baru saja menginstal versi terbaru dari sistem operasi jaringan populer. Dia juga mengetahui bahwa beberapa asisten digital pribadi mungkin tidak memiliki kekuatan pemrosesan yang cukup untuk WPA; namun karena perusahaannya belum mengeluarkan PDA kepada karyawannya, hal ini juga tidak menjadi masalah bagi Hannah—setidaknya belum.

Potensi masalah bagi Hannah adalah WPA menurunkan kinerja perangkat. Setelah seluruh upayanya untuk membuat pilihan terbaik untuk sistem jaringan area lokal perusahaannya, dia tidak suka menghadapi penurunan kinerja.

Untungnya, IEEE 802.11i, atau WPA2, kini tersedia untuk LAN nirkabel. Dengan metode enkripsi yang lebih kuat dan algoritma yang lebih cepat, sulit dikalahkan. Ini jelas terlihat sebagai perangkat lunak enkripsi terbaik untuk jaringan area lokal nirkabel. Mudah-mudahan dia tidak akan menemui terlalu banyak masalah kompatibilitas karena standar tersebut telah ada selama beberapa tahun.

Oleh karena itu, Hannah sedang mempertimbangkan untuk menginstal WPA2 di jaringan perusahaannya. Pertanyaan selanjutnya adalah: Di perangkat apa sebaiknya WPA2 diinstal? Agar jaringan nirkabel diamankan dengan baik, perangkat lunak keamanan harus beroperasi pada tiga titik berbeda dalam sistem: pada laptop nirkabel pengguna, pada titik akses nirkabel (koneksi antara pengguna nirkabel dan jaringan kabel), dan pada titik akses nirkabel server jaringan. Untungnya, perangkat lunak yang mendukung ketiga poin dalam sistem kini telah tersedia.

Hannah membeli dan menginstal sistem nirkabel WPA2 miliknya. Karena kata sandi dapat diberikan secara dinamis, dia cukup yakin bahwa jaringan perusahaan akan aman dari pengemudi perang di luar gedung. Para karyawan menikmati kebebasan baru mereka dalam memindahkan komputer laptop mereka secara nirkabel ke mana saja di dalam gedung.

RINGKASAN

- Keamanan jaringan terus menjadi topik yang semakin penting, khususnya dengan meningkatnya interkoneksi jaringan. Internet telah membantu membuka pintu bagi para pengacau di seluruh dunia, membuat sistem apa pun yang terhubung dengannya rentan terhadap serangan.
- Tiga serangan sistem yang umum adalah (1) menyerang kerentanan sistem operasi dan perangkat lunak aplikasi yang diketahui, (2) membombardir sistem sehingga tidak mampu menjalankan tugas normalnya (serangan penolakan layanan), dan (3) menggunakan pengguna yang valid akun untuk tujuan yang tidak sah.
- Personel dan pengguna jaringan harus menyadari (dan mengambil) tindakan perlindungan fisik, seperti menempatkan peralatan di lokasi yang tepat, untuk melindungi sistem mereka dari potensi banjir, vandalisme, dan faktor lingkungan merugikan lainnya. Tindakan perlindungan fisik lainnya seperti sistem pengawasan juga dapat mencegah vandalisme dan pencurian peralatan secara efektif.
- Mengontrol akses ke sistem komputer dan jaringannya merupakan aspek penting dari keamanan jaringan. Ada langkah-langkah keamanan jaringan yang memungkinkan administrator jaringan membatasi waktu, hari dalam seminggu, dan lokasi di mana seseorang dapat masuk ke sistem komputer.
- Kata sandi dan sistem ID lainnya merupakan teknik keamanan pengendalian akses yang sangat umum, namun kata sandi dapat dicuri dan digunakan oleh pihak yang tidak

bertanggung jawab. Teknik biometrik yang menggunakan beberapa bagian tubuh untuk mengidentifikasi seseorang lebih aman dibandingkan sistem kata sandi.

- Kebanyakan sistem komputer menerapkan hak akses terhadap sumber daya sistem dan pengguna. Dengan mengatur hak akses dengan benar, administrator jaringan dapat membuat sumber daya komputer menjadi lebih aman.
- Perangkat lunak yang melakukan audit berkelanjutan terhadap transaksi jaringan menciptakan jejak elektronik yang dapat digunakan perusahaan ketika mereka mencoba menangkap pengguna jahat.
- Memberikan keamanan pada data sistem sama pentingnya dengan mengamankan sistem itu sendiri. Teknologi enkripsi menyediakan serangkaian teknik penting yang dapat membantu memerangi penipuan komputer. Sandi berbasis substitusi menggantikan satu huruf atau rangkaian huruf dalam sebuah pesan dengan huruf atau rangkaian huruf kedua. Cipher berbasis transposisi mengatur ulang urutan huruf dalam sebuah pesan.
- Kriptografi kunci publik menggunakan dua kunci: satu kunci untuk menyandikan pesan dan kunci kedua untuk memecahkan kode pesan. Secure Sockets Layer, suatu bentuk kriptografi kunci publik, digunakan untuk mengenkripsi data yang berjalan bolak-balik antara server Web dan browser Web.
- Standar Enkripsi Data dibuat pada tahun 1977 dan menggunakan kunci 56-bit untuk mengenkripsi data yang dikirimkan antara dua lokasi bisnis. Standar Enkripsi Lanjutan telah menggantikan Standar Enkripsi Data dan memberikan tingkat perlindungan yang jauh lebih tinggi.
- Tanda tangan digital menggunakan kriptografi kunci publik dan dapat digunakan untuk memverifikasi bahwa suatu dokumen adalah milik orang tertentu.
- Pretty Good Privacy adalah perangkat lunak enkripsi gratis yang memungkinkan pengguna biasa serta pengguna komersial untuk mengenkripsi dan mendekripsi transmisi sehari-hari.
- Kerberos adalah teknik enkripsi kunci rahasia yang dapat digunakan oleh program aplikasi komersial untuk memverifikasi bahwa pengguna adalah siapa yang dia klaim.
- Infrastruktur kunci publik menggunakan kriptografi kunci publik, tanda tangan digital, dan sertifikat digital untuk memungkinkan jalur data yang aman melalui jaringan yang tidak aman.
- Steganografi adalah studi tentang menyembunyikan data rahasia di dalam dokumen yang tidak terkait—misalnya, menyembunyikan potongan pesan di dalam piksel suatu gambar.
- Selain mengamankan data jaringan, komunikasi jaringan juga harus aman. Teknologi spektrum tersebar adalah teknik menyebarkan data dan sinyalnya pada rentang frekuensi yang lebih luas untuk membuat transmisi aman. Ketika sinyal ditransmisikan menggunakan teknik spektrum penyebaran frekuensi hopping, sinyal tersebut terus berpindah dari satu frekuensi ke frekuensi lainnya untuk mencegah penyadapan, gangguan transmisi, atau intervensi jahat lainnya. Ketika sinyal ditransmisikan

menggunakan teknik spektrum penyebaran urutan langsung, angka 1 dan 0 dari data asli diubah menjadi urutan bit yang lebih panjang.

- Untuk mengamankan komunikasi, administrator jaringan dan pengguna harus waspada terhadap serangan komputer standar dan virus yang dapat merusak sistem komputer. Mereka juga harus mengetahui perangkat lunak dan perangkat keras yang dapat membantu melindungi sistem dan penggunanya dari serangan komputer dan virus. Pemindai virus memiliki tiga bentuk dasar: pemindaian berbasis tanda tangan, pemantauan penghentian dan tetap tinggal, dan pemeriksaan integritas.
- Cara lain untuk mengamankan komunikasi adalah firewall, suatu sistem atau kombinasi sistem yang mendukung kebijakan kontrol akses antara dua jaringan. Firewall hadir dalam tiga tipe dasar: (1) filter paket, yang memeriksa semua transmisi masuk dan keluar dan menyaring transmisi yang dianggap ilegal; (2) server proxy, yaitu komputer yang berjalan di pintu masuk jaringan komputer dan bertindak sebagai penjaga gerbang ke dalam jaringan perusahaan; dan (3) firewall berbasis aplikasi yang mengikuti paket tingkat aplikasi masuk dan keluar dari suatu situs.
- Standar keamanan jaringan nirkabel mencakup WPA dan WPA2 (IEEE 802.11i), yang kuat dan kokoh, serta memberikan perlindungan kunci dinamis dan otentikasi pengguna.
- Desain keamanan jaringan yang tepat membantu staf jaringan perusahaan dengan secara jelas menggambarkan transaksi jaringan mana yang diserahkan oleh karyawan internal dan pengguna eksternal yang dapat diterima.

PERTANYAAN

1. Bagaimana cara peretas mengeksploitasi kerentanan sistem operasi?
2. Apa itu kuda Troya?
3. Bagaimana cara kerja serangan penolakan layanan?
4. Apa itu spoofing dan bagaimana penerapannya pada serangan penolakan layanan?
5. Apa yang dimaksud dengan badai ping, dan bagaimana penerapannya pada serangan penolakan layanan?
6. Sebutkan tiga bentuk perlindungan fisik.
7. Bagaimana pengawasan dapat digunakan untuk meningkatkan keamanan jaringan?
8. Bagaimana cara kerja sistem deteksi intrusi?
9. Apa kelemahan utama sistem kata sandi? Apa kekuatan utamanya?
10. Jenis hak akses apa yang paling umum?
11. Bagaimana audit dapat digunakan untuk melindungi sistem komputer dari penggunaan yang tidak sah?
12. Jelaskan contoh sederhana sandi berbasis substitusi.
13. Jelaskan contoh sederhana sandi berbasis transposisi.
14. Bagaimana kriptografi kunci publik dapat membuat sistem lebih aman?
15. Berikan contoh umum aplikasi yang menggunakan Secure Sockets Layer.
16. Apa yang dimaksud dengan Standar Enkripsi Data?
17. Apa perbedaan Standar Enkripsi Lanjutan dengan Standar Enkripsi Data?

18. Apa yang dimaksud dengan tanda tangan digital?
19. Aplikasi apa saja yang dapat memanfaatkan Pretty Good Privacy?
20. Apakah Kerberos merupakan teknik enkripsi kunci publik atau kunci pribadi? Menjelaskan.
21. Sebutkan elemen dasar infrastruktur kunci publik.
22. Aplikasi seperti apa yang dapat memperoleh manfaat dari infrastruktur kunci publik?
23. Entitas apa yang menerbitkan sertifikat?
24. Dalam keadaan apa sertifikat dapat dicabut?
25. Bagaimana steganografi digunakan untuk menyembunyikan pesan rahasia?
26. Apa sajakah dua bentuk teknologi spektrum tersebar?
27. Apa yang dimaksud dengan virus komputer, dan apa saja jenis virus komputer yang utama?
28. Apa saja teknik berbeda yang digunakan untuk menemukan dan menghentikan virus?
29. Apa tanggung jawab utama firewall?
30. Apa tiga tipe dasar firewall?
31. Apa keuntungan menerapkan kebijakan keamanan?

LATIHAN SOAL

1. Sebuah universitas besar di Illinois biasa meletakkan hasil komputer dari pekerjaan mahasiswa di atas meja di ruang komputer. Ruang ini merupakan ruang komputer yang sama yang menampung seluruh komputer mainframe kampus dan perangkat pendukungnya. Siswa akan memasuki ruangan, mengambil pekerjaan mereka, dan pergi. Masalah keamanan macam apa yang mungkin dihadapi oleh layanan komputer dengan sistem seperti ini?
2. Anda lupa kata sandi Anda, jadi Anda menghubungi meja bantuan dan meminta perwakilan untuk mengambil kata sandi Anda. Setelah beberapa saat, perwakilan pusat bantuan memberi tahu Anda kata sandi Anda yang terlupa. Apa yang baru saja terjadi, dan apa maknanya?
3. Buat (di atas kertas) contoh sederhana sandi berbasis substitusi.
4. Buat (di atas kertas) contoh sederhana sandi berbasis transposisi.
5. Dengan menggunakan sandi Vigenère dan kunci NETWORK, kodekan frasa "ini adalah kelas yang menarik".
6. Dengan menggunakan contoh sandi berbasis transposisi yang dijelaskan dalam bab ini dan kunci yang sama, KOMPUTER, kodekan frasa "Ulang tahun hanya boleh datang setahun sekali".
7. Anda menggunakan browser Web dan ingin membeli CD musik dari pengecer elektronik. Pengecer meminta nomor kartu kredit Anda. Sebelum Anda mentransfer nomor kartu kredit Anda, browser memasukkan koneksi aman. Urutan kejadian apa yang menciptakan koneksi aman?
8. Anda ingin menulis sebuah lagu dan membubuhkan tanda tangan digital pada lagu tersebut, sehingga nantinya Anda dapat membuktikan bahwa itu adalah lagu Anda.

- Bagaimana Anda menerapkan tanda tangan; dan selanjutnya, bagaimana Anda menggunakannya untuk membuktikan bahwa lagu tersebut adalah milik Anda?
9. Sebutkan tiga contoh (selain yang tercantum dalam bab ini) tindakan sehari-hari yang mungkin mendapat manfaat dari penerapan PKI.
 10. Dapatkah firewall memfilter permintaan ke alamat IP tertentu, alamat port, atau keduanya? Apa bedanya?
 11. Salah satu fitur firewall adalah kemampuannya untuk menghentikan paket IP keluar, menghapus alamat IP asli, memasukkan alamat IP “palsu”, dan mengirimkan paket dalam perjalanannya. Bagaimana cara kerja fitur ini? Apakah menurut Anda ini akan efektif?
 12. Bagaimana ukuran kunci mempengaruhi kekuatan dan kelemahan teknik enkripsi? Pertimbangkan penggunaan kunci yang ramah dan penggunaan kunci yang tidak ramah.
 13. Asumsikan sebuah kunci berukuran 56 bit. Jika komputer memerlukan waktu 0,00024 detik untuk mencoba setiap kunci, berapa lama waktu yang diperlukan untuk mencoba semua kemungkinan kunci? Bagaimana jika 10.000 komputer bekerja sama untuk mencoba semua kunci?
 14. Apa jawaban dari pertanyaan pada Latihan 13 jika panjang kuncinya 128 bit?
 15. Anda ingin menyembunyikan pesan rahasia di dalam file gambar menggunakan steganografi. Anda telah memutuskan untuk menempatkan sedikit demi sedikit dari pesan ke dalam piksel gambar. Bagaimana Anda akan memilih piksel? Apakah semuanya akan dilakukan secara acak atau berturut-turut? Dan setelah satu piksel dipilih, bit manakah yang akan Anda ganti dengan bit dari pesan rahasia? Mengapa?
 16. Mengapa urutan yang benar-benar acak tidak dapat digunakan dalam sistem spektrum penyebaran frekuensi hopping?

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Buat skema pengkodean yang terdiri dari sandi berbasis substitusi, sandi berbasis transposisi, atau keduanya. Encode pesan “Temui aku di depan kebun binatang pada tengah malam”. Jelaskan teknik pengkodean Anda.
2. Ciptakan bisnis hipotetis dengan sekitar 50 hingga 100 karyawan. Tempatkan karyawan di dua atau tiga departemen berbeda. Tetapkan ke setiap departemen judul dan tugas pekerjaan dasar. Semua karyawan di semua departemen menggunakan komputer pribadi untuk berbagai aktivitas. Identifikasi aktivitas komputer untuk karyawan setiap departemen. Kemudian membuat kebijakan keamanan untuk karyawan masing-masing departemen. Pastikan untuk mengetahui kapan dan di mana karyawan memiliki akses ke sumber daya komputer, dan apakah jenis transaksi apa pun harus dibatasi.
3. Anda bekerja di perusahaan yang mengizinkan karyawannya mengakses sumber daya komputasi dari lokasi jarak jauh, dan mengizinkan pemasok mengirim dan menerima transaksi pesanan secara online. Perusahaan Anda sedang mempertimbangkan untuk

- memasukkan PKI. Bagaimana Anda merekomendasikan agar PKI diterapkan untuk mendukung kedua bidang penerapan ini?
4. Anda memiliki komputer di rumah dengan NIC nirkabel dan router nirkabel. Buat daftar semua langkah keamanan yang harus diterapkan agar jaringan rumah Anda aman.
 5. Atasan Anda meminta Anda mendalami konsep pengelolaan ID untuk perusahaan. Apa yang terlibat? Bagaimana hubungannya dengan topik keamanan? Apakah masuk akal bagi perusahaan untuk mempertimbangkan penerapan manajemen ID, atau apakah konsep ini terlalu baru (dan karena itu terlalu berisiko) untuk dipertimbangkan oleh bisnis yang masih berfungsi?
 6. Beberapa perusahaan menggunakan model pencegahan/deteksi/koreksi untuk membangun keamanan perusahaan. Bagaimana model ini beroperasi? Bisakah Anda memberikan contoh masing-masing dari ketiga kategori tersebut? Jika Anda saat ini bekerja, menurut Anda bagaimana perusahaan Anda cocok dengan model ini? Jika Anda seorang pelajar yang mengambil program kuliah, bagaimana perguruan tinggi atau universitas Anda sesuai dengan model ini?
 7. Temukan dan laporkan tiga teknik keamanan berbeda yang menggunakan sebagian karakteristik fisik seseorang untuk verifikasi.
 8. Deteksi intrusi adalah area keamanan jaringan yang populer. Sejumlah perusahaan menawarkan sistem perangkat lunak yang melakukan deteksi intrusi. Tulis makalah satu hingga dua halaman yang merangkum cara kerja sistem deteksi intrusi.
 9. Apa saja hak akses yang diperbolehkan untuk melindungi file dan objek lain pada sistem komputer di sekolah atau tempat kerja Anda? Buat daftar pilihan untuk “siapa” dan “bagaimana”.
 10. Buat daftar singkat beberapa virus terbaru yang menyebar di dalam makro aplikasi.
 11. Laporan status terkini standar enkripsi untuk bisnis yang mengirim data ke luar negeri. Apakah dunia usaha menginginkan pembatasan yang lebih kuat dalam pengiriman materi terenkripsi ke luar negeri, atau pembatasan yang lebih lemah? Apa posisi pemerintah? Jenis dokumen terenkripsi apa yang saat ini diizinkan oleh pemerintah untuk diekspor oleh perusahaan?
 12. Privasi Cukup Bagus dapat digunakan sebagai bentuk infrastruktur kunci publik. Jelaskan hubungan PGP dan PKI.
 13. Apa itu chip pemotong? Apakah hal itu pernah membuahkan hasil? Menjelaskan.
 14. Kadang-kadang Anda mendengar virus yang bukan virus melainkan hoax. Temukan situs Web yang berisi daftar virus tipuan dan laporkan beberapa virus yang lebih menarik.
 15. Apa sajakah teknologi spektrum tersebar lainnya selain frekuensi hopping dan direct sequence? Pastikan untuk mencantumkan sumber Anda.

BAB 13

DESAIN DAN MANAJEMEN JARINGAN

TUJUAN

Setelah membaca bab ini, Anda seharusnya dapat:

- Kenali Siklus Hidup Pengembangan Sistem dan tentukan setiap fasenya
- Jelaskan pentingnya membuat satu atau lebih peta konektivitas
- Uraikan perbedaan antara kelayakan teknis, finansial, operasional, dan waktu
- Membuat analisis biaya-manfaat yang menggabungkan nilai waktu dari uang
- Jelaskan mengapa melakukan perencanaan kapasitas dan analisis lalu lintas itu sulit
- Jelaskan langkah-langkah yang terlibat dalam melakukan studi dasar
- Diskusikan pentingnya administrator jaringan dan keterampilan yang dibutuhkan untuk posisi tersebut
- Menghitung keandalan dan ketersediaan komponen dan sistem
- Kenali alat diagnostik jaringan perangkat keras dan perangkat lunak dasar
- Jelaskan pentingnya meja bantuan sehubungan dengan pengelolaan operasi jaringan
- Sebutkan fitur-fitur utama *Simple Network Management Protocol* (SNMP) dan bedakan antara manajer dan agen
- Jelaskan penggunaan protokol Remote Network Monitoring (RMON) dan hubungannya dengan SNMP

Misalkan Anda adalah administrator jaringan atau analis sistem untuk perusahaan Anda, dan Anda perlu meminta uang kepada atasan Anda untuk membeli sistem jaringan baru atau peralatan baru. Majalah Network Computing menawarkan enam tip tentang cara membuat promosi yang efektif dalam kasus seperti ini:

Kenali orang-orang yang memegang kendali: Jika manajemen cenderung meminta model ROI (laba atas investasi) yang terperinci untuk permintaan Anda, maka buatlah model tersebut. Jika manajemen lebih fleksibel, Anda tetap harus mempertimbangkan untuk mendukung permintaan Anda dengan menyiapkan kasus bisnis yang tidak terlalu formal yang menunjukkan manfaat dan biaya subjektif dari pembelian baru.

Hitung jika memungkinkan: Karena membuat ROI yang valid bisa jadi sulit, jika Anda perlu membuatnya, Anda sebaiknya berkonsentrasi pada biaya dan manfaat yang dapat diukur dengan jelas dan sah.

Libatkan departemen keuangan: Jika Anda bisa mendapatkan akuntan perusahaan di pihak Anda di awal permainan (untuk memvalidasi perhitungan Anda dan mendukung permintaan Anda), itu akan membantu posisi Anda.

Lakukan riset: Bicaralah dengan siapa pun di perusahaan yang mungkin terlibat atau mendapat manfaat dari akuisisi sistem atau peralatan komputer baru. Pastikan untuk menggunakan informasi ini untuk membangun kasus Anda.

Bahkan lapangan permainannya: Gunakan penilaian nilai yang sesuai untuk jenis sistem yang diminta. Misalnya, untuk produk atau sistem terkait keamanan, Anda dapat menggunakan model penilaian berbasis risiko.

Menghasilkan bukti kualitatif: Kumpulkan kesaksian yang mendukung pembelian dari berbagai sumber, seperti karyawan lain yang mungkin mendapat manfaat dari penggunaan sistem dan manajer perusahaan mana pun yang mungkin sudah menggunakan produk baru. Untuk mendukung kasus Anda, Anda mungkin juga mempertimbangkan untuk menyelidiki apakah perusahaan lain (terutama pesaing) menggunakan produk tersebut.

Seberapa sulitkah menghitung ROI untuk produk baru?

Apakah para profesional mengikuti prosedur ketika mereka mengusulkan dan merancang sistem komputer?

13.1 PENDAHULUAN

Agar jaringan komputer berhasil, jaringan tersebut harus mampu mendukung jumlah lalu lintas saat ini dan masa depan, membayar sendiri dalam jangka waktu yang dapat diterima, dan menyediakan layanan yang diperlukan untuk mendukung pengguna sistem. Semua tujuan ini sangat sulit untuk dicapai. Mengapa? Pertama, jaringan komputer terus meningkat kompleksitasnya. Di banyak lingkungan bisnis, sangat sulit bagi satu orang untuk memahami sepenuhnya setiap komponen, protokol, dan aplikasi jaringan. Dengan demikian, manajemen jaringan menjadi semakin menantang.

Alasan kedua terkait dengan betapa sulitnya bagi individu atau bisnis untuk menentukan masa depan komputasi dalam suatu perusahaan dengan tepat. Setiap perusahaan memiliki harapannya sendiri mengenai layanan komputasi apa yang harus disediakan. Selain itu, setiap pengguna dalam perusahaan memiliki gagasannya sendiri tentang layanan komputasi yang harus tersedia. Oleh karena itu, sangatlah sulit untuk menentukan satu layanan atau serangkaian layanan yang dapat melayani kebutuhan seluruh perusahaan. Terakhir, teknologi jaringan komputer berubah dengan kecepatan sangat tinggi. Di beberapa daerah, perkembangan besar diperkirakan terjadi setiap enam bulan; dan di bidang lain, teknologi baru bermunculan hampir setiap hari. Mengikuti perkembangan perangkat keras, perangkat lunak, dan aplikasi jaringan baru merupakan pekerjaan penuh waktu. Memasukkan teknologi baru ke dalam teknologi yang sudah ada, sambil mencoba menebak kebutuhan pengguna, sangatlah melelahkan. Lingkungan yang selalu berubah ini adalah salah satu alasan utama mengapa merancang sistem baru dan memperbarui sistem yang ada saat ini merupakan area yang penuh dengan jebakan berbahaya. Dengan satu keputusan yang salah, banyak waktu dan uang yang terbuang sia-sia.

Sebagian besar topik yang diperkenalkan dalam bab ini berasal dari bidang studi yang sangat luas. Bidang perencanaan, analisis, perancangan, dan penerapan solusi berbasis komputer, misalnya, sering kali merupakan subjek dari keseluruhan mata kuliah atau serangkaian mata kuliah dua semester. Oleh karena itu, bab ini tidak akan mampu membahas topik-topik ini secara mendalam. Meskipun demikian, kami akan mencoba melakukan survei

lapangan untuk memberi Anda pemahaman tentang konsep dasar yang terlibat dalam menciptakan solusi berbasis komputer.

Mengapa penting untuk memahami konsep dasar yang digunakan untuk mengembangkan sistem komputer? Konsep-konsep ini penting karena, jika Anda mengejar karir yang melibatkan jaringan komputer, ada kemungkinan besar bahwa suatu saat nanti Anda akan merancang atau memperbarui sistem jaringan, atau membantu satu atau lebih orang yang merancang atau memperbarui jaringan. sistem. Jika Anda akan melakukan tugas ini sendiri, Anda perlu mengetahui cara mengatasi masalah secara logis dan menyiapkan langkah-langkah yang tepat. Jika Anda akan bekerja dengan satu atau lebih profesional jaringan, Anda harus mengetahui langkah-langkah yang terlibat dan bagaimana Anda dapat berpartisipasi di dalamnya.

Selain memahami konsep dasar desain jaringan, seorang manajer jaringan perlu mempelajari keterampilan kompleks lainnya, seperti bagaimana melakukan studi kelayakan, melakukan perencanaan kapasitas, melakukan analisis lalu lintas, dan membuat garis dasar. Bab ini akan memperkenalkan masing-masing aktivitas tersebut dan menyajikan contoh-contoh yang relatif sederhana yang menunjukkan kegunaannya. Bab ini akan diakhiri dengan penjelasan tentang keterampilan pribadi yang dibutuhkan seorang administrator jaringan dan melihat beberapa alat yang tersedia untuk mendukung jaringan dengan baik.

13.2 SIKLUS HIDUP PERKEMBANGAN SISTEM

Setiap perusahaan, baik organisasi nirlaba maupun nirlaba, biasanya memiliki sejumlah tujuan utama, beberapa di antaranya mungkin meliputi:

- Meningkatkan basis pelanggan perusahaan
- Menjaga kepuasan pelanggan dengan memberikan layanan perusahaan seefektif mungkin
- Meningkatkan tingkat keuntungan perusahaan, atau, dalam organisasi nirlaba, memperoleh dana yang diperlukan untuk memenuhi tujuan dan sasaran organisasi
- Menjalankan bisnis dengan lebih efisien dan efektif

Dari tujuan utama ini, perencana sistem dan personel manajemen dalam suatu perusahaan mencoba menghasilkan serangkaian pertanyaan yang, jika dijawab dengan memuaskan, akan membantu organisasi mereka mencapai tujuan dan memajukan organisasi. Misalnya, seseorang di manajemen mungkin bertanya: Apakah ada cara untuk menyederhanakan sistem pemesanan agar perusahaan dapat menjalankan bisnis dengan lebih efisien dan efektif? Bisakah kita mengotomatiskan sistem perpanjangan pelanggan untuk melayani pelanggan dengan lebih baik dan membuat mereka senang? Adakah cara yang lebih efisien untuk menawarkan produk baru guna membantu perusahaan meningkatkan basis pelanggan? Adakah cara yang lebih baik dalam mengelola sistem gudang kita untuk meningkatkan keuntungan perusahaan?

Seringkali dalam dunia bisnis saat ini, jawaban terhadap pertanyaan-pertanyaan semacam ini melibatkan solusi yang memerlukan penggunaan sistem komputer, dan sistem komputer yang digunakan seringkali berukuran besar dan kompleks. Ketika sejumlah besar

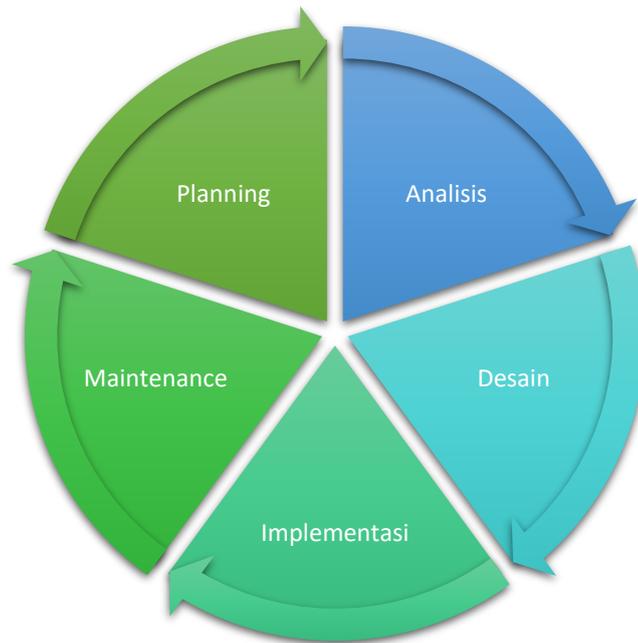
waktu, uang, dan sumber daya terlibat dalam solusi komputer tertentu, Anda ingin memastikan bahwa solusi ini adalah yang terbaik untuk masalah tersebut.

Untuk dapat memahami suatu masalah dengan benar, menganalisis semua solusi yang mungkin, memilih solusi terbaik, dan menerapkan serta memelihara solusi tersebut, Anda perlu mengikuti rencana yang jelas. Salah satu rencana paling populer dan sukses yang digunakan oleh bisnis saat ini adalah Siklus Hidup Pengembangan Sistem. Siklus Hidup Pengembangan Sistem (SDLC) adalah pendekatan terstruktur untuk pengembangan sistem bisnis. Meskipun teknik yang lebih baru seperti RAD (Rapid Application Development) dan Agile lebih cocok untuk proses pengembangan yang lebih berulang, demi kesederhanaan kami akan tetap menggunakan SDLC untuk saat ini. Pendekatan ini sering kali mencakup perencanaan, analisis, desain, implementasi, dan dukungan. Secara umum, pendekatan terstruktur adalah serangkaian langkah dan tugas yang dapat diikuti oleh para profesional, seperti pengembang sistem, untuk membangun sistem berkualitas tinggi dengan lebih cepat, dengan risiko lebih sedikit, dan dengan biaya lebih rendah. Meskipun hampir setiap perusahaan yang menggunakan SDLC dan setiap buku teks yang mengajarkan SDLC memiliki variasi metodologi yang sedikit berbeda, sebagian besar setuju bahwa SDLC setidaknya mencakup fase-fase berikut:

- Perencanaan—Identifikasi masalah, peluang, dan tujuan.
- Analisis—Menentukan kebutuhan informasi, menganalisis kebutuhan sistem, dan menyiapkan proposal sistem tertulis.
- Desain—Merancang dan membangun sistem yang direkomendasikan pada akhir tahap analisis dan membuat dokumentasi untuk melengkapi sistem.
- Implementasi—Menginstal sistem dan bersiap untuk berpindah dari sistem lama ke sistem baru; melatih penggunaannya.
- Pemeliharaan—Perbaiki dan perbarui sistem yang diinstal jika diperlukan.

Ide fase sangat penting untuk konsep SDLC. Tujuan dari SDLC adalah agar tahapan-tahapan tersebut tidak menjadi langkah-langkah yang terputus-putus dalam suatu rencana besar, namun merupakan lapisan-lapisan aktivitas yang tumpang tindih. Merupakan hal yang umum jika dua atau tiga fase dari satu proyek berlangsung pada waktu yang bersamaan. Misalnya, desain satu komponen sistem sedang berlangsung, sementara implementasi komponen lainnya sedang dilakukan.

Konsep penting kedua adalah siklus. Setelah suatu sistem dipelihara selama jangka waktu tertentu, biasanya fase perencanaan akan dimulai kembali—yaitu siklus berikutnya—dalam upaya mencari solusi yang lebih baik terhadap masalah tersebut. Dengan demikian, Siklus Hidup Pengembangan Sistem merupakan proses yang tidak pernah berakhir (lihat Gambar 13-1).



Gambar 13-1 Sifat siklus dari fase Siklus Hidup Pengembangan Sistem

Siapa yang bertanggung jawab untuk memulai tahapan dan mengarahkan proyek melalui siklus tersebut? Seorang profesional yang disebut analis sistem biasanya bertanggung jawab untuk mengelola proyek dan mengikuti fase SDLC, khususnya fase analisis dan desain. Meskipun menjadi seorang analis sistem memerlukan pelatihan profesional khusus, banyak individu yang bekerja dengan jaringan komputer dapat mempelajari analisis sistem dan metode perancangan dan menggabungkannya ke dalam perancangan jaringan komputer. Mungkin juga seseorang yang mendukung jaringan komputer dipanggil oleh analis sistem untuk memberikan masukan ke dalam solusi jaringan baru. Dalam hal ini, profesional jaringan harus mengetahui SDLC dan siap memberikan informasi atau materi desain apa pun yang diminta.

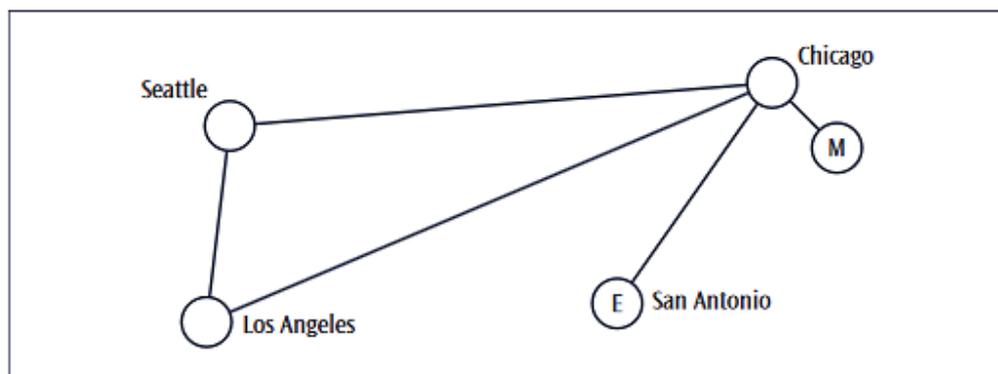
13.3 PEMODELAN JARINGAN

Ketika seorang analis sistem atau seseorang yang bertindak sebagai analis sistem diminta untuk merancang sistem komputer baru, dia biasanya akan membuat serangkaian model untuk sistem yang ada (jika ada) dan sistem yang diusulkan. Model ini biasanya dirancang untuk menunjukkan aliran data melalui sistem dan aliran prosedur dalam sistem, dan dengan demikian membantu analis dan profesional lainnya memvisualisasikan sistem saat ini dan yang diusulkan. Salah satu bagian yang sangat penting dari sebagian besar sistem komputer saat ini adalah jaringan. Sebagian besar bisnis memiliki setidaknya satu jaringan area lokal internal, dan satu atau lebih koneksi ke jaringan area luas eksternal seperti Internet. Banyak bisnis memiliki beberapa lokasi kantor yang tersebar di wilayah geografis. Model yang dibuat untuk desain jaringan dapat menggambarkan keadaan jaringan saat ini atau menggambarkan jaringan komputer yang diinginkan.

Model jaringan tidak harus berupa kreasi yang rumit. Seringkali, hanya model yang digambar tangan yang menggambarkan desain jaringan yang diusulkan. Salah satu teknik yang digunakan untuk memodelkan lingkungan jaringan perusahaan adalah dengan membuat peta konektivitas. Lebih tepatnya, tiga teknik pemodelan berbeda dapat digunakan, bergantung pada jenis jaringan yang Anda modelkan: peta konektivitas wilayah luas, peta konektivitas wilayah metropolitan, dan peta konektivitas wilayah lokal. Tidak semua proyek analisis dan desain memerlukan ketiga peta konektivitas jaringan. Misalnya, perusahaan Anda mungkin tidak menggunakan jaringan area metropolitan untuk menghubungkan jaringan area lokalnya ke dunia luar, sehingga tidak perlu membuat peta konektivitas area metropolitan. Meskipun demikian, ketiga peta tersebut akan dijelaskan di sini, karena masing-masing jenis memiliki karakteristik yang sedikit berbeda namun penting. Mari kita mulai dengan gambaran besar peta konektivitas wilayah luas dan berlanjut ke detail lebih kecil yang ditunjukkan pada peta konektivitas wilayah lokal.

Peta konektivitas area luas

Untuk membuat peta konektivitas wilayah yang luas, pemodeler memulai dengan mengidentifikasi setiap situs atau lokasi di mana perusahaan berkantor. Setiap lokasi tetap ditandai dengan lingkaran; situs seluler atau nirkabel ditandai dengan lingkaran yang mengandung huruf M; dan situs eksternal, seperti pemasok atau agen eksternal, dilambangkan dengan lingkaran yang mengandung huruf E. Garis padat antara dua situs menunjukkan jalur yang diinginkan untuk transmisi data (atau suara). Gambar 13-2 menunjukkan empat lokasi—Chicago, Seattle, Los Angeles, dan San Antonio—dalam peta tersebut. Pengguna di San Antonio sebenarnya adalah kantor pemerintah dan dengan demikian ditampilkan sebagai situs dengan huruf E. Selain itu, terdapat pengguna nirkabel di kantor Chicago, dan semuanya ditampilkan bersama dengan satu huruf M yang dilingkari.



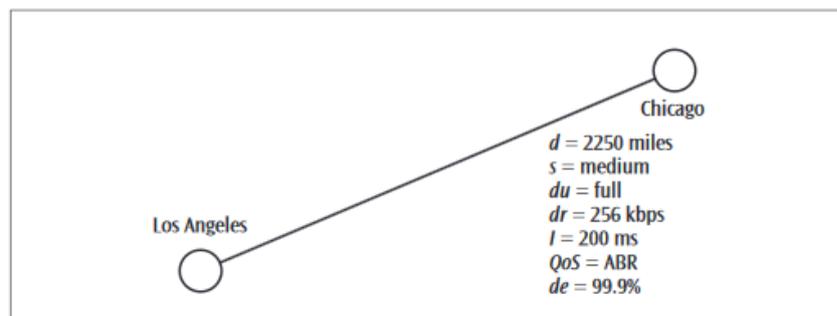
Gambar 13-2 Contoh peta konektivitas wilayah luas untuk lokasi di Chicago, Seattle, Los Angeles, dan San Antonio

Untuk mengidentifikasi hubungan antar situs, karakteristik tautan berikut dapat diterapkan pada setiap koneksi (dalam urutan apa pun):

- d = Jarak sambungan (biasanya ditunjukkan dalam mil atau kilometer)
- s = Tingkat keamanan (tinggi, sedang, rendah, atau tidak sama sekali)

- du = Dupleksitas (dupleks penuh, setengah dupleks, atau simpleks)
- dr = Kecepatan data yang diinginkan (dalam bps)
- l = Latensi, atau waktu tunda yang dapat diterima di seluruh jaringan (biasanya dalam milidetik, atau ms)
- Kualitas layanan QoS (CBR = bit rate konstan, VBR = bit rate variabel, ABR = bit rate tersedia, UBR = bit rate tidak dapat diandalkan, atau tidak ada sama sekali)
- de = Kecepatan pengiriman (terkadang disebut persentase throughput)

Gambar 13-3 menunjukkan bagaimana karakteristik hubungan ini dapat digunakan untuk mendefinisikan hubungan secara lebih lengkap—dalam hal ini, hubungan antara Chicago dan Los Angeles. Jarak kedua kota ini adalah 2.250 mil; tingkat keamanan koneksi sedang; dupleksitasnya penuh; kecepatan data yang diinginkan adalah 256 kbps; latensi di seluruh jaringan adalah 200 ms; kualitas layanan adalah ABR; dan tingkat pengirimannya 99,9 persen.



Gambar 13-3 Karakteristik hubungan rinci untuk hubungan antara Chicago dan Los Angeles

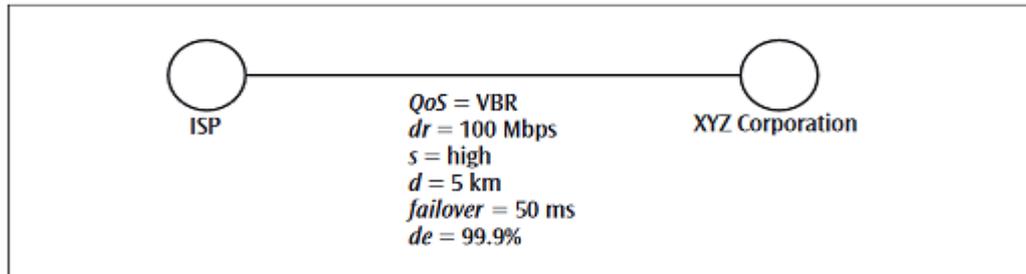
Setelah mengidentifikasi lokasi, pemodel kemudian akan menentukan karakteristik setiap link, membuat peta yang menunjukkan interkoneksi jaringan area luas untuk keseluruhan bisnis. Kini setelah jaringan area luas telah dipetakan, pemodel dapat memperbesar koneksi jaringan area metropolitan.

Peta konektivitas wilayah metropolitan

Jika sebuah perusahaan menginginkan koneksi jaringan area metropolitan antara salah satu kantornya dan bisnis lain, seperti penyedia layanan Internet (ISP), perusahaan dapat menggunakan peta konektivitas area metropolitan untuk menguraikan koneksi ini dan menentukan karakteristik jaringan yang diinginkan. Peta konektivitas wilayah metropolitan berbagi beberapa karakteristik peta wilayah luas dan beberapa karakteristik peta wilayah lokal. Kecepatan data, kualitas layanan, dan keamanan masih menjadi parameter penting di lapisan metropolitan, namun jarak mungkin tidak sepenting pada peta wilayah luas. Parameter baru yang mungkin berdampak pada desain wilayah metropolitan adalah waktu failover. Ingat dari Bab Sembilan bahwa waktu failover adalah jumlah waktu yang diperlukan jaringan area metropolitan untuk mengkonfigurasi ulang dirinya sendiri atau merutekan ulang paket jika link tertentu gagal. Contoh peta konektivitas wilayah metropolitan ditunjukkan pada Gambar 13-4.

Peta konektivitas wilayah metropolitan dapat berdiri sendiri dari peta konektivitas wilayah luas atau dapat digabungkan ke dalam peta wilayah luas. Pemodel akan melakukan

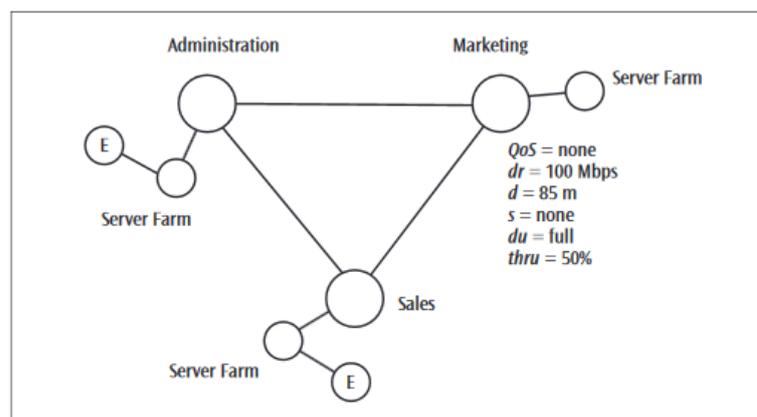
hal terakhir dengan memasukkan link wilayah metropolitan dan karakteristik pada lokasi konektivitas wilayah luas yang sesuai. Setelah peta konektivitas wilayah metropolitan selesai (atau jika tidak perlu membuat peta wilayah metropolitan karena tidak ada jaringan metropolitan), pemodel kemudian melanjutkan ke rangkaian peta terakhir: peta konektivitas wilayah lokal.



Gambar 13-4 Dua node dan link penghubung dalam peta konektivitas wilayah metropolitan

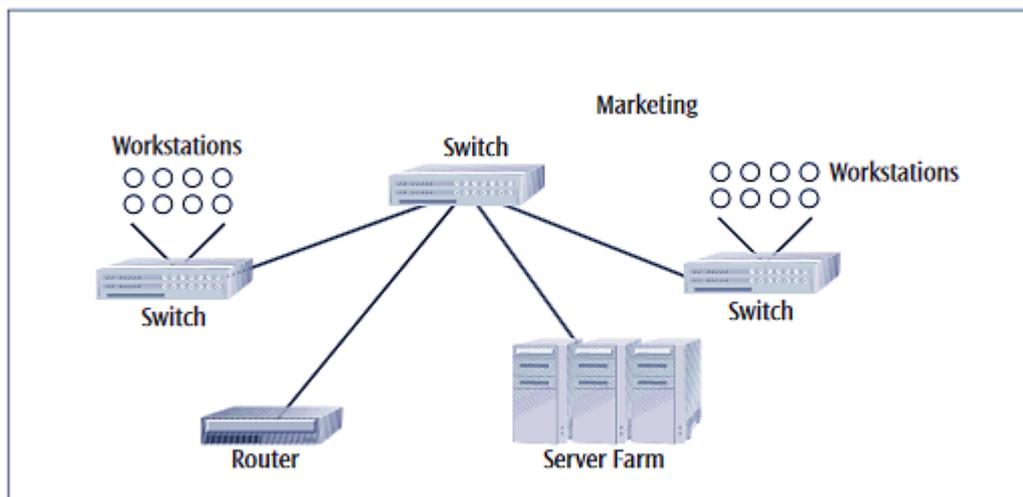
Peta konektivitas area lokal

Untuk memeriksa node dalam peta konektivitas area luas secara lebih rinci, seorang analis dapat memperluas setiap situs ke dalam peta konektivitas area lokal. Desain jaringan area lokal kemudian dapat dilakukan dalam satu atau dua tahap, tergantung pada tingkat detail yang diinginkan. Jika hanya gambaran umum jaringan lokal yang diinginkan, maka analis dapat membuat peta konektivitas gambaran umum area lokal. Pada tahap ini, seluruh kelompok logis atau fisik, seperti kelompok pengguna dan stasiun kerja, dilambangkan sebagai satu node. Hubungan antara node tersebut ditentukan oleh faktor-faktor seperti jarak, keamanan, kecepatan data, QoS, duplexity, dan throughput (atau melalui), yang merupakan persentase data aktual yang dikirimkan dalam jangka waktu tertentu. Latensi, tingkat pengiriman, dan failover biasanya bukan merupakan faktor yang cukup signifikan untuk dimasukkan pada tingkat area lokal. Gambar 13-5 menunjukkan contoh peta konektivitas ikhtisar area lokal. Perhatikan bahwa peta ikhtisar tidak menyertakan titik koneksi apa pun, seperti hub, sakelar, atau router.



Gambar 13-5 Contoh peta konektivitas ikhtisar area lokal

Jika diinginkan lebih detail, analis dapat membuat peta konektivitas area lokal secara rinci. Peta terperinci dapat menunjukkan bagaimana masing-masing stasiun kerja atau kelompok stasiun kerja dikelompokkan dengan switch, router, hub, dan kumpulan server. Misalnya, peta konektivitas rinci area lokal pada Gambar 13-6 telah memperbesar node Pemasaran dari peta ikhtisar pada Gambar 13-5 untuk menunjukkan stasiun kerja node ini dan interkoneksinya dengan switch node. Tingkat kerincian yang ditampilkan dalam peta konektivitas rinci wilayah setempat bergantung pada kebutuhan proyek tertentu. Beberapa proyek memerlukan semua interkoneksi antar komponen untuk ditampilkan, sementara proyek lain dapat bekerja dari peta yang hanya menunjukkan interkoneksi utama. Seperti yang dapat Anda bayangkan, peta konektivitas rinci area lokal umumnya menangkap cukup banyak informasi.



Gambar 13-6 Peta konektivitas rinci area lokal untuk Pemasaran

Sekarang kita telah mempelajari pemodelan jaringan, mari kita periksa alat lain yang digunakan dalam model SDLC: studi kelayakan.

13.4 STUDI KELAYAKAN

Menganalisis dan merancang sistem komputer baru dapat memakan waktu dan mahal. Ketika proyek sedang dalam tahap analisis, dan sebelum sistem dirancang dan dipasang, solusi yang layak harus ditemukan. Istilah “layak” mempunyai beberapa arti bila diterapkan pada proyek berbasis komputer. Sistem yang diusulkan harus layak secara teknis. Kelayakan teknis suatu sistem adalah sejauh mana sistem tersebut dapat dibuat dan diimplementasikan dengan menggunakan teknologi yang ada saat ini.

Apakah teknologi yang ditentukan dalam proposal sistem ada, dan dapatkah teknologi tersebut dimasukkan ke dalam solusi yang berfungsi? Jika teknologi dari dua vendor atau lebih disarankan, apakah teknologi yang berbeda akan bekerja sama? Ketika vendor mengklaim bahwa sistem perangkat keras atau perangkat lunak tertentu akan melakukan apa yang diinginkan, apakah klaim vendor tersebut akurat atau menyesatkan? Apakah perusahaan

Anda memiliki keahlian teknis untuk membangun, memasang, atau memelihara sistem yang diusulkan?

Sistem yang diusulkan juga harus layak secara finansial. Kelayakan finansial suatu sistem adalah sejauh mana sistem dapat dibuat, dengan mempertimbangkan kondisi keuangan perusahaan saat ini. Apakah sistem yang diusulkan dapat menyelesaikan masalah perusahaan saat ini dan tetap sesuai anggaran? Akankah sistem yang diusulkan menghasilkan keuntungan? Jika ya, berapa lama hal ini akan terjadi?

Selain itu, sistem yang diusulkan harus layak secara operasional. Ketika suatu sistem menunjukkan kelayakan operasional, maka sistem tersebut beroperasi sebagaimana dirancang dan diimplementasikan. Oleh karena itu, perusahaan harus bertanya: Apakah sistem yang diusulkan akan memberikan hasil yang diharapkan? Akankah pengguna dapat menggunakan sistem yang diusulkan, atau adakah kemungkinan bahwa sistem tersebut akan sangat sulit atau tidak nyaman untuk digunakan sehingga pengguna tidak akan mengadopsinya?

Yang terakhir, sistem yang diusulkan harus layak untuk dilaksanakan. Kelayakan waktu suatu sistem adalah sejauh mana sistem dapat dipasang secara tepat waktu dan memenuhi kebutuhan organisasi. Dapatkah sistem yang diusulkan dirancang, dibangun, diuji, dan dipasang dalam jangka waktu yang dianggap masuk akal dan disetujui oleh semua pihak?

Semua pertanyaan kelayakan ini sulit untuk dijawab, namun harus dijawab. Kelayakan teknis, operasional, keuangan, dan waktu paling baik ditentukan ketika studi didasarkan pada pengetahuan yang baik tentang sistem komputer, pemahaman tentang keadaan pasar saat ini dan produk-produknya, serta pengalaman. Individu yang mulai merancang dan menginstal jaringan komputer baru akan bekerja lebih baik jika mereka juga memahami teknik analisis dan desain, teknik manajemen proyek dan waktu, serta teknik analisis keuangan. Teknik-teknik ini merupakan bagian integral dari studi kelayakan.

Sebagai contoh bagaimana teknik ini digunakan, mari kita pertimbangkan teknik analisis keuangan umum yang melibatkan penentuan biaya dan manfaat sistem yang diusulkan: analisis pengembalian. Analisis pengembalian memetakan biaya awal dan biaya berulang tahunan dari sistem yang diusulkan terhadap proyeksi pendapatan (manfaat) tahunan yang diperoleh dari sistem yang diusulkan. Analisis sistem dan manajemen menengah dan atas menggunakan analisis pengembalian, bersama dengan teknik keuangan lainnya, untuk menentukan kelayakan finansial suatu proyek.

Sebelum Anda melihat cara melakukan penghitungan analisis pengembalian, Anda perlu meninjau beberapa konsep keuangan umum yang diterapkan pada sistem komputer. Untuk menentukan biaya suatu sistem, perlu mencakup semua biaya yang mungkin terjadi. Untuk melakukan ini, pertama-tama Anda harus mempertimbangkan semua biaya satu kali seperti:

- Biaya personel terkait dengan individu yang secara khusus direkrut untuk bekerja mengembangkan sistem; ini mungkin termasuk gaji analis, desainer, pemrogram, konsultan, spesialis, operator, sekretaris, dan sebagainya

- Biaya penggunaan komputer, yang mencerminkan kebutuhan komputasi untuk melakukan analisis dan studi kelayakan
- Biaya perangkat keras dan perangkat lunak untuk sistem yang diusulkan
- Biaya untuk melatih pengguna, personel pendukung, dan manajemen untuk menggunakan sistem yang diusulkan
- Persediaan, duplikasi, dan biaya furnitur untuk personel yang membuat sistem yang diusulkan

Namun untuk mendapatkan pemahaman komprehensif tentang biaya sistem, Anda juga harus menghitung biaya berulang dari sistem yang diusulkan. Ini termasuk:

- Pembayaran sewa perangkat keras komputer atau peralatan lainnya
- Biaya lisensi berulang untuk perangkat lunak yang dibeli
- Gaji dan upah personel yang akan mendukung sistem
- Persediaan berkelanjutan yang akan menjaga sistem yang diusulkan tetap berfungsi
- Biaya pemanasan, pendinginan, dan listrik untuk mendukung sistem yang diusulkan
- Biaya penggantian yang direncanakan untuk mengganti bagian-bagian sistem yang rusak atau usang

Setelah biaya satu kali dan biaya berulang telah ditetapkan, sekarang saatnya menentukan manfaat yang akan dihasilkan dari sistem yang diusulkan. Saat menghitung manfaat, Anda perlu memasukkan manfaat berwujud dan manfaat tidak berwujud. Sehubungan dengan manfaat nyata, pengukuran yang paling umum adalah penghematan bulanan atau tahunan yang dihasilkan dari penggunaan sistem yang diusulkan. Manfaat tak berwujud adalah manfaat yang sulit ditentukan jumlahnya; hal ini mencakup niat baik pelanggan dan semangat kerja karyawan.

Tabel 13-1 Nilai sekarang satu dolar dari waktu ke waktu, dengan tingkat diskonto 4, 6, 8, dan 10 persen

Nilai Sekarang dari Seribu Rupiah untuk Tingkat Diskonto yang Berbeda				
Tahun	4%	6%	8%	10%
1	0.961	0.943	0.926	0.909
2	0.924	0.889	0.857	0.826
3	0.888	0.839	0.794	0.751
4	0.854	0.792	0.735	0.683
5	0.821	0.747	0.681	0.621
6	0.790	0.704	0.630	0.564
7	0.759	0.665	0.583	0.513

Sekarang setelah biaya dan manfaat telah ditentukan, Anda dapat menerapkannya pada analisis pengembalian. Saat melakukan penghitungan analisis pengembalian, Anda harus menunjukkan semua jumlah dolar menggunakan nilai waktu uang. Nilai waktu uang adalah sebuah konsep yang menyatakan bahwa satu dolar saat ini bernilai lebih dari satu dolar yang dijanjikan satu tahun dari sekarang karena dolar saat ini dapat diinvestasikan sekarang dan karenanya mengakumulasi bunga. Ini juga berarti bahwa jika sesuatu akan berharga satu dolar

dalam satu tahun dari sekarang, Anda perlu menyisihkan kurang dari satu dolar hari ini untuk membayarnya. Apalagi bergantung pada asumsi yang Anda buat tentang tingkat diskonto. Tingkat diskonto adalah biaya peluang untuk dapat menginvestasikan uang pada proyek lain, seperti saham dan obligasi. Nilai tingkat diskonto sering kali ditentukan oleh kepala keuangan perusahaan. Dengan asumsi tingkat diskonto, misalnya, 8 persen, berarti Anda hanya perlu menyisihkan 92,6 sen hari ini untuk membayar sesuatu yang akan bernilai satu dolar dalam satu tahun. Jadi, dalam kasus ini, nilai 92,6 sen adalah nilai sekarang satu dolar satu tahun dari sekarang. Tabel 13-1 menunjukkan nilai sekarang satu dolar selama periode tujuh tahun, dengan empat tingkat diskonto yang berbeda.

Gambar 13-7 menunjukkan contoh analisis pengembalian. Saat memeriksa gambar tersebut, perhatikan bahwa Biaya Pengembangan adalah biaya satu kali yang terjadi pada Tahun 0, dan biaya berulang tersebut dicantumkan sebagai Biaya Operasi dan Pemeliharaan pada Tahun 1–6. (Nilai negatif ditunjukkan dengan tanda kurung.) Secara keseluruhan, Biaya Pengembangan dan Biaya Operasi dan Pemeliharaan menjumlahkan biaya proyek selama umur proyek yang diharapkan. Dengan asumsi tingkat diskonto sebesar 6 persen, baris Time-Adjusted Costs mencerminkan total biaya setiap tahun dikalikan dengan nilai sekarang satu dolar pada tahun tersebut. Biaya Kumulatif yang Disesuaikan dengan Waktu hanyalah jumlah berjalan dari Biaya yang Disesuaikan dengan Waktu selama bertahun-tahun. Manfaat Nilai turunan adalah manfaat, atau jumlah pendapatan, yang diharapkan setiap tahunnya. Masih dengan asumsi tingkat diskonto 6 persen, Time-Adjusted Benefits adalah Manfaat yang Diperoleh dikalikan dengan nilai sekarang satu dolar setiap tahunnya. Nilai Kumulatif Manfaat yang Disesuaikan dengan Waktu adalah jumlah berjalan dari Manfaat yang Disesuaikan dengan Waktu selama bertahun-tahun. Biaya Kumulatif Seumur Hidup yang Disesuaikan adalah Biaya Kumulatif yang Disesuaikan dengan Waktu ditambah Manfaat Kumulatif yang Disesuaikan dengan Waktu untuk setiap tahun.

Payback Analysis for New Network Installation							
Description	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
Development Cost	(\$620,000)						
Operation and Maintenance Costs		(\$17,400)	(\$16,500)	(\$17,700)	(\$17,900)	(\$18,300)	(\$18,350)
Discount Factor: 6%	1.00	0.943	0.889	0.839	0.792	0.747	0.704
Time-Adjusted Costs	(\$620,000.00)	(\$16,408.20)	(\$14,668.50)	(\$14,850.30)	(\$14,176.80)	(\$13,670.10)	(\$12,918.40)
Cumulative Time-Adjusted Costs	(\$620,000.00)	(\$636,408.20)	(\$651,076.70)	(\$665,970.00)	(\$680,103.80)	(\$693,773.90)	(\$706,692.30)
Benefits Derived	\$0.00	\$172,000.00	\$184,000.00	\$194,000.00	\$199,000.00	\$204,000.00	\$208,000.00
Discount Factor: 6%	1.00	0.943	0.889	0.839	0.792	0.747	0.704
Time-Adjusted Benefits	\$0.00	\$162,196.00	\$163,576.00	\$162,766.00	\$157,608.00	\$152,388.00	\$146,432.00
Cumulative Time-Adjusted Benefits	\$0.00	\$162,196.00	\$325,772.00	\$448,538.00	\$646,146.00	\$798,534.00	\$944,966.00
Cumulative Lifetime Time-Adjusted Costs	(\$620,000.00)	(\$474,212.20)	(\$325,304.70)	(\$177,389.00)	(\$33,957.80)	(\$104,760.10)	\$238,273.70

The graph illustrates the cumulative lifetime costs over a 7-year period. The y-axis represents 'Cumulative Lifetime Costs' ranging from \$800,000.00 (negative) to \$400,000.00 (positive). The x-axis represents 'Years' from 1 to 7. The line starts at a negative value of approximately \$620,000.00 at year 0 and trends upwards, crossing the zero line between year 5 and year 6, indicating the payback period.

Gambar 13-7 Perhitungan analisis pengembalian untuk proyek yang diusulkan

Seperti yang dapat Anda lihat pada Gambar 13-7, nilai pada baris Biaya yang Disesuaikan Waktu Seumur Hidup Kumulatif menjadi positif pada tahun keenam proyek—yang berarti proyek akhirnya menghasilkan keuntungan pada saat ini. Jadi, dalam kasus ini, diperlukan waktu sekitar lima setengah tahun agar pengembalian modal, atau laba atas investasi (ROI), dapat terwujud. Sebagian besar perusahaan menetapkan periode ROI yang dapat diterima. Jika analisis pengembalian sebelumnya telah dilakukan untuk perusahaan yang periode ROI-nya enam hingga tujuh tahun, hasilnya akan menunjukkan kepada perusahaan bahwa proyek yang diusulkan ini mungkin layak secara finansial.

Sekarang mari kita mengalihkan perhatian kita ke teknik tambahan yang harus digunakan ketika mengembangkan solusi sistem.

13.5 PERENCANAAN KAPASITAS

Jaringan komputer adalah sistem yang sangat penting, dan merancang jaringan komputer baru atau meningkatkan kapasitas sistem saat ini memerlukan perencanaan yang cermat. Jika Anda merancang sistem untuk sebuah perusahaan, dan sistem tersebut tidak mampu mendukung lalu lintas yang dihasilkan dalam perusahaan, waktu respons akan lambat, dan pengguna mungkin tidak dapat menyelesaikan pekerjaannya tepat waktu. Ketidakmampuan melaksanakan tugas pekerjaan ini akan menyebabkan tenggat waktu terlewat, proyek terhambat atau bahkan gagal, dan rendahnya semangat kerja karyawan. Jika perusahaan ini menjual produk yang dapat dibeli secara elektronik, waktu respons yang lambat juga akan menyebabkan pelanggan tidak puas. Di era Internet, ketika situs Web pesaing hanya berjarak satu klik saja, pelanggan yang tidak puas akan segera beralih ke situs lain.

Di sisi lain, jika Anda mendesain sistem secara berlebihan, Anda akan mengeluarkan uang yang tidak perlu untuk menciptakan sistem yang mungkin tidak akan pernah mencapai kapasitasnya. Dapat dikatakan bahwa jika Anda akan melakukan kesalahan dalam desain, mungkin yang terbaik adalah melakukan desain yang berlebihan, terutama karena sulit untuk memprediksi tingkat pertumbuhan pengguna dan aplikasi baru. Namun kenyataannya sebagian besar sistem yang dirancang selama 10 tahun terakhir mungkin terlalu kecil dan tidak akan mampu—atau sudah tidak bisa—mendukung kebutuhan yang ada. Persentase yang lebih kecil dari sistem jaringan dirancang secara berlebihan dan relatif tidak digunakan.

Perencanaan kapasitas melibatkan upaya menentukan jumlah bandwidth jaringan yang diperlukan untuk mendukung suatu aplikasi atau sekumpulan aplikasi. Perencanaan kapasitas adalah operasi yang cukup sulit dan memakan waktu. Namun jika perencanaan kapasitas tidak dilakukan dengan baik, akan sangat mudah untuk membuat perencanaan yang buruk sehingga merancang suatu sistem yang tidak akan mendukung penerapan yang diharapkan. Ada sejumlah teknik untuk melakukan perencanaan kapasitas, termasuk proyeksi linier, simulasi komputer, benchmarking, dan pemodelan analitis.

ROI untuk LAN Nirkabel dan Keamanan Jaringan

Ketika sebuah perusahaan menghitung ROI (laba atas investasi) untuk proyek yang diusulkan, ia membandingkan pendapatan yang dihasilkan dari proyek tersebut dengan biaya yang dikeluarkan. Ketika pendapatan lebih besar dari pengeluaran, perusahaan telah memperoleh laba atas investasinya. Apa yang terjadi jika proyek tersebut tidak menghasilkan pendapatan—yakni jika proyek tersebut tidak dirancang untuk menghasilkan pendapatan? Lalu bagaimana Anda mengukur laba atas investasi perusahaan Anda? Selain itu, jika Anda tidak dapat menghitung ROI, bagaimana Anda “menjual” pentingnya proyek baru ini kepada manajemen?

Dua teknologi dalam jaringan komputer yang seringkali tidak menghasilkan pendapatan adalah LAN nirkabel dan keamanan jaringan. Atau mungkin kita harus mengatakan bahwa keduanya tidak menghasilkan pendapatan dalam perhitungan ROI konvensional. Untuk menentukan bagaimana perusahaannya bisa mendapatkan keuntungan dari investasi pada LAN nirkabel dan keamanan jaringan, seorang administrator jaringan harus

melihat lebih jauh dari teknik konvensional yang hanya memperhitungkan peningkatan keuntungan dan pengurangan biaya, dan sebagai gantinya mempertimbangkan faktor kualitatif.

Misalnya, jika sebuah perusahaan sedang mempertimbangkan untuk memasang jaringan area lokal nirkabel, biaya yang biasanya timbul adalah biaya yang terkait dengan:

- Perangkat keras (termasuk biaya titik akses dan NIC nirkabel)
- Perangkat Lunak
- Instalasi
- Pelatihan dan dokumentasi
- Pemeliharaan berkelanjutan

Bagaimana dengan manfaatnya? Keuntungan memasang LAN nirkabel meliputi:

- Tidak diperlukan kabel jaringan untuk perangkat nirkabel
- Biaya pemeliharaan lebih rendah karena jack jaringan tidak harus dipindahkan setiap kali karyawan memindahkan meja atau lokasi kerjanya
- Peningkatan produktivitas (dan semangat kerja) karyawan diperoleh dengan memberikan manfaat seperti kebebasan bekerja di lokasi mana pun serta kemampuan untuk, misalnya, mengakses catatan mereka secara langsung selama rapat atau segera mengambil spesifikasi produk dari pabrik

Perlu dicatat bahwa meskipun konsekuensi finansial dari manfaat ketiga—peningkatan produktivitas karyawan—kurang dapat diukur secara langsung dibandingkan dua manfaat pertama, namun dampaknya tidak kalah pentingnya.

Sekarang mari kita pertimbangkan keamanan. Berapa biaya umum untuk menambah atau meningkatkan keamanan jaringan? Biasanya, biaya-biaya ini berhubungan dengan:

- Perangkat keras (termasuk biaya router firewall dan perangkat lainnya)
- Perangkat Lunak
- Pemeliharaan dan dukungan berkelanjutan

Manfaat menambahkan keamanan adalah sebagai berikut:

- Mengurangi waktu henti sistem karena berkurangnya virus akan membantu meminimalkan kegagalan sistem dan perlambatan sistem
- Peningkatan produktivitas karyawan karena karyawan akan menghabiskan lebih sedikit waktu untuk pulih dari virus
- Mengurangi kebutuhan penyimpanan karena lebih sedikit virus yang menggunakan atau merusak ruang hard disk

Dengan semakin banyaknya artikel tentang tingginya biaya yang terkait dengan infeksi virus yang diterbitkan, semakin banyak administrator jaringan yang menyadari bahwa semakin mudah untuk mendokumentasikan waktu produktivitas yang hilang akibat virus.

Kesimpulannya, bukan tidak mungkin menghitung ROI untuk proyek jaringan nirkabel dan keamanan. Namun untuk melakukan hal ini, administrator jaringan harus melihat lebih jauh dari definisi normal pendapatan dan mempertimbangkan cara yang lebih kreatif untuk mendefinisikan manfaat. Seringkali, hal ini melibatkan penghitungan biaya yang terkait dengan berbagai skenario “bagaimana jika”—yang utama adalah: Bagaimana jika kita tidak

menerapkan perbaikan yang diusulkan? Apa dampaknya bagi kita dalam hal hilangnya produktivitas dan waktu henti?

Proyeksi linier melibatkan prediksi satu atau lebih kapasitas jaringan berdasarkan parameter jaringan saat ini dan mengalikan kapasitas tersebut dengan konstanta tertentu. Misalkan Anda saat ini memiliki jaringan, katakanlah, 10 node, dan jaringan tersebut memiliki waktu respons x . Dengan menggunakan proyeksi linier, Anda dapat menyimpulkan bahwa sistem dengan 20 node akan memiliki waktu respons $2x$. Namun, beberapa sistem tidak mengikuti proyeksi linier. Jika Anda menerapkan proyeksi linier pada sistem ini, Anda mungkin menghasilkan prediksi yang tidak akurat. Dalam kasus ini, diperlukan strategi alternatif.

Simulasi komputer melibatkan pemodelan sistem yang ada atau sistem yang diusulkan menggunakan alat simulasi berbasis komputer dan menerapkan model tersebut pada berbagai tingkat permintaan pengguna (disebut beban). Keuntungan menggunakan simulasi komputer adalah dapat meniru kondisi yang sangat sulit, bahkan tidak mungkin, untuk diciptakan pada jaringan nyata. Sisi negatifnya, simulasi komputer sulit dibuat, terutama karena kesalahan dalam proses pemodelan mudah dilakukan dan sulit ditemukan. Ditambah lagi, satu kesalahan saja dalam simulasi dapat memberikan hasil yang salah. Oleh karena itu, kehati-hatian harus diberikan saat membuat simulasi.

Benchmarking melibatkan pembuatan statistik sistem dalam lingkungan yang terkendali dan kemudian membandingkan statistik tersebut dengan pengukuran yang diketahui. Ada sejumlah tes benchmark jaringan yang dapat digunakan untuk mengevaluasi kinerja jaringan atau komponennya. Dibandingkan dengan simulasi, benchmarking adalah teknik yang relatif mudah dan dapat memberikan informasi berguna ketika digunakan untuk menganalisis jaringan. Namun menyiapkan tes benchmark bisa memakan waktu cukup lama. Sayangnya, seperti simulasi, proses ini juga dapat mengalami kemungkinan kesalahan. Selain itu, jika semua variabel dalam lingkungan pengujian tidak sama dengan semua variabel dalam lingkungan benchmark, maka akan terjadi perbandingan yang tidak akurat. Misalnya, jika lingkungan pengujian jaringan menggunakan satu merek router atau switch dan jaringan benchmark menggunakan merek yang berbeda, hasil perbandingan kedua jaringan mungkin tidak valid.

Pemodelan analitik melibatkan pembuatan persamaan matematika untuk menghitung berbagai nilai jaringan. Misalnya, untuk menghitung pemanfaatan (persentase waktu penggunaan saluran) dari satu saluran komunikasi dalam suatu jaringan, Anda dapat menggunakan persamaan:

$$U = t_{frame} / (2t_{prop} + t_{frame})$$

dimana t_{frame} adalah waktu untuk mengirimkan suatu frame data, dan t_{prop} adalah waktu propagasi, yaitu waktu yang dibutuhkan sinyal untuk ditransfer melalui kabel atau melalui gelombang udara.

Banyak ahli merasa pemodelan analitis adalah cara yang baik untuk menentukan kapasitas jaringan. Seperti dalam teknik simulasi komputer, Anda dapat membuat model analitik yang mewakili sistem jaringan yang sulit dibuat di dunia nyata. Sayangnya, sangat mudah untuk membuat model analisis yang tidak akurat sehingga menghasilkan hasil yang tidak valid.

Karena sebagian besar jaringan mendukung banyak aplikasi, seseorang yang melakukan perencanaan kapasitas untuk suatu jaringan harus menghitung kapasitas setiap aplikasi di jaringan. Setelah kapasitas setiap aplikasi ditentukan, kapasitas untuk seluruh jaringan dapat ditentukan. Anda dapat menghitung kapasitas individual menggunakan metode analitis dan kemudian memperkirakan total kapasitas jaringan menggunakan proyeksi linier. Mari kita perhatikan dua contoh sederhana perencanaan kapasitas untuk aplikasi tunggal pada jaringan komputer.

Contoh pertama didasarkan pada skenario yang ditampilkan di bagian Beraksi di Bab Sebelas. Ini adalah perhitungan matematis sederhana yang melibatkan pemilihan teknologi telekomunikasi yang tepat yang akan mendukung transfer catatan penjualan yang sangat besar. Setiap catatan penjualan berukuran 400.000 byte dan harus diunduh dalam waktu 20 detik atau kurang. Persamaan berikut menghitung kapasitas (atau kecepatan transfer data, n) yang diperlukan untuk satu pengguna mengunduh satu file:

$$400.000 \text{ byte} \times 8 \text{ bits/byte} = 3.200.000 \text{ bits}$$

$$n \text{ bps} = 3.200.000 \text{ bits}/20 \text{ second} = 160.000 \text{ bps}$$

Oleh karena itu, aplikasi ini memerlukan jalur telekomunikasi yang mampu mendukung kecepatan data minimal 160.000 bps.

Contoh lain dari perencanaan kapasitas—kali ini menggunakan proyeksi linier—misalkan Anda bekerja di perusahaan yang mengizinkan karyawannya mengakses Internet. Berbagai penelitian melaporkan bahwa rata-rata pengguna Internet di Amerika Serikat menggunakan sekitar 10 gigabyte bandwidth per bulan. Pekerja kantor mungkin menggunakan kurang dari ini, namun sebagai tindakan pencegahan, kami akan tetap menggunakan angka 10 gigabyte. Jika sistem Anda memiliki 100 pengguna potensial, konsumsi bandwidth bulanan Anda adalah 100 pengguna dikalikan 10 gigabyte, atau 10.000 gigabyte. Bisakah penyedia Internet Anda mendukung lalu lintas sebanyak ini? Dan jika mampu, apakah perusahaan Anda mampu membayar tagihan DSL? Dalam contoh ini, perencanaan kapasitas menunjukkan bahwa jika perusahaan Anda tidak bersedia menanggung biaya yang diperlukan, perusahaan mungkin harus menerapkan pembatasan terhadap cara karyawannya menggunakan Internet. Misalnya, perusahaan mungkin harus membatasi jumlah pengguna secara bersamaan atau membatasi jumlah atau jenis unduhan untuk setiap pengguna. Alternatifnya, perusahaan bisa berharap bahwa tidak lebih dari 40 persen penggunanya akan mengakses Internet pada saat yang sama.

Seperti yang Anda lihat, perencanaan kapasitas adalah hal yang sulit dan tidak sepele. Namun, setelah perencanaan kapasitas dilakukan dengan benar, administrator jaringan dapat

menentukan apakah jaringan area lokal dan koneksi jaringan area luas perusahaan dapat mendukung aplikasi yang dimaksudkan. Namun mengetahui kapasitas yang dibutuhkan bukanlah keseluruhan cerita. Masih ada pertanyaan penting lainnya yang harus diselesaikan. Misalnya: Bagaimana Anda mengetahui apakah jaringan saat ini dapat atau tidak dapat menangani aplikasi yang dimaksud? Setelah kapasitas yang dibutuhkan ditentukan, Anda perlu memeriksa jaringan saat ini dengan cermat untuk menentukan kapasitas sebenarnya. Salah satu teknik terbaik untuk menentukan kapasitas jaringan saat ini adalah dengan membuat garis dasar.

13.6 MENCIPTAKAN GARIS DASAR

Membuat garis dasar untuk jaringan komputer yang ada melibatkan pengukuran dan pencatatan status operasi jaringan selama periode waktu tertentu. Seperti yang akan Anda pelajari segera, membuat garis dasar sebenarnya melibatkan pengambilan banyak pengukuran jaringan pada seluruh segmen jaringan, termasuk berbagai pengukuran pada stasiun kerja, aplikasi pengguna, jembatan, router, dan switch. Karena pengumpulan informasi ini tampaknya merupakan tugas yang besar, mengapa Anda ingin membuat data dasar? Personil jaringan membuat garis dasar untuk menentukan kondisi operasi normal dan saat ini dari jaringan. Setelah garis dasar dibuat, hasilnya dapat digunakan untuk mengidentifikasi kelemahan dan kekuatan jaringan, yang kemudian dapat digunakan untuk meningkatkan jaringan secara cerdas.

Seringkali, administrator jaringan merasakan tekanan dari pengguna dan pemilik jaringan untuk meningkatkan bandwidth jaringan. Tanpa pemahaman menyeluruh apakah masalah jaringan benar-benar ada—atau, jika memang ada, di mana letak masalah tersebut—administrator jaringan yang mencoba meningkatkan operasi jaringan mungkin secara tidak sengaja “memperbaiki” masalah yang salah. Meningkatkan operasi jaringan mungkin melibatkan peningkatan bandwidth jaringan, namun bisa juga melibatkan sesuatu yang lebih murah, seperti memperbarui beberapa peralatan lama atau melakukan segmentasi jaringan dengan menggunakan switch. Dengan melakukan studi dasar (sebaiknya studi lanjutan), administrator jaringan dapat memperoleh pemahaman yang lebih baik tentang jaringan dan dapat meningkatkan kualitas keseluruhannya dengan lebih efektif.

Studi dasar dapat dimulai kapan saja, namun paling efektif bila dimulai pada saat jaringan tidak mengalami masalah yang parah, seperti kegagalan node atau jabber (kartu antarmuka jaringan yang mentransmisikan data tanpa henti). Oleh karena itu, sebelum memulai studi dasar, Anda harus segera memadamkan semua kebakaran dan mencoba membuat jaringan beroperasi normal. Karena Anda akan menghasilkan statistik dalam jumlah besar, Anda perlu memiliki akses ke aplikasi database atau spreadsheet yang baik agar data tetap teratur. Setelah database atau spreadsheet disiapkan, Anda siap memulai studi dasar.

Pertanyaan selanjutnya adalah: Pada item apa saja Anda akan mengumpulkan informasi dasar? Anda mungkin merasa berguna untuk mengumpulkan informasi tentang item seperti pengguna sistem, node sistem, protokol operasional, aplikasi jaringan, dan tingkat pemanfaatan jaringan. Mengumpulkan informasi tentang pengguna sistem melibatkan

penentuan jumlah maksimum pengguna, jumlah rata-rata pengguna, dan jumlah puncak pengguna.

Untuk mengumpulkan informasi dasar tentang node sistem, Anda membuat daftar jumlah dan jenis node sistem dalam jaringan. Ini mungkin termasuk stasiun kerja komputer, router, switch, hub, dan server. Merupakan praktik yang baik untuk memiliki gambar terkini tentang lokasi semua node, beserta nomor model, nomor seri, dan informasi alamat apa pun seperti alamat Ethernet dan IP. Informasi ini juga harus mencakup nama dan nomor telepon masing-masing vendor produk, jika bantuan teknis diperlukan.

Pengumpulan informasi dasar tentang protokol operasional melibatkan pembuatan daftar jenis protokol operasional yang digunakan di seluruh sistem. Sebagian besar jaringan mendukung banyak protokol, seperti TCP, IP, NetBIOS, dan lainnya. Semakin banyak protokol yang didukung, semakin banyak waktu pemrosesan yang diperlukan untuk mengkonversi dari satu protokol ke protokol lainnya. Jika studi dasar menemukan protokol lama yang dapat diganti, hal ini dapat berkontribusi pada peningkatan efisiensi jaringan.

Selama studi dasar, Anda juga harus membuat daftar semua aplikasi jaringan yang ditemukan di jaringan, termasuk jumlah, jenis, dan tingkat pemanfaatan setiap aplikasi. Memiliki daftar lengkap aplikasi di jaringan akan membantu Anda mengidentifikasi aplikasi lama yang tidak lagi didukung dan karenanya harus dihapus dari sistem. Daftar aplikasi juga akan membantu Anda mengidentifikasi jumlah salinan aplikasi tertentu dan dengan demikian membantu perusahaan menghindari pelanggaran lisensi perangkat lunaknya. Saat membuat daftar lengkap aplikasi jaringan, jangan lupa untuk menyertakan aplikasi yang disimpan di stasiun kerja pengguna individual dan server jaringan.

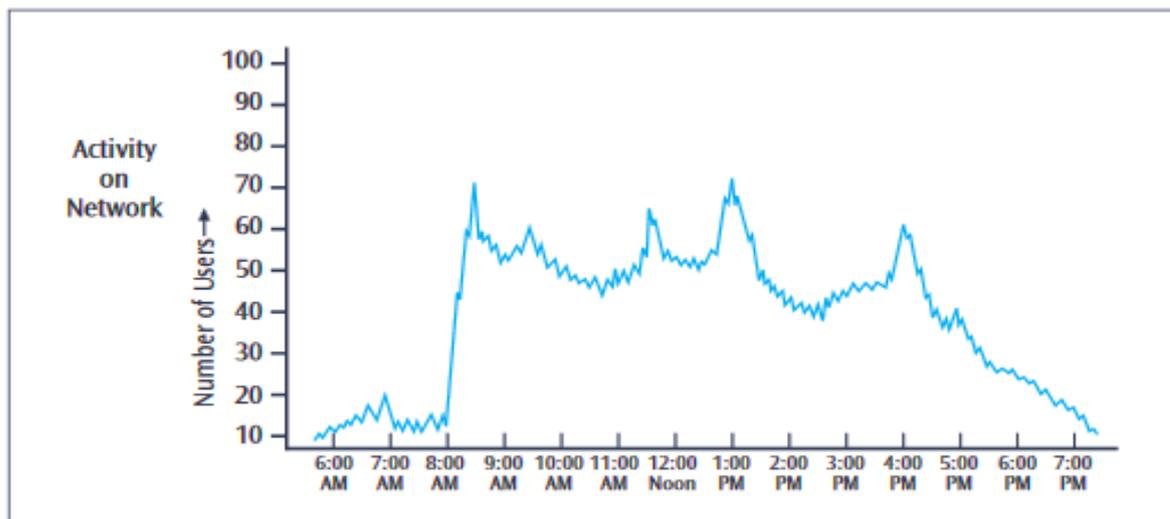
Mengumpulkan informasi tentang tingkat pemanfaatan jaringan mengharuskan Anda membuat daftar statistik yang cukup ekstensif. Statistik ini mencakup banyak nilai berikut:

- Rata-rata pemanfaatan jaringan (%)
- Pemanfaatan jaringan puncak (%)
- Ukuran bingkai rata-rata
- Ukuran bingkai puncak
- Rata-rata frame per detik
- Bingkai puncak per detik
- Total tabrakan jaringan
- Tabrakan jaringan per detik
- Total kerdil
- Jumlah ocehan
- Kesalahan total cyclic redundancy checksum (CRC).
- Node dengan persentase pemanfaatan tertinggi dan jumlah lalu lintas yang sesuai

Setelah Anda mengumpulkan dan menganalisis data pemanfaatan jaringan, Anda dapat melakukan beberapa pengamatan penting. Pertama, Anda dapat mendeteksi kapan jaringan mencapai saturasi. Biasanya, jaringan mencapai saturasi ketika pemanfaatan jaringannya mencapai 100 persen, yang berarti 100 persen ruang transmisi yang dapat digunakan pada jaringan digunakan oleh data yang valid. Namun dalam kasus tertentu, jaringan dapat

mencapai kejenuhan pada tingkat pemanfaatan jaringan yang lebih rendah. Ambil contoh CSMA/CD LAN segmen bersama. Karena jaringan CSMA/CD segmen bersama berbasiskan perselisihan, maka jaringan tersebut mengalami benturan. Ketika jumlah stasiun transmisi meningkat, jumlah tabrakan meningkat, sehingga menurunkan pemanfaatan jaringan. Dengan demikian, jaringan CSMA/CD yang secara konsisten mengalami pemanfaatan jaringan dalam kisaran 40 hingga 50 persen mungkin mengalami banyak tabrakan dan mungkin perlu disegmentasi dengan switch.

Pengamatan kedua yang dapat Anda lakukan adalah kapan periode puncak penggunaan jaringan terjadi. Melakukan pengamatan tentang periode puncak penggunaan jaringan paling mudah dilakukan saat Anda membuat grafik data aktivitas jaringan. Perhatikan contoh hipotetis yang ditunjukkan pada Gambar 13-8. Periode puncak terjadi sekitar pukul 08.30, 11.30, 13.00, dan 16.00. Alasan yang paling mungkin untuk puncak ini adalah pengguna masuk dan memeriksa email pada pukul 08.30 dan 13.00, serta pengguna menyelesaikan pekerjaan sebelum makan siang (11.30) atau pulang ke rumah (16.00). Setelah Anda mengidentifikasi periode puncak yang teratur dan penyebab utamanya, Anda dapat mengenali kapan periode puncak terjadi pada waktu yang tidak biasa. Selain itu, jika Anda mengetahui kapan periode puncak terjadi dan mengapa hal tersebut terjadi, Anda dapat mengatur ulang sumber daya jaringan untuk membantu mengurangi beban selama periode tersebut.



Gambar 13-8 Periode puncak aktivitas jaringan pada hari-hari biasa

Memeriksa jumlah lalu lintas pada setiap node juga menghasilkan informasi berharga tentang kinerja jaringan. Biasanya, persentase kecil dari node jaringan menghasilkan persentase lalu lintas jaringan yang besar. Bukan hal yang aneh untuk menemukan sebuah node, seperti router atau server, yang menjadi pusat dari banyak lalu lintas. Namun, stasiun kerja pengguna yang menghasilkan lalu lintas dalam jumlah besar patut dicurigai dan harus diperiksa lebih dekat. Contoh umum saat ini adalah pengguna mengunduh musik atau video melalui jaringan perusahaan atau sekolah. Pengunduhan musik dan video menghabiskan banyak bandwidth

dan menghabiskan sumber daya jaringan, sehingga menyebabkan penundaan bagi karyawan dan pelajar dengan permintaan jaringan yang sah. Administrator jaringan dapat dan harus mendeteksi pengunduhan ini, yang seringkali tidak sah, dan meminta pengguna untuk berhenti melakukannya di stasiun kerja jaringan.

Setelah Anda melakukan studi dasar, jangan berhenti mengamati jaringan. Agar studi dasar benar-benar efektif, Anda perlu mempertahankannya. Studi dasar yang sedang berlangsung memberikan manajer sistem alat yang efektif untuk mengidentifikasi masalah jaringan, memperbaiki jaringan, menanggapi keluhan, memperbaiki titik lemah, dan meminta pendanaan tambahan.

Sekarang kita telah mempelajari semua alat dan langkah-langkah yang diperlukan untuk mengembangkan jaringan, mari kita periksa jenis keterampilan yang dibutuhkan seorang administrator jaringan untuk menjaga sistem tetap beroperasi dengan sukses.

13.7 KETERAMPILAN ADMINISTRATOR JARINGAN

Setelah tahap analisis dan desain pengembangan jaringan selesai dan jaringan komputer sudah siap dan beroperasi, administrator jaringan bertanggung jawab untuk menjaganya tetap berjalan. (Beberapa perusahaan mulai menyebut posisi ini sebagai insinyur jaringan, meskipun insinyur jaringan cenderung melakukan lebih banyak perancangan jaringan sementara administrator jaringan mungkin melakukan lebih banyak pemeliharaan jaringan. Terlepas dari itu, istilah-istilah ini tidak baku.) Menjaga jaringan tetap berjalan melibatkan melakukan perbaikan pada komponen yang gagal, menginstal aplikasi baru dan memperbarui yang sudah ada, menjaga pengguna sistem tetap up-to-date, dan mencari cara baru untuk meningkatkan keseluruhan sistem dan tingkat layanan. Ini bukanlah pekerjaan mudah. Dengan kompleksitas jaringan saat ini dan ketergantungan bisnis pada aplikasi mereka, administrator jaringan sangatlah berharga, terlihat, dan selalu bergerak.

Karena banyak administrator jaringan yang berurusan dengan komputer dan manusia, mereka memerlukan keterampilan yang diperlukan untuk bekerja dengan keduanya. Daftar keterampilan untuk administrator jaringan akan mencakup keterampilan teknologi platform luas, termasuk, namun tidak terbatas pada, pengetahuan tentang jaringan area lokal, jaringan area luas, sistem telekomunikasi suara, sistem transmisi data, transmisi video, dasar-dasar komunikasi, konsep perangkat keras, dan keterampilan perangkat lunak dasar. Seorang administrator jaringan juga harus memiliki keterampilan interpersonal, termasuk kemampuan untuk berbicara dengan pengguna untuk mengatasi masalah dan mengeksplorasi aplikasi baru. Selain keterampilan interpersonal, administrator jaringan juga memerlukan keterampilan pelatihan, yang melibatkan kemampuan untuk melatih pengguna atau personel pendukung jaringan lainnya.

Untuk memanfaatkan sumber daya yang terbatas secara efektif, administrator jaringan juga harus memiliki sejumlah keterampilan manajemen umum. Pertama, administrator jaringan harus memiliki keterampilan manajemen anggaran, termasuk mengetahui cara menyiapkan anggaran untuk membenarkan pendanaan yang berkelanjutan atau untuk meminta dana tambahan. Selain keterampilan tersebut, administrator jaringan

memerlukan keterampilan statistik dasar, yang berarti bahwa ia harus mengetahui cara mengumpulkan dan menggunakan statistik sistem untuk membenarkan kinerja sistem yang ada atau untuk memvalidasi penambahan sistem baru. Keterampilan manajemen waktu juga diperlukan. Hal ini mencakup kemampuan untuk mengelola tidak hanya waktu sendiri, tetapi juga waktu proyek dan pekerja teknologi informasi yang mungkin bekerja untuk administrator. Sama berharganya dengan keterampilan manajemen waktu adalah keterampilan manajemen proyek, yang berpusat pada kemampuan untuk menjaga proyek sesuai jadwal dan menggunakan alat estimasi proyek, alat penjadwalan proyek, dan metode lain untuk penilaian proyek berkelanjutan. Terakhir, seorang administrator jaringan harus memiliki keterampilan pembuatan dan penegakan kebijakan, yang mencakup kemampuan untuk membuat kebijakan mengenai penggunaan sistem komputer, akses ke fasilitas, perlindungan kata sandi, akses ke aplikasi, akses ke database, distribusi perangkat keras dan perangkat lunak, penggantian perangkat keras dan perangkat lunak, dan penanganan permintaan layanan.

Untuk mempelajari keterampilan baru dan menunjukkan kemahiran dalam bidang tertentu, administrator jaringan dapat memperoleh sertifikasi. Dimungkinkan untuk mendapatkan sertifikasi pada jenis sistem operasi jaringan tertentu, seperti Windows Server, atau pada merek peralatan jaringan tertentu, seperti router Cisco. Berikut ini adalah daftar beberapa program sertifikasi yang lebih populer:

- Microsoft Certified Systems Engineer (MCSE)—Sertifikat ini membahas desain, instalasi, dan dukungan sistem operasi jaringan Windows.
- Cisco Certified Network Associate (CCNA)—Sertifikat ini mencakup topik pemasangan, konfigurasi, pengoperasian, dan pemecahan masalah router dan jaringan switch tingkat perusahaan.
- IBM Certified Systems Expert (CSE) dan Certified Administrator (CA)—Sertifikat ini menunjukkan kemampuan untuk merencanakan, menginstal, dan mendukung produk jaringan IBM dengan sukses.

Posisi administrator jaringan sangat menuntut, menantang, dan selalu berubah. Menjadi administrator jaringan yang sukses memerlukan berbagai keterampilan teknis, manajemen, dan interpersonal. Administrator jaringan yang baik terus-menerus mempelajari keterampilan baru dan berusaha mengikuti perkembangan teknologi yang berkembang pesat. Sebuah sistem jaringan komputer tidak dapat bertahan tanpa adanya administrator jaringan. Administrator jaringan harus ingat, bagaimanapun, bahwa sistem juga tidak akan bertahan tanpa pengguna. Mari kita lihat alat tambahan yang dapat digunakan administrator jaringan untuk mendukung atau meningkatkan sistem: statistik.

13.8 MENGHASILKAN STATISTIK YANG DAPAT DIGUNAKAN

Jaringan komputer selalu mengalami perubahan. Pengguna dan aplikasi baru ditambahkan, sedangkan pengguna lama dan aplikasi yang tidak diinginkan dihapus. Usia suatu jaringan (dan teknologi yang mendasarinya) sering kali didasarkan pada tahun Internet, yang oleh banyak ahli disamakan dengan sekitar 90 hari kalender. Karena teknologi berubah begitu cepat dan jaringan terus-menerus diminta untuk mendukung aplikasi baru dan

komputasi intensif, administrator jaringan terus berupaya meningkatkan kecepatan transfer data dan throughput aplikasi jaringan.

Untuk mendukung perubahan pada suatu jaringan, seorang administrator jaringan memerlukan dana. Sayangnya, manajemen tidak selalu mau menginvestasikan lebih banyak dana di bidang teknologi. Seringkali, manajemen perlu diyakinkan bahwa pelayanan sedang buruk atau waktu tanggap tidak sesuai dengan yang diharapkan. Statistik sistem jaringan komputer dapat menjadi alat yang sangat berguna untuk menunjukkan perlunya investasi di bidang teknologi. Jika dihasilkan dengan benar, statistik dapat digunakan untuk mendukung permintaan sistem baru atau modifikasi pada sistem yang sudah ada.

Empat statistik, atau ukuran, yang berguna dalam mengevaluasi jaringan adalah waktu rata-rata antara kegagalan, waktu rata-rata untuk perbaikan, ketersediaan, dan keandalan. Waktu rata-rata antar kegagalan (MTBF) adalah waktu rata-rata suatu perangkat atau sistem akan beroperasi sebelum gagal. Nilai ini terkadang dihasilkan oleh produsen peralatan dan diteruskan ke pembeli. Namun seringkali nilai ini tidak tersedia, dan pemilik peralatan harus menghasilkan nilai MTBF dari kinerja peralatan di masa lalu. Meskipun setiap perangkat berbeda, semakin lama waktu rata-rata antar kegagalan, semakin baik.

Mean time to Repair (MTTR) adalah waktu rata-rata yang diperlukan untuk memperbaiki kegagalan dalam jaringan komputer. Waktu ini mencakup waktu yang diperlukan untuk mengisolasi kegagalan. Ini juga mencakup waktu yang diperlukan untuk menukar komponen yang rusak dengan komponen yang berfungsi atau memperbaiki komponen — baik di lokasi atau dengan melepas komponen dan mengirimkannya ke pusat perbaikan. Terakhir, waktu rata-rata untuk perbaikan mencakup waktu yang diperlukan untuk mengembalikan sistem ke pengoperasian normal. Nilai waktu rata-rata untuk perbaikan bergantung pada setiap instalasi dan, dalam suatu instalasi, pada setiap jenis komponen. Misalnya, server jaringan dengan perangkat hot-swappable harus memiliki waktu perbaikan yang lebih singkat dibandingkan perangkat yang harus dimatikan, dibuka, diperbaiki, dan kemudian di-boot ulang.

Statistik ketiga, ketersediaan, adalah probabilitas bahwa suatu komponen atau sistem tertentu akan tersedia selama jangka waktu tertentu. Komponen atau jaringan dengan ketersediaan tinggi (mendekati 1.0) hampir selalu beroperasi. Perangkat lunak yang menghasilkan statistik sering kali menghitung nilai ketersediaan berdasarkan waktu rata-rata untuk perbaikan dan waktu rata-rata antara nilai kegagalan. Komponen dengan MTTR kecil dan MTBF besar akan menghasilkan nilai ketersediaan yang sangat mendekati 1,0. Namun, untuk mempermudah, kami akan menghitung ketersediaan dengan mengurangi waktu henti dari total waktu tersedia dan kemudian membaginya dengan total waktu tersedia:

$$\text{Availability}\% = (\text{Total available time} - \text{Downtime}) / \text{Total available time}$$

Misalkan kita ingin menghitung ketersediaan printer selama satu bulan (24 jam per hari selama 30 hari, atau 720 jam), dengan mengetahui bahwa printer akan mati (tidak dapat dioperasikan) selama 2 jam selama periode tersebut.

$$\text{Availability\%} = \frac{720 - 2}{720} = 0.997$$

Karena ketersediaannya mendekati 1,0, kemungkinan besar printer akan tersedia selama periode satu bulan tersebut.

Untuk menghitung ketersediaan suatu sistem komponen, Anda harus menghitung ketersediaan setiap komponen dan mencari produk dari semua ketersediaan. Misalnya, jika jaringan memiliki tiga perangkat dengan ketersediaan 0,992, 0,894, dan 0,999, ketersediaan jaringan adalah hasil kali $0,992 \times 0,894 \times 0,999$, atau 0,886. Perusahaan biasanya ingin melihat nilai ketersediaan di angka “sembilan”, dan semakin banyak angka sembilan semakin baik. Misalnya, 0,9999 lebih baik dari 0,999.

Statistik keempat, keandalan, menghitung probabilitas bahwa suatu komponen atau sistem akan beroperasi selama durasi transaksi waktu t . Keandalan ditentukan oleh persamaan

$$R(t) = e^{-bt}$$

di mana:

$$b = 1/MTBF$$

$$t = \text{interval waktu transaksi}$$

Berapa keandalan router jika MTBF 3000 jam dan transaksi memakan waktu 20 menit, atau 1/3 jam (0,333 jam)?

$$R(0.333 \text{ jam}) = e^{-(1/3000)(0.333)} = e^{-0.000111} = 0.99989$$

Keandalan router sangat mendekati 1.0. Keandalan yang tepat 1,0 berarti jaringan atau perangkat dapat diandalkan 100 persen sepanjang waktu.

Bagaimana jika keandalan perangkat kedua dihitung dan ternyata 0,995? Meskipun nilai ini juga tampak mendekati 1,0, terdapat perbedaan antara kedua reliabilitas: 0,00489. Perbedaan ini pada dasarnya berarti bahwa dalam 1000 pengulangan percobaan, kegagalan tertentu dapat terjadi lima kali pada perangkat kedua. Dalam sebuah jaringan, banyak kejadian yang terjadi atau berulang ribuan kali, sehingga Anda tentu tidak ingin mengalami lima kegagalan perangkat dalam setahun, terutama saat transmisi data. Oleh karena itu, banyak administrator jaringan berusaha untuk mempertahankan nilai ketersediaan dan keandalan sistem dari 0,9999 hingga 0,99999.

Sekarang mari kita lihat beberapa alat lain yang dapat digunakan oleh administrator jaringan, bersama dengan statistik yang dapat digunakan ini, untuk memantau dan mendukung suatu sistem.

13.9 ALAT DIAGNOSTIK JARINGAN

Untuk mendukung jaringan komputer dan semua stasiun kerja, node, pengkabelan, aplikasi, dan protokolnya, administrator jaringan dan staf pendukungnya memerlukan seperangkat alat diagnostik. Peralatan diagnostik yang ada terus bertambah, dengan alat yang lebih canggih dan bermanfaat yang tersedia setiap hari. Alat diagnostik dapat dikelompokkan menjadi dua kategori: alat yang menguji dan men-debug perangkat keras jaringan, dan alat yang menganalisis data yang dikirimkan melalui jaringan. Terakhir, pusat komando dan meja bantuan harus dipertimbangkan. Meskipun bukan alat yang lazim, pusat komando dan meja bantuan merupakan tambahan yang berharga bagi gudang staf pendukung jaringan. Kami akan memeriksa alat yang menguji perangkat keras jaringan terlebih dahulu.

Alat yang menguji dan men-debug perangkat keras jaringan

Alat yang menguji dan men-debug perangkat keras jaringan berkisar dari perangkat yang sangat sederhana hingga perangkat yang lebih rumit dan kompleks. Tiga perangkat pengujian yang umum adalah penguji listrik (yang paling sederhana), penguji kabel, dan penguji jaringan area lokal (yang paling rumit).

Penguji listrik mengukur volt AC dan DC, resistansi, dan kontinuitas. Penguji listrik akan menunjukkan apakah ada tegangan pada saluran, dan jika ya, berapa besar tegangannya. Jika dua kabel telanjang saling bersentuhan, maka akan terjadi korsleting, dan penguji kelistrikan akan menunjukkan hambatan nol. Penguji kontinuitas adalah perangkat praktis yang menunjukkan apakah dua kabel dihubungkan satu sama lain. Penguji kelistrikan dan kontinuitas digunakan untuk menentukan apakah kabel itu sendiri mengalami masalah kelistrikan sederhana.

Penguji kabel adalah perangkat yang sedikit lebih rumit. Mereka dapat memverifikasi konektivitas dan menguji gangguan saluran, seperti sirkuit terbuka, sirkuit pendek, sirkuit terbalik, dan sirkuit bersilangan. Jenis penguji kabel genggam tertentu juga dapat menguji jalur serat optik, jaringan Mode Transfer Asinkron, dan sirkuit T-1. Misalnya, jika konektor yang tersembunyi di lemari kabel berisi dua kabel yang dialihkan, penguji kabel akan mendeteksi masalahnya dan menunjukkan sumber masalahnya.

Salah satu perangkat yang paling rumit adalah penguji jaringan area lokal. Penguji ini dapat beroperasi pada Ethernet baik mereka mempunyai switch atau tidak. Beberapa penguji jaringan area lokal memiliki tampilan yang secara grafis menunjukkan segmen jaringan dan semua perangkat yang terpasang padanya. Ketika dicolokkan ke jack jaringan yang tersedia, penguji ini dapat memecahkan masalah jaringan dan menyarankan kemungkinan koreksi. Masalah umum yang dipecahkan oleh perangkat ini adalah identifikasi dan lokasi kartu antarmuka jaringan (NIC) yang melakukan transmisi terus-menerus tetapi tidak mengirimkan data yang valid (jabber). Penguji akan menentukan NIC yang tepat dengan menunjukkan alamat NIC 48-bit. Administrator jaringan kemudian dapat mencari alamat NIC tertentu dalam dokumentasi sistem dan memetakannya ke mesin unik di kantor unik.

Sniffer jaringan

Kategori kedua dari alat diagnostik mencakup alat yang menganalisis data yang dikirimkan melalui jaringan. Alat-alat ini mencakup penganalisis protokol dan perangkat atau

perangkat lunak yang meniru protokol dan aplikasi. Salah satu alat yang paling umum adalah penganalisis lalu lintas atau penganalisis protokol. Penganalisis protokol, atau sniffer, memantau jaringan 24 jam sehari, tujuh hari seminggu, dan menangkap serta mencatat semua paket yang dikirimkan. Protokol setiap paket dianalisis, dan statistik dihasilkan yang menunjukkan perangkat mana yang berbicara satu sama lain dan aplikasi mana yang sedang digunakan. Informasi ini kemudian dapat digunakan untuk memperbaiki jaringan agar beroperasi lebih efektif. Misalnya, jika penganalisis protokol menunjukkan bahwa aplikasi tertentu sering digunakan dan membebani sumber daya jaringan, administrator jaringan dapat mempertimbangkan alternatif seperti mengganti aplikasi dengan yang lebih efisien atau mendistribusikan ulang aplikasi ke lokasi tempat yang paling sering digunakan.

Sniffer yang sangat populer yang dapat digunakan pada jaringan UNIX dan Windows adalah Wireshark (sebelumnya disebut Ethereal). Wireshark memungkinkan Anda memeriksa data yang dikumpulkan dari jaringan langsung atau dari file pengambilan di disk. Anda dapat menelusuri data yang diambil secara interaktif dan melihat informasi rinci untuk setiap paket atau informasi ringkasan untuk seluruh jaringan. Yang mungkin lebih menarik tentang Wireshark adalah gratis.

Bahkan perusahaan dengan alat dan teknik terkini mungkin mengalami kesulitan dalam mendukung penggunaannya dengan baik. “Alat” lain yang diperlukan adalah pusat kendali dan meja bantuan. Dengan pusat kendali dan meja bantuan, tim dukungan jaringan dapat menghadirkan “wajah” yang ramah kepada pengguna, seseorang yang dapat dihubungi ketika pengguna mengalami kesulitan.

Mengelola operasi

Untuk membantu administrator jaringan dan ahli teknologi informasi dalam melakukan pekerjaannya, bisnis memiliki pusat kendali untuk layanan komputasi mereka. Pusat kendali adalah jantung dari semua operasi jaringan. Ini berisi, di satu tempat yang mudah diakses, semua dokumentasi jaringan, termasuk manual sumber daya jaringan, manual pelatihan, studi dasar, semua dokumentasi peralatan, panduan pengguna, nama vendor dan nomor telepon, manual prosedur, dan formulir yang diperlukan untuk meminta layanan atau peralatan. Pusat kendali juga dapat berisi pusat pelatihan untuk membantu pengguna dan ahli teknologi informasi lainnya. Selain itu, pusat kendali berisi semua perangkat keras dan perangkat lunak yang diperlukan untuk mengendalikan dan memantau jaringan dan operasinya.

Salah satu elemen terpenting dari pusat kendali adalah meja bantuan. Meja bantuan menjawab semua panggilan telepon dan pertanyaan langsung mengenai layanan komputer di dalam perusahaan. Baik digunakan untuk mengatasi masalah perangkat keras, menjawab pertanyaan tentang menjalankan paket perangkat lunak tertentu, atau memperkenalkan pengguna perusahaan pada layanan komputasi baru, meja bantuan adalah pintu gerbang antara pengguna dan layanan komputasi dan jaringan. Untungnya, tersedia paket perangkat lunak help desk yang baik sehingga staf operasi yang mendukung layanan komputasi dapat digunakan untuk melacak dan mengidentifikasi area masalah dalam sistem.

Pusat kendali dan meja bantuan yang dirancang dengan baik dapat memberikan dampak besar pada pengguna dalam bisnis. Ketika pengguna mengetahui ada orang yang ramah dan siap membantu mereka untuk mengatasi masalah komputasi apa pun, gesekan sistem komputer/pengguna komputer akan jauh lebih sedikit.

Sekarang kita telah memeriksa alat fisik yang dapat membantu administrator jaringan mendukung jaringan perusahaan, kita akan memeriksa beberapa alat perangkat lunak yang dapat meringankan beban administrasi jaringan.

Protokol manajemen jaringan sederhana

Bayangkan Anda adalah administrator jaringan dari suatu jaringan yang terdiri dari berbagai jenis perangkat, termasuk workstation, router, bridge, switch, dan hub. Pengoperasian jaringan telah berjalan lancar selama beberapa waktu, namun kemudian tiba-tiba jaringan mulai mengalami masalah. Ini menjadi lamban, dan pengguna mulai menelepon Anda mengeluhkan waktu respons jaringan yang buruk. Adakah yang dapat Anda lakukan untuk memantau atau menganalisis jaringan tanpa meninggalkan kantor Anda dan berlari dari ruangan ke ruangan atau gedung ke gedung? Ada—jika semua atau sebagian besar perangkat di jaringan mendukung protokol manajemen jaringan. Protokol manajemen jaringan memfasilitasi pertukaran informasi manajemen antar perangkat jaringan. Informasi ini dapat digunakan untuk memantau kinerja jaringan, menemukan masalah jaringan, dan kemudian menyelesaikan masalah tersebut—semuanya tanpa harus ada personel jaringan yang menyentuh perangkat yang terpengaruh secara fisik.

Meskipun terdapat sejumlah protokol yang berbeda untuk mendukung manajemen jaringan, ada satu protokol yang menonjol sebagai protokol yang paling sederhana untuk dioperasikan, paling mudah diterapkan, dan paling banyak digunakan: Protokol Manajemen Jaringan Sederhana. Simple Network Management Protocol (SNMP) adalah standar industri yang dibuat oleh Internet Engineering Task Force dan awalnya dirancang untuk mengelola komponen Internet; sekarang juga digunakan untuk mengelola jaringan area luas dan sistem telekomunikasi. Saat ini SNMP sudah memasuki versi ketiga.

Ketiga versi SNMP didasarkan pada serangkaian prinsip berikut. Objek jaringan terdiri dari elemen jaringan seperti server, komputer mainframe, printer, hub, jembatan, router, dan switch. Masing-masing elemen ini dapat diklasifikasikan menjadi terkelola atau tidak terkelola. Elemen yang dikelola memiliki perangkat lunak manajemen, yang disebut agen, yang berjalan di dalamnya dan lebih rumit serta mahal dibandingkan elemen yang tidak dikelola. Jenis objek kedua—perangkat lunak pengelola SNMP—mengendalikan operasi elemen yang dikelola dan memelihara database informasi tentang semua elemen yang dikelola. Manajer SNMP dapat menanyakan setiap agen dan menerima data manajemen, yang kemudian disimpan dalam database. Seorang agen dapat mengirimkan informasi yang tidak diminta kepada manajer dalam bentuk alarm. Akhirnya, seorang manajer SNMP sendiri juga dapat bertindak sebagai agen jika manajer SNMP tingkat yang lebih tinggi memanggil manajer tersebut untuk memberikan informasi untuk database tingkat yang lebih tinggi. Semua pengelolaan dan penyampaian informasi ini dapat dilakukan secara lokal atau jarak jauh, misalnya, dari seluruh negeri jika informasi tersebut dikirimkan melalui Internet.

Basis data yang menyimpan informasi tentang semua perangkat yang dikelola disebut Basis Informasi Manajemen (MIB). Informasi yang disimpan di MIB dapat digunakan untuk memperbaiki atau mengelola jaringan, atau sekadar mengamati pengoperasian jaringan. Seorang manajer dapat menanyakan elemen yang dikelola (agen), menanyakan detail tertentu dari operasi elemen tersebut pada saat itu. Informasi ini kemudian dikirim dari elemen terkelola ke MIB untuk disimpan. Misalnya, seorang manajer mungkin bertanya kepada router berapa banyak paket yang masuk ke router, berapa banyak paket yang keluar dari router, dan berapa banyak paket yang dibuang karena ruang buffer tidak mencukupi. Informasi ini nantinya dapat digunakan oleh program manajemen, yang mungkin, setelah melihat informasi di MIB, menyimpulkan bahwa elemen tertentu tidak bekerja dengan baik.

SNMP juga dapat melakukan jenis operasi penemuan otomatis. Operasi ini digunakan untuk menemukan elemen baru yang telah ditambahkan ke jaringan. Ketika SNMP menemukan elemen baru yang ditambahkan, informasi tentang elemen tersebut ditambahkan ke MIB. Dengan demikian, SNMP merupakan protokol dinamis yang secara otomatis dapat beradaptasi dengan perubahan jaringan. Adaptasi ini tidak memerlukan intervensi manusia (kecuali intervensi yang melibatkan menghubungkan elemen baru ke jaringan).

Elemen yang dikelola dipantau dan dikontrol menggunakan tiga perintah dasar SNMP: baca, tulis, dan jebakan. Perintah baca dikeluarkan oleh manajer untuk mengambil informasi dari agen dalam elemen yang dikelola. Perintah write juga dikeluarkan oleh manajer, namun digunakan untuk mengontrol agen dalam elemen terkelola. Dengan menggunakan perintah tulis, manajer dapat mengubah pengaturan di agen, sehingga membuat elemen yang dikelola bekerja secara berbeda.

Kelemahan dari dua versi pertama SNMP adalah kurangnya keamanan pada perintah tulis ini. Siapapun yang menyamar sebagai manajer SNMP dapat mengirimkan perintah tulis palsu ke elemen yang dikelola dan dengan demikian menyebabkan potensi kerusakan pada jaringan. SNMP versi 3 mengatasi masalah keamanan, sehingga pengelola palsu tidak dapat mengirimkan perintah tulis berbahaya.

Perintah ketiga—perangkap—digunakan oleh elemen terkelola untuk mengirim laporan ke manajer. Ketika jenis kejadian tertentu, seperti buffer overflow, terjadi, elemen yang dikelola dapat mengirimkan jebakan untuk melaporkan kejadian tersebut.

Lebih sering daripada tidak, manajer SNMP meminta informasi langsung dari elemen yang dikelola di jaringan yang sama. Namun bagaimana jika seorang manajer ingin mengumpulkan informasi dari jaringan jarak jauh? Pemantauan Jaringan Jarak Jauh (RMON) adalah protokol yang memungkinkan administrator jaringan memantau, menganalisis, dan memecahkan masalah sekelompok elemen yang dikelola dari jarak jauh. RMON didefinisikan sebagai perpanjangan dari SNMP, dan versi terbaru yang paling populer adalah RMON versi 2 (sering disebut sebagai RMON2). RMON dapat didukung oleh perangkat pemantauan perangkat keras (dikenal sebagai probe), melalui perangkat lunak, atau melalui kombinasi perangkat keras dan perangkat lunak. Sejumlah vendor menyediakan produk jaringan dengan dukungan RMON. Misalnya, rangkaian switch jaringan area lokal Cisco mencakup switch

dengan perangkat lunak yang dapat merekam informasi saat lalu lintas melewati switch dan menyimpan informasi ini di MIB switch. RMON dapat mengumpulkan beberapa jenis informasi dasar, seperti jumlah paket yang dikirim, jumlah byte yang dikirim, jumlah paket yang dijatuhkan, statistik host, dan jenis peristiwa tertentu yang telah terjadi. Seorang administrator jaringan dapat mengetahui berapa banyak bandwidth atau lalu lintas yang diterapkan setiap pengguna pada jaringan dan dapat mengatur alarm untuk memperingatkan masalah yang akan datang.

Untuk melengkapi pembahasan kita mengenai desain dan manajemen jaringan, kita akan mengkaji Better Box Corporation untuk melihat bagaimana mereka dapat meningkatkan kapasitas komputasinya.

13.10 PERENCANAAN KAPASITAS DAN DESAIN JARINGAN

Untuk melihat bagaimana perencanaan kapasitas dan desain jaringan bekerja dalam situasi yang realistis, mari kita kembali ke Better Box Corporation dari Bab Sebelas. Ingatlah bahwa kantor pusat administratif Better Box berada di Chicago, dan memiliki kantor penjualan regional di Seattle, San Francisco, dan Dallas. Grup pemasaran di Chicago menjalankan aplikasi pada 25 stasiun kerja yang berdiri sendiri. Situs lain saat ini hanya memiliki beberapa workstation. Dalam Bab Sebelas, kami memecahkan masalah jaringan utama Better Box dengan menemukan cara untuk menyediakan akses jaringan kepada kantor penjualan regionalnya sehingga mereka dapat mengunggah catatan penjualan ke kantor pusat perusahaan. Solusi tersebut, seperti yang mungkin Anda ingat, melibatkan pembuatan koneksi MPLS/LAN virtual antara Seattle dan Chicago, San Francisco dan Chicago, serta Dallas dan Chicago.

Better Box kini memperluas kemampuan jaringan datanya dan meminta Anda membantu merancang jaringan perusahaan barunya. Ia ingin menambah perangkat keras dan perangkat lunak baru serta menyediakan aplikasi data baru. Meskipun perusahaan memiliki cukup dana untuk mendukung aplikasi baru, perusahaan ingin mencari solusi yang paling hemat biaya untuk jangka panjang. Better Box berencana menambah 10 stasiun kerja tambahan ke kantor Chicago dan 35 stasiun kerja ke masing-masing kantor lainnya, di Seattle, San Francisco, dan Dallas.

Di jaringan barunya, perusahaan juga akan memasang enam server berikut:

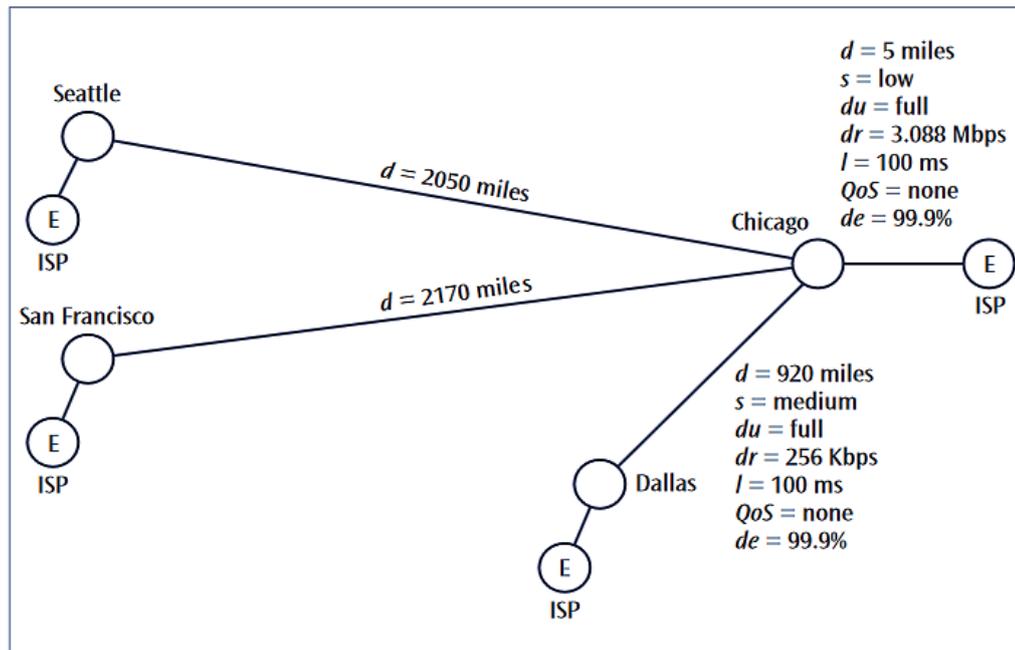
- Server web (Chicago)—Server HTTP untuk menyimpan halaman Web untuk akses publik terhadap informasi pemasaran perusahaan
- Server inventaris (Chicago)—Server database yang menyimpan informasi tentang inventaris produk yang tersedia
- Server situs (Chicago, Seattle, San Francisco, Dallas)—Empat server, satu di setiap situs, yang menyediakan layanan email untuk memungkinkan karyawan berkomunikasi tentang proyek penting, menyimpan file manajemen dan file penjualan spesifik lokasi, dan menyimpan staf perangkat lunak dan informasi untuk pekerja administrasi

Setelah stasiun kerja, server, dan peralatan jaringan baru terpasang, Better Box ingin menggunakan jaringan tersebut untuk mendukung akses server situs lokal, layanan email, dan akses Internet, dan untuk terus mendukung akses jaringan ke catatan penjualan. Setiap karyawan perlu mengakses file data di server situs di lokasinya. Selain itu, setiap server situs harus dapat bertukar pesan email dengan server situs lainnya. Selain itu, server Web harus terhubung ke Internet, sehingga pelanggan saat ini dan calon pelanggan di seluruh dunia dapat menggunakan browser Web untuk mengakses informasi perusahaan.

Sekarang mari kita cari solusi untuk masalah lengkap—untuk menyiapkan akses server situs lokal, akses email, akses Internet, dan jaringan area lokal internal, dan juga untuk menghubungkan akses jaringan yang baru diinstal ke catatan penjualan.

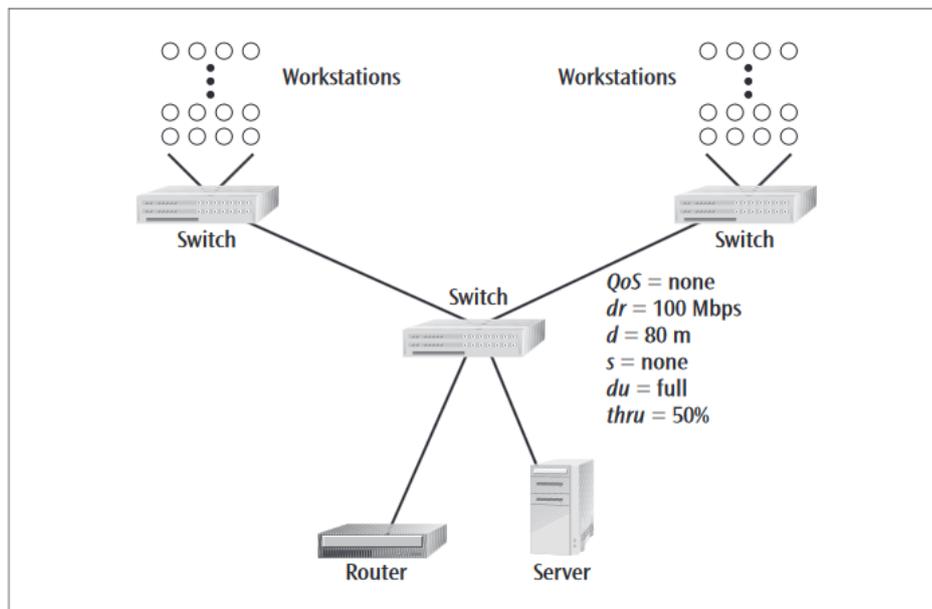
Untuk dapat mendukung akses email dan akses halaman Web Internet, setiap situs memerlukan koneksi berkecepatan tinggi ke penyedia layanan Internet lokal. Setiap pengguna Internet akan diberikan koneksi berkapasitas 100 kbps (berdasarkan perhitungan yang telah dilakukan sebelumnya pada bab ini, pada bagian perencanaan kapasitas). Dengan asumsi bahwa sepertiga dari 35 pengguna (katakanlah, 12 pengguna) di sebuah situs akan mengakses Internet pada satu waktu, proyeksi linier 12 kali 100 kbps per link menghasilkan kebutuhan koneksi 1,2 Mbps. Karena sambungan dari suatu situs ke penyedia layanan Internet harus berupa sambungan lokal, jalur T-1 lokal dapat ditambahkan ke setiap situs untuk mendukung akses Internet. Ingatlah bahwa saluran T-1 mampu mendukung aliran data 1,544-Mbps secara terus-menerus antara dua lokasi. Karena akses email juga melalui penyedia layanan Internet dan memerlukan kapasitas yang sangat rendah dibandingkan penelusuran halaman Web, jalur T-1 tambahan ini juga dapat digunakan untuk mendukung email. Mengaktifkan kantor Better Box di Chicago untuk meng-host server Web akan memerlukan koneksi lain ke penyedia layanan Internet lokal, dan penggunaan setidaknya satu jalur T-1 lagi untuk menyediakan akses 1,544-Mbps ke server Web.

Untuk membantu kita melihat tata letak fisik keseluruhan dari empat lokasi geografis, kita akan membuat peta konektivitas wilayah luas yang sederhana (Gambar 13-9). Peta konektivitas harus mencakup empat lokasi: Chicago, Seattle, San Francisco, dan Dallas. Kebutuhan jaringan yang melibatkan pengunduhan catatan penjualan dari kantor Chicago mengharuskan kita membuat koneksi antara Seattle dan Chicago, San Francisco dan Chicago, serta Dallas dan Chicago. Perhatikan pada Gambar 13-9 bahwa jarak tempuh antar lokasi disertakan di samping sambungan masing-masing. Untuk menyediakan akses email Internet dan akses Web kepada penggunanya, setiap situs memerlukan koneksi lokal ke penyedia layanan Internet. Karena penyedia layanan Internet berada di luar Better Box Corporation, setiap ISP ditampilkan sebagai lingkaran dengan huruf E melewatinya.



Gambar 13-9 Peta konektivitas area luas sederhana yang menunjukkan lokasi Seattle, San Francisco, Dallas, dan Chicago

Untuk mendukung akses server situs lokal (yang mencakup layanan email yang memungkinkan karyawan berkomunikasi tentang proyek penting, layanan penyimpanan untuk file manajemen dan penjualan spesifik lokasi, dan layanan penyimpanan untuk perangkat lunak staf dan informasi untuk pekerja administrasi), setiap situs akan perlu membuat solusi jaringan area lokal. Gambar 13-10 menunjukkan kemungkinan peta konektivitas rinci wilayah setempat. Saat ini, setiap karyawan mengakses file lokal yang cukup sehingga diperlukan setidaknya 1 Mbps bandwidth untuk setiap stasiun kerja di LAN bersama. Jika setiap situs memiliki 35 stasiun kerja, jaringan area lokal harus mendukung setidaknya kapasitas total 35-Mbps. Oleh karena itu, LAN CSMA/CD 100-Mbps akan lebih bijaksana. CSMA/CD juga merupakan pilihan yang baik karena merupakan jaringan area lokal paling populer, yang akan mengurangi biaya keseluruhan dan meningkatkan peluang tersedianya dukungan berkualitas. Versi 100-Mbps memiliki biaya yang sangat wajar, dan seharusnya cukup untuk mendukung total 35 pengguna per situs. Mungkin bermanfaat untuk menggunakan sakelar berkecepatan tinggi di jaringan area lokal ini daripada hub untuk mendukung 35 stasiun kerja; switch memberikan segmentasi jaringan yang lebih baik dan mengurangi kemungkinan tabrakan, sehingga meningkatkan throughput jaringan secara keseluruhan. Selain itu, biaya switch terus menurun, menjadikannya sangat hemat biaya, mengingat tingginya tingkat segmentasi jaringan yang mereka sediakan.



Gambar 13-10 Peta konektivitas rinci area lokal untuk salah satu situs Better Box

Kesimpulannya, Better Box akan memerlukan berbagai perangkat jaringan untuk mendukung peningkatan kebutuhan komputasinya. Koneksi MPLS/LAN virtual dari penyedia nasional akan menciptakan koneksi virtual antara masing-masing kantor penjualan regional dan kantor administrasi di Chicago. Koneksi T-1 akan menghubungkan setiap kantor ke penyedia LAN virtual menggunakan layanan jarak lokal. Setiap kantor juga memerlukan koneksi T-1 lokal tambahan ke penyedia layanan Internet. Koneksi ini akan menyediakan akses email Internet dan akses World Wide Web. Terakhir, jaringan area lokal Ethernet akan menyediakan perekat di tempat yang memungkinkan setiap stasiun kerja mengakses server lokal serta server jarak jauh melalui Internet.

RINGKASAN

- Saat membuat jaringan baru atau menambah jaringan yang sudah ada, terdapat banyak potensi kendala dan peluang terjadinya penilaian yang tidak akurat dan tidak lengkap.
- Siklus Hidup Pengembangan Sistem adalah salah satu teknik paling populer yang digunakan untuk memandu analisis melalui proses pengambilan keputusan yang sulit dalam desain jaringan. Meskipun ada banyak versi model SDLC, sebagian besar model terdiri dari tahapan berikut: perencanaan, analisis, desain, implementasi, dan pemeliharaan.
- Orang yang merancang jaringan baru atau meningkatkan jaringan yang sudah ada mungkin ingin membuat satu atau lebih model jaringan untuk membantu mereka memvisualisasikan sistem. Peta konektivitas merupakan salah satu model jaringan yang digunakan untuk menggambarkan struktur jaringan internal dan eksternal.
- Bagian penting dari SDLC adalah melakukan satu atau lebih studi kelayakan. Studi kelayakan dapat dilakukan pada tahap perencanaan, tahap analisis, dan tahap desain.

Namun studi kelayakan juga dapat berdiri sendiri (dengan kata lain tidak harus dilakukan bersamaan dengan SDLC). Empat tipe dasar studi kelayakan adalah teknis, keuangan, operasional, dan waktu.

- Analisis pengembalian adalah salah satu teknik analisis keuangan yang dapat diterapkan pada sistem jaringan komputer yang diusulkan untuk menentukan biaya dan manfaat sistem.
- Perencanaan kapasitas adalah teknik penting yang memungkinkan administrator jaringan menentukan bandwidth jaringan yang diperlukan untuk mendukung satu atau lebih aplikasi dalam suatu bisnis. Ada sejumlah teknik untuk melakukan perencanaan kapasitas, termasuk proyeksi linier, simulasi komputer, benchmarking, dan pemodelan analitis.
- Studi dasar (baseline study) melibatkan pengukuran dan pencatatan kondisi operasi jaringan selama periode waktu tertentu. Banyak administrator jaringan merasa studi dasar adalah suatu keharusan untuk semua operasi jaringan, terlepas dari apakah lebih banyak sumber daya jaringan sedang diminta. Studi dasar dapat mempunyai beberapa tujuan, seperti memberikan pemahaman tentang sistem saat ini, membantu mengisolasi dan mengidentifikasi masalah jaringan, dan memberikan bukti bahwa lebih banyak sumber daya komputasi akan dibutuhkan dalam waktu dekat.
- Setelah jaringan beroperasi, manajemen jaringan yang baik diperlukan untuk menjaga jaringan beroperasi pada efisiensi puncak. Administrator jaringan bertanggung jawab untuk memastikan bahwa jaringan beroperasi pada efisiensi puncak. Seorang administrator jaringan harus memiliki sejumlah keterampilan, termasuk pengetahuan perangkat keras dan perangkat lunak; manajemen sumber daya manusia, manajemen waktu, manajemen anggaran, dan keterampilan pemecahan masalah; dan pengetahuan tentang statistik. Untuk mengembangkan keterampilan teknis manajer, vendor perangkat keras dan sistem perangkat lunak jaringan yang lebih populer menawarkan sejumlah program sertifikat.
- Administrator jaringan harus mampu membuat dan menggunakan statistik dasar, seperti waktu rata-rata antara kegagalan, waktu rata-rata untuk perbaikan, ketersediaan, dan keandalan. Statistik ini dapat digunakan untuk membenarkan sumber daya jaringan saat ini atau untuk memvalidasi kebutuhan sumber daya jaringan tambahan.
- Tersedia berbagai macam alat diagnostik yang dapat membantu personel jaringan dalam memecahkan masalah dan memelihara jaringan komputer kompleks yang umum ditemukan saat ini. Alat diagnostik yang lebih umum mencakup pengujian kelistrikan, pengujian kontinuitas, pengujian kabel, pengujian jaringan area lokal, penganalisis protokol, serta perangkat dan program yang dapat meniru protokol dan aplikasi.
- Semua jaringan memerlukan pusat komando. Di pusat komando inilah Anda menemukan meja bantuan, dokumentasi, pusat pelatihan, dan sistem saraf pusat operasi jaringan.

- Protokol Manajemen Jaringan Sederhana membantu personel pendukung jaringan memantau kinerja jaringan, menemukan masalah jaringan, dan kemudian menyelesaikan masalah tersebut tanpa menyentuh perangkat yang terpengaruh secara fisik. Dengan SNMP, ada perangkat atau elemen yang dikelola dan tidak dikelola. Elemen yang dikelola mempunyai agen perangkat lunak yang berjalan di dalamnya sehingga manajer perangkat lunak SNMP dapat meminta informasi. Manajer SNMP juga dapat mengirimkan informasi ke elemen yang dikelola untuk mengontrol operasi di jaringan. Basis data yang menyimpan informasi tentang setiap perangkat yang dikelola disebut Basis Informasi Manajemen. Pemantauan Jaringan Jarak Jauh adalah protokol yang memungkinkan administrator jaringan memantau, menganalisis, dan memecahkan masalah sekelompok elemen yang dikelola dari jarak jauh. RMON merupakan perpanjangan dari SNMP dan saat ini berada dalam versi kedua.

PERTANYAAN

1. Jelaskan setiap fase Siklus Hidup Pengembangan Sistem.
2. Apa tujuan utama tahap perencanaan SDLC?
3. Apa tujuan utama tahap analisis SDLC?
4. Apa tujuan utama tahap desain SDLC?
5. Apa yang dimaksud dengan peta konektivitas, dan bagaimana peta tersebut dapat membantu Anda dalam merancang jaringan?
6. Jelaskan empat jenis studi kelayakan.
7. Apa yang dimaksud dengan nilai waktu uang?
8. Jelaskan empat cara berbeda untuk melakukan perencanaan kapasitas.
9. Untuk alasan apa seseorang mungkin melakukan studi dasar?
10. Sebutkan tiga keterampilan terpenting yang harus dimiliki seorang administrator jaringan.
11. Apa perbedaan antara waktu rata-rata antara kegagalan dan waktu rata-rata perbaikan?
12. Apa yang dimaksud dengan istilah statistik “ketersediaan”?
13. Apa yang dimaksud dengan istilah “pemanfaatan”?
14. Apa yang dimaksud dengan istilah statistik “keandalan”?
15. Alat diagnostik dasar apa yang digunakan untuk mendukung jaringan komputer?
16. Apa yang harus ditemukan di pusat kendali untuk pengoperasian jaringan?
17. Apa fungsi dari Protokol Manajemen Jaringan Sederhana?
18. Apa perbedaan antara manajer dan agen di SNMP?
19. Bagaimana Remote Network Monitoring digunakan untuk membantu SNMP?

LATIHAN SOAL

1. Nyatakan selama fase atau tahapan Siklus Hidup Pengembangan Sistem yang mana tindakan berikut dilakukan:
 - A. Menginstal sistem

- B. Pengguna pelatihan
 - C. Menulis dokumentasi
 - D. Melakukan studi kelayakan
 - E. Menguji sistem
 - F. Memperbarui sistem
2. Dengan menggunakan data berikut, hitung periode pengembaliannya.
 1. Biaya pengembangan: \$418.040
 2. Biaya operasi dan pemeliharaan tahun 0 s/d tahun 6 masing-masing: 0; \$15.045; \$16.000; \$17.000; \$18.000; \$19.000; \$20.000 Tingkat diskon: 6%
 3. Manfaat (tahun 0–tahun 6): \$0; \$150.000; \$170.000; \$190.000; \$210,000; \$230.000; \$250.000
 4. Buat model analitik sederhana yang mencakup dua rumus untuk menghitung perkiraan total waktu t untuk n terminal untuk melakukan polling panggilan masuk dan polling hub. Gunakan TD = waktu untuk mengirimkan data, TRP = waktu untuk mengirimkan polling panggilan, dan THP = waktu untuk mengirimkan polling hub.
 5. Anda sedang melakukan studi dasar untuk perusahaan Anda yang berlokasi di Pantai Timur. Perusahaan Anda melakukan banyak pekerjaan dengan bisnis di Pantai Barat. Anda mencatat bahwa puncak pemanfaatan jaringan terjadi sekitar tengah hari, ketika sebagian besar karyawan Anda sedang istirahat makan siang. Apa yang menyebabkan aktivitas puncak ini?
 6. Selama studi dasar, sejumlah besar kesalahan checksum siklik ditemukan namun tidak ada yang kerdil. Jelaskan dengan tepat apa hubungan informasi ini dengan panjang segmen jaringan.
 7. Suatu komponen telah beroperasi terus menerus selama tiga bulan. Selama jangka waktu tersebut, telah gagal dua kali, sehingga mengakibatkan waktu henti selama 4,5 jam. Hitung ketersediaan komponen selama periode tiga bulan ini.
 8. Jika suatu komponen mempunyai $MTBF = 10$ jam dan transaksi memakan waktu 20 menit, hitunglah keandalan komponen tersebut.
 9. Jika suatu komponen memiliki $MTBF = 500$ jam dan transaksi membutuhkan waktu 4 detik, hitung keandalan komponen tersebut.
 10. Jika suatu jaringan mempunyai empat perangkat dengan ketersediaan 0,994, 0,778, 0,883, dan 0,5, berapakah ketersediaan seluruh jaringan?
 11. Apakah mungkin agen SNMP di perangkat yang dikelola juga berfungsi sebagai manajer? Jelaskan bagaimana situasi ini bisa terjadi.
 12. Apa perbedaan antara penguji kontinuitas jalur jaringan dan penguji kabel jaringan?
 13. Anda bekerja di perusahaan kecil yang memiliki jaringan area lokal dengan dua hub. Jalur komunikasi antar hub baru saja terputus, tetapi Anda belum mengetahuinya. Bagaimana Anda bisa menentukan apa yang telah terjadi?

DISKUSIKAN DENGAN KELOMPOK ANDA

1. Anda diminta membuat meja bantuan untuk divisi dukungan komputer di perusahaan Anda. Layanan apa yang akan disediakan oleh layanan bantuan Anda? Bagaimana Anda akan menyediakan layanan tersebut? Jenis karyawan apa yang akan Anda pekerjakan untuk bekerja di meja bantuan?
2. Perusahaan Anda ingin membuat server Web untuk mempromosikan bisnisnya. Salah satu fitur server Web adalah memungkinkan pengguna jarak jauh mengunduh buletin layanan dan manual perbaikan. Buletin dan manual perbaikan ini berukuran sekitar 240.000 byte. Anda mengantisipasi bahwa sekitar 30 pengguna per jam ingin mengunduh dokumen-dokumen ini. Berapa kecepatan jalur komunikasi yang Anda perlukan untuk mendukung permintaan ini?
3. Perusahaan tempat Anda bekerja menjual boneka dan pakaiannya melalui gerai ritel dan katalog pesanan lewat pos. Sekarang mereka mempertimbangkan untuk menjual barang dagangan melalui Web. Buat rencana SDLC untuk menambahkan sistem merchandising Web ke bisnis yang menunjukkan setiap langkah yang terlibat dalam fase analisis, desain, dan implementasi. Rencananya harus tampak seperti garis besar. Misalnya, tahap analisis dapat dimulai dengan hal berikut:
Tahap Analisis
 - A. Wawancara manajemen tingkat atas
 - B. Membuat kuesioner dan menyajikannya kepada karyawan saat ini
 - C. Membuat model yang menunjukkan aliran data terkini dari bisnis katalog pesanan lewat pos
 - D. Dll.
4. Buat serangkaian peta konektivitas untuk tempat kerja atau sekolah Anda. Cobalah untuk memasukkan sebanyak mungkin lokasi eksternal yang berbeda. Untuk salah satu lokasi eksternal ini, buatlah satu peta konektivitas area luas dan satu atau lebih peta konektivitas area lokal.
5. Lakukan studi dasar untuk jaringan di tempat kerja atau sekolah Anda. Buat daftar semua perangkat jaringan (server, router, bridge, switch, hub, dan sebagainya). Protokol apa yang didukung oleh jaringan? Aplikasi apa saja yang didukung oleh jaringan? Cobalah mengumpulkan beberapa statistik untuk satu jenis perangkat di jaringan. Jika tidak mungkin mendapatkan nilai sebenarnya, cukup buat daftar statistik yang berguna untuk perangkat tertentu.
6. Program sertifikasi apa, selain yang tercantum dalam bab ini, yang tersedia untuk administrator jaringan? Untuk jenis sistem apa sertifikat ini dirancang?
7. Apa saja macam tes benchmark yang tersedia untuk menguji sistem komputer atau jaringan komputer? Tulislah sebuah paragraf tentang setiap tes benchmark, dengan menyatakan apa yang sebenarnya diukur oleh tes benchmark tersebut.
8. Pindai daftar pekerjaan rahasia di surat kabar lokal Anda. Berapa persentase pengiklan yang mencari personel pendukung jaringan yang memerlukan gelar sertifikasi?

9. Sertifikasi apa yang saat ini dicari perusahaan sehubungan dengan administrator jaringan?
10. Akhir-akhir ini ada pembicaraan tentang jenis posisi baru dalam industri jaringan: arsitek TI. Apa itu arsitek TI, dan apa saja tugas pekerjaan umum yang terkait dengan posisi ini?
11. SNMP hanyalah salah satu dari beberapa protokol manajemen. Protokol manajemen apa lagi yang ada? Siapa yang menciptakannya? Situasi seperti apa yang mereka kelola?
12. Bagaimana SNMP versi 3 menangani keamanan? Tulis laporan satu atau dua halaman yang merangkum fitur-fitur utama versi 3.
13. Bagaimana cara kerja fitur penemuan otomatis SNMP?

DAFTAR PUSTAKA

- Adams, K., 2021, "Satellite Data Communication Systems", Sydney: Artech House.
- Almeroth, K. C., 2015, "Computer Networks: A Systems Approach", Burlington, MA: Morgan Kaufmann.
- Bala, K., 2017, "Data Communication and Networking", New Delhi: Pearson India.
- Behrouz, A., 2013, "Data Communication and Networking", New York: McGraw-Hill Education.
- Behrouz, A., Forouzan, B., 2016, "Data Communications and Networking", New York: McGraw-Hill Education.
- Bertsekas, D. P., Gallager, R. G., 2016, "Data Networks", Upper Saddle River, NJ: Prentice Hall.
- Blake, S., Black, C., 2015, "Java Network Programming", Sebastopol, CA: O'Reilly Media.
- Brown, C., 2019, "Wireless Data Communications", San Francisco: Morgan Kaufmann.
- Chen, Q., 2021, "Next-Generation Data Communication Technologies", Hong Kong: Springer Nature.
- Cisco Systems, Inc., 2019, "Cisco Networking Essentials", Indianapolis: Cisco Press.
- Clark, J., 2018, "High-Speed Data Communications", Paris: CRC Press.
- Clegg, R. G., 2014, "Computers and Data Processing", New York: Routledge.
- Comer, D. E., 2014, "Computer Networks and Internets", Boston: Pearson Education.
- Comer, D. E., 2015, "Internetworking with TCP/IP: Principles, Protocols, and Architecture", Boston: Pearson Education.
- Comer, D. E., 2015, "TCP/IP Illustrated, Volume 1: The Protocols", Boston: Addison-Wesley.
- Crowcroft, J., 2018, "Principles of Computer Communication Networks", Cambridge: Cambridge University Press.
- Davies, E., 2016, "Computer and Communication Networks", Boston: Pearson Education.
- Davis, M., 2016, "Fundamentals of Wireless Communication", Cambridge: Cambridge University Press.
- Fall, K. R., Stevens, W. R., 2011, "TCP/IP Illustrated, Volume 1: The Protocols", Boston: Addison-Wesley.

- Flanagan, D., Matsumoto, Y., 2015, "The Ruby Programming Language", Sebastopol, CA: O'Reilly Media.
- Forouzan, B. A., 2013, "Data Communications and Networking", New York: McGraw-Hill Education.
- Forouzan, B., 2013, "Data Communication and Networking", New York: Tata McGraw Hill.
- Frenzel, L., 2012, "Communication Electronics", New Delhi: Tata McGraw Hill.
- Garcia, F., 2018, "Mobile Data Communication Technologies", Berlin: Springer.
- Gibson, J. D., 2015, "The Communications Handbook", Boca Raton, FL: CRC Press.
- Gupta, N., 2018, "Data Communication and Computer Networks", Delhi: Pearson India.
- Halabi, S., McQuerry, S., 2016, "Internet Routing Architectures", Indianapolis: Cisco Press.
- Halsall, F., 2014, "Data Communications, Computer Networks and Open Systems", New Delhi: Pearson Education.
- Hucaby, D., 2018, "CCNA Routing and Switching 200-125 Official Cert Guide Library", Indianapolis: Cisco Press.
- Hunt, C., 2017, "TCP/IP Network Administration", Sebastopol, CA: O'Reilly Media.
- Johnson, B., 2018, "Data Communication Systems: Principles and Applications", London: Pearson Education.
- Kasera, S. K., Patel, R. B., 2017, "Computer Networks: A Systems Approach", Boston: Pearson Education.
- Kelly, K. J., 2017, "Communications Systems and Networks", London: Springer.
- Keshav, S., 2016, "An Engineering Approach to Computer Networking", New York: Addison-Wesley.
- Kim, P., 2017, "Data Communication Fundamentals", Seoul: McGraw-Hill Education.
- Kleinrock, L., Lam, F., 2010, "Computer Networks", Upper Saddle River, NJ: Prentice Hall.
- Kumar, S., 2018, "Advanced Data Communication Techniques", Mumbai: Tata McGraw-Hill.
- Kurose, J. F., Ross, K. W., 2017, "Computer Networking: A Top-Down Approach", Boston: Pearson Education.
- Lammle, T., 2016, "CCNA Routing and Switching Complete Study Guide", Indianapolis: Sybex.

- Lathi, B. P., Ding, Z., 2016, "Modern Digital and Analog Communication Systems", Oxford: Oxford University Press.
- Lee, H., 2020, "Data Communication Protocols and Systems", Singapore: McGraw-Hill.
- Lee, W. C. Y., 2015, "Mobile Communications Engineering: Theory and Applications", New York: McGraw-Hill Education.
- Liew, S. C., 2016, "Wireless Communication Systems: Advanced Techniques for Signal Reception", Cambridge: Cambridge University Press.
- Lin, S., Costello, D. J., 2015, "Error Control Coding", Upper Saddle River, NJ: Pearson Education.
- Martinez, I., 2019, "Data Communication in the Internet Age", Chicago: Wiley.
- Mattson, T. G., 2016, "Understanding Digital Signal Processing", Upper Saddle River, NJ: Pearson Education.
- Meyers, M., 2018, "All-in-One CompTIA Network+ Certification Exam Guide", New York: McGraw-Hill Education.
- Moeller, S., 2017, "Business Data Communications and Networking", Hoboken, NJ: Wiley.
- Moher, M., 2018, "Understanding Data Communications and Networks", Boston: Cengage Learning.
- O'Brien, R., 2019, "Data Communication in the Cloud", Dublin: Wiley-Blackwell.
- Pahlavan, K., Krishnamurthy, P., 2016, "Principles of Wireless Networks: A Unified Approach", Upper Saddle River, NJ: Prentice Hall.
- Panko, R. R., Panko, J. M., 2015, "Business Data Networks and Security", Boston: Pearson.
- Patel, T., 2020, "Data Communication Networks: Concepts and Trends", Ahmedabad: CRC Press.
- Perkins, C. E., McGinnis, J., 2017, "Mobile IP: Design Principles and Practices", Upper Saddle River, NJ: Addison-Wesley.
- Perlman, R., 2017, "Interconnections: Bridges, Routers, Switches, and Internetworking Protocols", Boston: Addison-Wesley.
- Peterson, L. L., Davie, B. S., 2012, "Computer Networks: A Systems Approach", Amsterdam: Morgan Kaufmann.
- Proakis, J. G., Salehi, M., 2014, "Digital Communications", New York: McGraw-Hill Education.

- Ramakrishnan, K. K., 2016, "Database Management Systems", New York: McGraw-Hill Education.
- Rice, M., 2016, "Ethernet: The Definitive Guide", Sebastopol, CA: O'Reilly Media.
- Rodriguez, M., 2020, "Data Communication Security", Madrid: Springer.
- Rose, M. T., 2017, "Computer Networking: A Beginner's Guide", New York: McGraw-Hill Education.
- Rosen, K. H., 2015, "Discrete Mathematics and Its Applications", New York: McGraw-Hill Education.
- Ross, K. W., 2017, "Networking", New York: Pearson Education.
- Schwartz, M., 2017, "Mobile Wireless Communications", Cambridge: Cambridge University Press.
- Seacord, R. C., 2017, "Secure Coding in C and C++", Boca Raton, FL: CRC Press.
- Smith, A., 2020, "Advancements in Data Communication Technology", New York: Springer.
- Stallings, W., 2014, "Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud", Boston: Pearson Education.
- Stallings, W., 2016, "Data and Computer Communications", Upper Saddle River, NJ: Pearson Education.
- Stallings, W., 2018, "High-Speed Networks and Internets: Performance and Quality of Service", Upper Saddle River, NJ: Pearson Education.
- Stevens, R. W., 2015, "TCP/IP Illustrated, Volume 2: The Implementation", Boston: Addison-Wesley.
- Stevens, R. W., 2017, "UNIX Network Programming", Boston: Addison-Wesley.
- Tanenbaum, A. S., 2014, "Computer Networks", Boston: Pearson Education.
- Tanenbaum, A. S., Wetherall, D. J., 2011, "Computer Networks", Boston: Pearson Education.
- Taylor, D., 2021, "Data Communication and Networking", Boston: Cengage Learning.
- Thomas, V., 2021, "Data Communication for Industrial Internet of Things", Zurich: Springer.
- Tittel, E., Chellis, J., Stewart, J. T., 2016, "Networking All-in-One For Dummies", Hoboken, NJ: Wiley.
- Wang, L., 2019, "Optical Fiber Communication Systems", Beijing: Tsinghua University Press.

Wayne, T., 2015, "Data Communications", New Delhi: Oxford University Press.

Westcott, D., 2015, "802.11 Wireless Networks: The Definitive Guide", Sebastopol, CA: O'Reilly Media.

White, C. S., 2018, "Data Communications and Computer Networks: A Business User's Approach", Boston: Cengage Learning.

White, E., 2017, "Fundamentals of Data Communication Networks", Amsterdam: Elsevier.

Wilson, U., 2017, "Wireless Sensor Data Communication", Manchester: Elsevier.

Zeng, H., 2017, "Fundamentals of Wireless Communication Engineering Technologies", New York: Wiley-IEEE Press.

LAMPIRAN DAFTAR TARIF SEWA WIFI

#Tarif per Juni 2024

Harga Pasang Wifi Iconnet (Jawa + Bali)

Paket	Benefit	Harga
Iconnet 20	- Up To 20 Mbps - Unlimited Quota	Rp 220.000
Iconnet 35	- Up To 35 Mbps - Unlimited Quota	Rp 230.000
Iconnet 50	- Up To 50 Mbps - Unlimited Quota	Rp 330.000
Iconnet 100	- Up To 100 Mbps - Unlimited Quota	Rp 560.000

Harga Pasang Wifi Iconnet (Sumatera & Kalimantan)

Paket	Benefit	Harga
Iconnet 20	- Up To 20 Mbps - Unlimited Quota	Rp 250.000
Iconnet 35	- Up To 35 Mbps - Unlimited Quota	Rp 260.000
Iconnet 50	- Up To 50 Mbps - Unlimited Quota	Rp 390.000
Iconnet 100	- Up To 100 Mbps - Unlimited Quota	Rp 630.000

Harga Pasang Wifi Iconnet (Indonesia Timur)

Paket	Benefit	Harga
Iconnet 20	- Up To 20 Mbps - Unlimited Quota	Rp 280.000
Iconnet 35	- Up To 35 Mbps - Unlimited Quota	Rp 290.000
Iconnet 50	- Up To 50 Mbps - Unlimited Quota	Rp 410.000
Iconnet 100	- Up To 100 Mbps - Unlimited Quota	Rp 680.000

Harga Pasang Wifi IndiHome Paket JITU 1 - 1P

Kecepatan	Benefit	Harga
-----------	---------	-------

30 Mbps	- Promo biaya pasang Rp150.000 (Normal Rp500.000) - Up to 30 Mbps	Rp 280.000
30 Mbps	- Promo biaya pasang Rp150.000 (Normal Rp500.000) - Disney+ Hotstar - Up to 30 Mbps	Rp 295.000
50 Mbps	- Bebas Biaya Pasang - Up to 50 Mbps	Rp 350.000
100 Mbps	- Bebas Biaya Pasang - Up to 100 Mbps	Rp 425.000

Harga Pasang Wifi IndiHome Paket JITU 1 - 2P

Kecepatan	Benefit	Harga
30 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Disney+ Hotstar - Telepon Rumah 100 Menit - Up to 30 Mbps	Rp 300.000
30 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Disney+ Hotstar - Indihome TV - Paket TV 81 Channel - Up to 30 Mbps	Rp 340.000
30 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 30 Mbps - Paket TV 81 Channel - Minipack Big Combo List Channel - Indihome TV - HBO Go	Rp 370.000
30 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 30 Mbps - Paket TV 81 Channel - Minipack Big Combo List Channel - Indihome TV - HBO Go - Disney+ Hotstar - Vidio - Catchplay - WeTV	Rp 455.000
50 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 50 Mbps - Telepon Rumah 100 Menit - Disney+ Hotstar	Rp 360.000
50 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 50 Mbps	Rp 505.000

- Paket TV 81 Channel
- Minipack Big Combo List Channel
- Indihome TV
- HBO Go
- Disney+ Hotstar
- Vidio
- Catchplay
- WeTV

Harga Pasang Wifi IndiHome Paket JITU 1 - 3P

Kecepatan	Benefit	Harga
30 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 30 Mbps - Telepon Rumah 100 Menit - Indihome TV - Disney+ Hotstar	Rp 360.000
30 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 30 Mbps - Telepon Rumah 100 Menit - Indihome TV - HBO Go	Rp 390.000
30 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 30 Mbps - Telepon Rumah 100 Menit - Indihome TV - Disney+ Hotstar - Catchplay - WeTV - Vidio - HBO Go	Rp 475.000
50 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 50 Mbps - Telepon Rumah 100 Menit - Indihome TV - Disney+ Hotstar - Catchplay - WeTV - Vidio - HBO Go	Rp 515.000

Harga Pasang Wifi IndiHome Netflix

Kecepatan	Benefit	Harga
30 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 30 Mbps - Paket TV 30 Channel - Netflix - Indihome TV	Rp 365.000
30 Mbps	- Promo biaya pasang Rp250.000 (Normal Rp500.000)	Rp 385.000

	<ul style="list-style-type: none"> - Up to 30 Mbps - Paket TV 30 Channel - Netflix - Indihome TV - Disney+ Hotstar 	
30 Mbps	<ul style="list-style-type: none"> - Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 30 Mbps - Telepon Rumah 50 Menit - Paket TV 77 Channel - Indihome TV - Netflix 	Rp 410.000
30 Mbps	<ul style="list-style-type: none"> - Promo biaya pasang Rp250.000 (Normal Rp500.000) - Up to 30 Mbps - Telepon Rumah 50 Menit - Paket TV 77 Channel - Indihome TV - Netflix - Disney+ Hotstar 	Rp 430.000

Harga Pasang Wifi Biznet Home Internet Only

Paket	Benefit	Harga
Internet 0D	<ul style="list-style-type: none"> - Up To 30 Mbps - Wi-Fi Fiber Modem included - IP Dynamic Private - Unlimited Bandwidth - Biznet Wifi akses - Biznet Video akses - 1 - 3 device 	Rp 250.000
Internet 1C	<ul style="list-style-type: none"> - Up To 100 Mbps - Wi-Fi Fiber Modem included - IP Dynamic Private - Unlimited Bandwidth - Biznet Wifi akses - Biznet Video akses - Biznet NEO Web Space - 1 - 10 device 	Rp 375.000
Internet 2D	<ul style="list-style-type: none"> - Up To 200 Mbps - Wi-Fi Fiber Modem included - IP Dynamic Private - Unlimited Bandwidth - Biznet Wifi akses - Biznet Video akses - Biznet NEO Web Space - 11- 20 device 	Rp 575.000

Harga Pasang Wifi Biznet Home Internet IPTV

Paket	Benefit	Harga
Home Combo 1D	<ul style="list-style-type: none"> - Wi-Fi Fiber Modem - Up To 100 Mbps 	Rp 575.000

	<ul style="list-style-type: none"> - 56 Channel IPTV - Biznet IPTV STB - IP Dynamic Private - Unlimited Bandwidth - Biznet Wifi akses - Biznet Video akses - 1-10 device 	
Home Combo 2D	<ul style="list-style-type: none"> - Wi-Fi Fiber Modem - Up To 200 Mbps - 56 Channel IPTV - Biznet IPTV STB - IP Dynamic Private - Unlimited Bandwidth - Biznet Wifi akses - Biznet Video akses - 21-40 device 	Rp 775.000

Harga Pasang Wifi Biznet Home Gamers

Paket	Benefit	Harga
Home Gamers 3D	<ul style="list-style-type: none"> - Wi-Fi Fiber Modem - Up To 250 Mbps - Biznet IPTV STB - IP Dynamic Private - Unlimited Bandwidth - Biznet Wifi akses - Biznet Video akses - 21 - 40 device 	Rp 700.000

Harga Pasang Wifi MNC Play

Paket	Benefit	Harga
20 Mbps	<ul style="list-style-type: none"> - 100% Fiber Optic - True Unlimited - Set Top Box Linux - Vision+ Premium - 73 Channel 	Rp 279.000
30 Mbps	<ul style="list-style-type: none"> - 100% Fiber Optic - True Unlimited - Set Top Box Linux - Vision+ Premium - 73 Channel 	Rp 339.000
50 Mbps	<ul style="list-style-type: none"> - 100% Fiber Optic - True Unlimited - Set Top Box Linux - Vision+ Premium - 73 Channel 	Rp 459.000
100 Mbps	<ul style="list-style-type: none"> - 100% Fiber Optic - True Unlimited 	Rp 709.000

	<ul style="list-style-type: none"> - Set Top Box Linux - Vision+ Premium - 73 Channel 	
200 Mbps	<ul style="list-style-type: none"> - 100% Fiber Optic - True Unlimited - Set Top Box Linux - Vision+ Premium - 73 Channel 	Rp 779.000

Harga Pasang Wifi Groovy Internet Unlimited Data

Paket	Benefit	Harga
Level 1 Personal	<ul style="list-style-type: none"> - Fiber Optic - 20 Mbps Speed Usage - Support 24/7 - Ticketing System - FREE installation fee - WiFi Access Point - Static IP Address - 1-4 device 	Rp 194.250
Level 2 Couples	<ul style="list-style-type: none"> - Fiber Optic - 20 Mbps Speed Usage - Support 24/7 - Ticketing System - FREE installation fee - WiFi Access Point - Static IP Address - 2-6 device 	Rp 277.500
Level 3 Family	<ul style="list-style-type: none"> - Fiber Optic - 20 Mbps Speed Usage - Support 24/7 - Ticketing System - FREE installation fee - WiFi Access Point - Static IP Address - 4-10 device 	Rp 388.500

Harga Pasang Wifi Groovy Internet Unlimited Data (Bulanan)

Paket	Benefit	Harga
Level 1 Personal	<ul style="list-style-type: none"> - 10 Mbps speed - Fiber-optic - Static IP Address - Support 24/7 - Wi-Fi Access Point - Ticketing System - Rp 499.500 installation fee - +1 month deposit - 1-4 device 	Rp 298.590
Level 2 Couples	<ul style="list-style-type: none"> - 20 Mbps speed - Fiber-optic - Static IP Address - Support 24/7 	Rp 409.590

	<ul style="list-style-type: none"> - Wi-Fi Access Point - Ticketing System - Rp 499.500 installation fee - +1 month deposit - 2-6 device 	
Level 3 Family	<ul style="list-style-type: none"> - 30 Mbps speed - Fiber-optic - Static IP Address - Support 24/7 - Wi-Fi Access Point - Ticketing System - Rp 499.500 installation fee - +1 month deposit - 4-10 device 	Rp 520.590

Harga Pasang Wifi First Media Paket Stream

Paket	Benefit	Harga
Value	<ul style="list-style-type: none"> - Up To 30 Mbps - 1-4 perangkat - HBO Go - Streamtainment - Cashback Rp 15.000/bulan 	Rp 275.000
Pro	<ul style="list-style-type: none"> - Up To 150 Mbps - Hingga 8 perangkat - HBO Go - Streamtainment - Cashback Rp 15.000/bulan 	Rp 525.000
Premium	<ul style="list-style-type: none"> - Up To 250 Mbps - untuk 9 - 15 perangkat - HBO Go. Cinema, world, Viu - Double Cashback Rp 70.000/bulan - Cashback Rp 35.000/bulan 	Rp 695.000

Harga Pasang Wifi First Media Paket Joy

Paket	Benefit	Harga
Value	<ul style="list-style-type: none"> - Up To 50 Mbps - 1-5 device - 84 TV Channel - Cashback 15rb/bulan 	Rp 340.000
Pro	<ul style="list-style-type: none"> - Up To 100 Mbps - 8 device - 84 TV Channel - Cashback 25rb/bulan 	Rp 415.000
Premium	<ul style="list-style-type: none"> - Up To 175 Mbps - 9-15 device - 184 Channel - Cashback 35rb/bulan 	Rp 665.000

Harga Pasang Wifi First Media Paket Star

Paket	Benefit	Harga
Value	<ul style="list-style-type: none"> - Up To 250 Mbps - 15 device - HBO GO, CP+, LGP, VIU - Streamtainment - 207 TV Channels - Cashback 50rb/bulan 	Rp 975.000
Pro	<ul style="list-style-type: none"> - Up To 350 Mbps - 20 device - HBO GO, CP+, LGP, VIU - Streamtainment - 207 TV Channels - Cashback 100rb/bulan - Extra Cashback Rp 100.000 	Rp 1.798.500
Premium	<ul style="list-style-type: none"> - Up To 500 Mbps - 20 device - HBO GO, CP+, LGP, VIU - Streamtainment - 228 TV Channels - Cashback 200rb/bulan 	Rp 3.106.500

Harga Pasang Wifi XL Satu Fiber

Paket	Benefit	Harga
Value	<ul style="list-style-type: none"> - Up To 75 Mbps - Unlimited - Kuota +8GB (2 nomor) - 2 kartu perdana XL Prabayar - Free Nelpon dan SMS ke XL & AXIS - Free Sewa STB (termasuk dalam paket) - Gratis biaya instalasi 	Rp 259.000
Smart	<ul style="list-style-type: none"> - Up To 150 Mbps - Unlimited - Kuota +15GB (2 nomor) - 2 kartu perdana XL Prabayar - Free Nelpon dan SMS ke XL & AXIS - Free Sewa STB (termasuk dalam paket) - Gratis biaya instalasi 	Rp 334.000
Family	<ul style="list-style-type: none"> - Up To 200 Mbps - Unlimited - Kuota +25GB (2 nomor) - 2 kartu perdana XL Prabayar - Free Nelpon dan SMS ke XL & AXIS - Free Sewa STB (termasuk dalam paket) - Gratis biaya instalasi 	Rp 399.000

Harga Pasang Wifi XL Satu Lite

Paket	Benefit	Harga
Value	<ul style="list-style-type: none"> - Unlimited (FUP 30GB) - Kuota +15GB (2 nomor) - 2 perdana XL Prabayar - Gratis Nelpon dan SMS ke XL & AXIS - Gratis biaya instalasi 	Rp 129.000
Smart	<ul style="list-style-type: none"> - Unlimited (FUP 60GB) - Kuota +25GB (2 nomor) - 2 perdana XL Prabayar - Gratis Nelpon dan SMS ke XL & AXIS - Gratis biaya instalasi 	Rp 199.000
Family	<ul style="list-style-type: none"> - Unlimited (FUP 120GB) - Kuota +50GB (2 nomor) - 2 perdana XL Prabayar - Gratis Nelpon dan SMS ke XL & AXIS - Gratis biaya instalasi 	Rp 299.000

Harga Pasang Wifi XL Satu Biz

Paket	Benefit	Harga
Starter	<ul style="list-style-type: none"> - Unlimited (up to 100mbps) - Kuota +50GB (5 nomor) - 5 perdana XL Prabayar Biz On - Gratis Nelpon dan SMS ke XL & AXIS - Gratis biaya instalasi - Gratis aplikasi Majoo 	Rp 419.000
Prime	<ul style="list-style-type: none"> - Unlimited (up to 300mbps) - Kuota +100GB (10 nomor) - 5 perdana XL Prabayar Biz On - Gratis Nelpon dan SMS ke XL & AXIS - Gratis biaya instalasi - Gratis aplikasi Majoo 	Rp 609.000

Harga Pasang Wifi CBN Fiber

Paket	Benefit	Harga
Fiber 50	<ul style="list-style-type: none"> - Up To 50 Mbps - Dens.TV+Lite - 1-3 perangkat 	Rp 229.000
Fiber 100	<ul style="list-style-type: none"> - Up To 100 Mbps - Dens.TV Box+Apps - Vision+ Premium Sports - 4-5 perangkat 	Rp 429.000
Fiber 250	<ul style="list-style-type: none"> - Up To 250 Mbps - Dens.TV Box+Premium - Vision+ Premium Sports - 5-7 perangkat 	Rp 799.000
Fiber 500	<ul style="list-style-type: none"> - Up To 500 Mbps - Dens.TV Box+Premium - Vision+ Premium Sports - 5-10 perangkat 	Rp 1.399.000

Fiber 1G	<ul style="list-style-type: none"> - Up To 1 Gbps - Dens.TV Box+Premium - Vision+ Premium Sports - 10-15 perangkat 	Rp 3.999.000
-----------------	--	--------------

Harga Pasang Wifi My Republic Internet + TV

Paket	Benefit	Harga
Value	<ul style="list-style-type: none"> - Up To 30 Mbps - Unlimited Quota - 73 Channel - 1-5 device 	Rp 316.000
Fast	<ul style="list-style-type: none"> - Up To 50 Mbps - Unlimited Quota - 76 Channel - 1-10 device 	Rp 399.000
Nova	<ul style="list-style-type: none"> - Up To 100 Mbps - Unlimited Quota - 76 Channel - 1-15 device - Exclusive Router 	Rp 482.000
MyGamer	<ul style="list-style-type: none"> - Up To 260 Mbps - Unlimited Quota - 76 Channel - 1-25 device - Exclusive Router 	Rp 704.850

Harga Pasang Wifi Oxygen Stream

Paket	Benefit	Harga
30 Mbps	<ul style="list-style-type: none"> - Kuota unlimited - WiFi modem - Gratis instalasi 	Rp 306.000
50 Mbps	<ul style="list-style-type: none"> - Kuota unlimited - WiFi modem - Gratis instalasi 	Rp 414.000
75 Mbps	<ul style="list-style-type: none"> - Kuota unlimited - WiFi modem - Gratis instalasi 	Rp 495.000
100 Mbps	<ul style="list-style-type: none"> - Kuota unlimited - WiFi modem - Gratis instalasi 	Rp 576.000

Harga Pasang Wifi Oxygen Stream+

Paket	Benefit	Harga
-------	---------	-------

30 Mbps	<ul style="list-style-type: none">- Kuota unlimited- WiFi modem- Gratis instalasi- 68 saluran TV	Rp 324.000
50 Mbps	<ul style="list-style-type: none">- Kuota unlimited- WiFi modem- Gratis instalasi- 68 saluran TV	Rp 432.000
75 Mbps	<ul style="list-style-type: none">- Kuota unlimited- WiFi modem- Gratis instalasi- 68 saluran TV	Rp 515.000
100 Mbps	<ul style="list-style-type: none">- Kuota unlimited- WiFi modem- Gratis instalasi- 68 saluran TV	Rp 595.000

KOMUNIKASI DATA BISNIS dan 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

ISBN 978-623-8642-11-3 (PDF)



9 786238 642113