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

Jaringan Sistem Komputer

Jilid 2

YAYASAN PRIMA AGUS TEKNIK

Jaringan Sistem Komputer

Jilid 2

Dr. Ir. 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 Salatiga (UKSW). Disiplin ilmu yang dikuasai 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. 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 978-623-5734-26-2 (jil_2 PDF)

9 786235 734262

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

Jaringan Sistem Komputer

Jilid 2

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

JARINGAN SISTEM KOMPUTER jilid 2

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

ISBN : 9 786235 734262

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

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

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

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

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

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

Hak cipta dilindungi undang-undang
Dilarang memperbanyak karya tulis ini dalam bentuk dan dengan cara apapun tanpa ijin dari penulis

Kata Pengantar

Puji syukur penulis panjatkan kepada Tuhan semesta alam atas selesainya buku "Jaringan SIstem Komputer Jilid 2" ini. Jaringan komputer memberikan banyak manfaat bagi kehidupan umat manusia. Dengan semakin berkembangnya teknologi khususnya di bidang komputerisasi saat ini, pengetahuan dan penguasan yang mendalam tentang sistem dan program komputer niscaya menjadi salah satu kebutuhan pokok bagi setiap individu agar tidak tertinggal dalam dinamisme perubahan teknologi.

Buku Jaringan Sistem Komputer merupakan buku yang memberikan pengetahuan secara lengkap dan jelas tentang pengertian dan dasar dasar pemrograman jaringan komputer dan internet. Buku ini adalah lanjutan dari buku Jilid 1 Jaringan Sistem Komputer. Buku ini sebagai pelengkap dari buku Jilid 1, sehingga memudahkan para pembaca khususnya mahasiswa untuk lebih memahami dan lebih memperdalam pengetahuan tentang seluk beluk jaringan komputer.

Buku Jaringan Sistem Komputer Jilid 2 ini mempelajari tentang dasar-dasar pemrograman sistem teknologi protocol dalam komputer dan sistem keamanan jaringan. Setiap bagian dan bab-bab yang ada dalam buku Jilid 2 ini disusun secara jelas dan sistematis untuk memudahkan dalam memahami buku ini. Penulis menyadari masih banyak kekurangan dalam buku ini, sehingga masukan dan saran sangat diharapkan untuk menyempurnakan buku ini.

Semarang, 1 Januari 2022
Penulis

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

DAFTAR ISI

Kata Pengantar ..... **v**
Daftar Isi ..... **vi**

BAGIAN IV Internetworking Menggunakan Arsitektur Internet TCP/IP, Pengalamatan, Pengikatan, Enkapsulasi, dan Protokol dalam Rangkaian TCP/IP

Bab 1 Internetworking: KonsepArsitektur, dan Protokol **2**
1.1 Tujuan Internetworking 2
1.2 Konsep Pelayanan Universal 3
1.3 Internetworking 4
1.4 Koneksi Jaringan Fisik dengan Router 5
1.5 Arsitektur Internet 6
1.6 Mencapai Layanan Universal 6
1.7 Jaringan Virtual 7
1.8 Protokol untuk Internetworking 8
1.9 Tinjauan Pelapisan TCP/IP 9
1.10 Komputer Host, Router, dan Lapisan ProtokoL 10
1.11 Ringkasan 10

Bab 2 Internet Protocol Address: Pengalamatan Internet **12**
2.1 Alamat untuk Internet Virtual 12
2.2 Skema Pengalamatan IP 13
2.3 Hirarki Alamat IP 14
2.4 Jenis Kelas Alamat IP 14
2.5 Notasi Desimal Bertitik 15
2.6 Pembagian Ruang Alamat 16
2.7 Pengalamatan Subnet dan Tanpa Kelas 16
2.8 Subnet Mask (Masker Subjaringan) 18
2.9 Notasi CIDR 19
2.10 Alamat Host CIDR 21
2.11 Alamat IP Khusus 21
2.12 Ringkasan Alamat IP Khusus 23
2.13 Formulir Alamat Berkeley Broadcast 23
2.14 Router dan Prinsip Pengalamatan IP 24
2.15 Skema Host sebagai Multi Host 25
2.16 Ringkasan 25

Bab 3 Penerusan Datagram **27**
3.1 Layanan Tanpa Koneksi 27
3.2 Paket Virtual 28

3.3 Datagram IP 28
3.4 Format Header Datagram IP 29
3.5 Meneruskan Datagram IP 30
3.6 Ekstraksi Prefiks Jaringan dan Penerusan Datagram 31
3.7 Pencocokan Prefiks yang Panjang 32
3.8 Alamat Tujuan dan Alamat Next-Hop 32
3.9 Pelayanan Terbaik IP 33
3.10 Enkapsulasi IP 33
3.11 Transmisi Melalui Internet 34
3.12 MTU dan Fragmentasi Datagram 36
3.13 Perakitan Kembali Datagram dari Fragmen 37
3.14 Mengumpulkan Fragmen Datagram 38
3.16 Memotong Fragmen 38
3.17 Ringkasan 39

Bab 4 Protokol dan Teknologi Pendukung 40
4.1 Address Resolution 40
4.2 Address Resolution Protocol (ARP) 42
4.3 Format Pesan ARP 43
4.4 Enkapsulasi ARP 45
4.5 ARP Caching dan Pemrosesan Pesan 45
4.6 Batas Alamat Konseptual 47
4.7 Internet Control Message Protocol (ICMP) 48
4.8 Format Pesan dan Enkapsulasi ICMP 49
4.9 Perangkat Lunak Protokol, Parameter, dan Konfigurasi 49
4.10 Dynamic Host Configuration Protocol (DHCP) 50
4.11 Operasi dan Optimalisasi Protokol DHCP 51
4.12 Format Pesan DHCP 52
4.13 Akses Server DHCP Tidak Langsung Melalui Relay 53
4.14 Network Address Translation (NAT) 53
4.15 Operasi NAT dan Alamat Pribadi 54
4.16 Transport-Layer NAT (NAPT) 55
4.17 NAT dan Server 56
4.18 Perangkat Lunak dan Sistem NAT untuk Penggunaan Rumahan 57
4.19 Ringkasan 57

Bab 5 IP Masa Depan (IPv6) 60
5.1 Keberhasilan IP 60
5.2 Motivasi untuk Perubahan 61
5.3 Model Jam Pasir dan Kendala Perubahan 61
5.4 Nama dan Nomor Versi 62
5.5 Fitur IPv6 62
5.6 Format Datagram IPv6 63
5.7 Format Header Basis IPv6 64
5.8 Ukuran Header Implisit dan Eksplisit 65
5.9 Fragmentasi, Perakitan Ulang, Dan Jalur MTU 65
5.10 Tujuan Beberapa Header 66
5.11 Pengalamatan IPv6 67

5.12 Notasi Heksadesimal Kolon IPv6 68
5.13 Ringkasan 69

Bab 6 UDP: Layanan Transportasi Datagram 71
6.1 Protokol Transportasi dan Komunikasi End-To-End 71
6.2 Protokol Datagram Pengguna 72
6.3 Paradigma Tanpa Koneksi 72
6.4 Antarmuka Berorientasi Pesan 73
6.5 Semantik Komunikasi UDP 73
6.6 Mode Interaksi dan Pengiriman Siaran 74
6.7 Identifikasi Titik Akhir dengan Nomor Port Protokol 74
6.8 Format Datagram UDP 75
6.9 Checksum UDP dan Header Pseudo 75
6.10 Enkapsulasi UDP 76
6.11 Ringkasan 76

Bab 7 TCP: Layanan Transportasi yang Andal 78
7.1 Protokol Kontrol Transmisi 78
7.2 Layanan yang Diberikan TCP ke Aplikasi 79
7.3 Layanan End-To-End dan Koneksi Virtual 79
7.4 Teknik yang Digunakan Protokol Transportasi 80
7.5 Teknik Menghindari Kemacetan 84
7.6 Seni Desain Protokol 85
7.7 Teknik Yang Digunakan Dalam TCP Untuk Menangani Packet Loss 86
7.8 Transmisi Ulang Adaptif 87
7.9 Perbandingan Waktu Transmisi Ulang 87
7.10 Buffer, Kontrol Aliran, dan Windows 88
7.11 Model TCP: Three-Way Handshake 89
7.12 Kontrol Kemacetan TCP 91
7.13 Format Segmen TCP 92
7.14 Ringkasan q 93

Bab 8 Perutean Internet dan Protokol Perutean 95
8.1 Perutean Statis dan Dinamis 95
8.2 Perutean Statis dalam Host dan Rute Default 96
8.3 Perutean dan Router Dinamis 97
8.4 Perutean dalam Internet Global 98
8.5 Konsep Sistem Otonom 98
8.6 Dua Jenis Protokol Perutean Internet 99
8.7 Rute dan Lalu Lintas Data 101
8.8 Border Gateway Protocol (BGP) 102
8.9 Routing Information Protocol (RIP) 103
8.10 Format Paket RIP 104
8.11 Open Shortest Path First Protocol (OSPF) 105
8.12 Contoh Grafik OSPF 105
8.13 Area OSPF 106
8.14 Intermediate System - Intermediate System (IS-IS) 107
8.15 Perutean Multicast 107

8.16 Ringkasan 111

BAGIAN V Aspek Lain Jaringan Komputer Kinerja Jaringan, QoS, Keamanan, Manajemen, dan Teknologi Baru

Bab 9 Kinerja Jaringan (QoS dan DiffServ) 114
9.1 Ukuran Kinerja 114
9.2 Latensi atau Penundaan 115
9.3 Throughput, Kapasitas, dan Goodput 116
9.4 Memahami Throughput dan Delay 118
9.5 Jitter 118
9.6 Hubungan antara Delay dan Throughput 119
9.7 Mengukur Delay, Throughput, dan Jitter 121
9.8 Pengukuran Pasif, Paket Kecil, dan NetFlow 122
9.9 Quality Of Servic (QoS) 123
9.10 Butir Halus dan Butir Kasar QoS 123
9.11 Implementasi QoS 125
9.12 Teknologi QoS Internet 127
9.13 Ringkasan 128

Bab 10 Multimedia dan IP Telephony (VoIP) 131
10.1 Transmisi Data Real-Time dan Pengiriman Best-Effort 131
10.2 Pemutaran Tertunda dan Buffer Jitter 132
10.3 Protokol Transportasi Waktu Nyata (RTP) 132
10.4 RTP Enkapsulasi 133
10.5 IP Telepon 134
10.6 Pensinyalan dan Standar Pensinyalan VoIP 135
10.7 Komponen Sistem Telepon IP 136
10.8 Ringkasan Protokol dan Layering 139
10.9 H.323 Karakteristik 139
10.10 H.323 Pelapisan 140
10.11 Karakteristik dan Metode SIP 140
10.12 Contoh Sesi SIP 141
10.13 Pemetaan dan Perutean Nomor Telepon 142
10.14 Ringkasan 143

Bab 11` Keamanan Jaringan 145
11.1 Keamanan Jaringan 145
11.2 Kebijakan Keamanan 148
11.3 Tanggung Jawab dan Kontrol 149
11.4 Teknologi Keamanan 150
11.5 Hashing: Mekanisme Integritas dan Otentikasi 150
11.6 Kontrol Akses dan Kata Sandi 151
11.7 Enkripsi: Teknik Keamanan Mendasar 151
11.8 Enkripsi Kunci Pribadi 152
11.9 Enkripsi Kunci Publik 152
11.10 Otentikasi dengan Tanda Tangan Digital 153
11.11 Otoritas Utama dan Sertifikat Digital 154

11.12 Firewall 155
11.13 Implementasi Firewall dengan Filter Paket 157
11.14 Sistem Deteksi Intrusi 158
11.15 Pemindaian Konten dan Inspeksi Paket Dalam 159
11.16 Virtual Private Networks (VPN) 160
11.17 Penggunaan Teknologi VPN untuk Telecommuting 161
11.18 Enkripsi Paket Vs. Tunneling 162
11.19 Teknologi Keamanan 164
11.20 Ringkasan 165

Bab 12 Manajemen Jaringan (SNMP) 168
12.1 Mengelola Intranet 168
12.2 FCAPS: Model Standar Industri 169
12.3 Contoh Elemen Jaringan 170
12.4 Alat Manajemen Jaringan 170
12.5 Aplikasi Manajemen Jaringan 173
12.6 Protokol Manajemen Jaringan Sederhana 173
12.7 Paradigma Fetch-Store SNMP 174
12.8 SNMP MIB dan Nama Objek 175
12.9 Variasi Variabel MIB 175
12.10 Variabel MIB yang Sesuai dengan Array 175
12.11 Ringkasan 176

Bab 13 Tren Teknologi dan Penggunaan Jaringan 178
13.1 Kebutuhan Akan Layanan Internet yang Dapat Diskalakan 178
13.2 Penyimpanan Konten (Akamai) 179
13.3 Penyeimbang Beban Web 179
13.4 Virtualisasi Server 180
13.5 Komunikasi Peer-To-Peer 180
13.6 Pusat Data Terdistribusi dan Replikasi 180
13.7 Representasi Universal (XML) 180
13.8 Jejaring Sosial 181
13.9 Mobilitas dan Jaringan Nirkabel 181
13.10 Video Digital 181
13.11 Pengiriman Multicast 182
13.12 Akses dan Peralihan Berkecepatan Lebih Tinggi 182
13.13 Pengalihan Optik 182
13.14 Penggunaan Jaringan dalam Bisnis 183
13.15 Sensor Skala Besar dan Rumahan 183
13.16 Jaringan Ad Hoc 183
13.18 CPU Multi-Core Dan Prosesor Jaringan 183
13.18 IPv6 184
13.19 Ringkasan 184

Daftar Pustaka 186

BAGIAN IV
Internetworking Menggunakan Arsitektur Internet TCP/IP, Pengalamatan, Pengikatan, Enkapsulasi, dan Protokol dalam Rangkaian TCP/IP

Bab 1 Internetworking: Konsep, Arsitektur, dan Protokol

Bab ini akan membahas tentang:

- Manfaat dan konsep internetworking
- Teknologi internetworking yang dapat digunakan
- Komponen perangkat keras yang digunakan, menjelaskan arsitektur di mana komponen terhubung, dan membahas pentingnya konsep tersebut

1.1 Tujuan Internetworking.

Setiap teknologi jaringan dirancang agar sesuai dengan serangkaian batasan tertentu. Misalnya, teknologi LAN dirancang untuk menyediakan komunikasi berkecepatan tinggi melintasi jarak pendek, sedangkan teknologi WAN dirancang untuk menyediakan komunikasi di area yang luas. Akibatnya, tidak ada teknologi jaringan tunggal yang terbaik untuk semua kebutuhan.

Sebuah organisasi besar dengan kebutuhan jaringan yang beragam membutuhkan beberapa jaringan fisik. Lebih penting lagi, jika organisasi memilih jenis jaringan yang terbaik untuk setiap tugas, organisasi akan memiliki beberapa jenis jaringan. Misalnya, teknologi LAN seperti Ethernet mungkin merupakan solusi terbaik untuk menghubungkan komputer di situs tertentu, tetapi sirkuit data sewaan mungkin digunakan untuk menghubungkan situs di satu kota dengan situs di kota lain.

Internetworking adalah praktek menghubungkan jaringan komputer dengan jaringan lain melalui penggunaan gateway yang menyediakan metode umum dari routing informasi paket antara jaringan. Sistem yang dihasilkan dari jaringan interkoneksi disebut internetwork, atau hanya internet. Saat ini dengan perkembangan perangkat IT terutama dibidang Networking telah menjadikan kebutuhan akan infrastruktur sangat tinggi yang membuat para vendor berlomba untuk membuat solusi terintegrasi.

Internet dapat dimanfaatkan dalam segala bidang, untuk bidang pendidikan, pemerintah, perbankan, penyuluhan kepada masyarakat, kesehatan, dan masih banyak lagi. Untuk tulisan kali ini yang akan dibahas adalah manfaat internet untuk dunia bisnis.

Internet telah merevolusi cara dunia melakukan bisnis baik di tingkat lokal dan global. Dari cara mengumpulkan data untuk merekrut karyawan pada perusahaan, cara bisnis menggunakan Internet sangat banyak, sebagai manfaat dari Internet untuk komunitas bisnis. Orang telah menemukan berbagai manfaat internet untuk bisnisnya. Banyak perusahaan kecil dan besar telah memanfaatkan Internet demi menunjang bisnis mereka. Bahkan ada yang dinamakan bisnis Online dimana semata-mata menjadikan Internet sebagai bisnis utama.

Banyak perusahaan, terutama yang menerapkan perdagangan online, telah mengintegrasikan situs Web mereka dengan sistem back-office seperti database, paket akuntansi dan kontrol stok dan penelusuran pelanggan mereka. Hal ini dapat mengurangi biaya administrasi dan meningkatkan layanan pelanggan dengan memberikan informasi yang cepat dan mudah tentang kemajuan order kepada pelanggan.

Adanya Internet mendobrak batasan ruang dan waktu. Sebuah perusahaan di Indonesia memiliki kesempatan yang sama untuk mengakses pasar Amerika dibandingkan dengan perusahaan di Eropa, atau bahkan dengan perusahaan di Amerika. Perlu diingat, hal yang sebaliknya (perusahaan luar mengakses pasar Indonesia) dapat juga dilakukan dengan mudah.

Tujuan utama dari internetworking adalah interoperabilitas yang maksimun, yaitu memaksimalkan kemampuan program pada sistem komputer yang berbeda dan system jaringan yang berbeda untuk berkomunikasi secara handal dan efisien. Ini akan menunjang ketersediaaan informasi pada sistem komputer dan jaringan yang beragam, baik perangkat lunak, perangkat keras maupun model data dari informasi tersebut.

1.2 Konsep Pelayanan Universal

Hilangnya batasan ruang dan waktu dengan adanya Internet membuka peluang baru untuk melakukan pekerjaan dari jarak jauh. Istilah teleworker atau teleworking mulai muncul. Seorang pekerja dapat melakukan pekerjaannya dari rumah tanpa perlu pusing dengan masalah lalulintas. Kesemua hal di atas menunjukkan adanya peluang-peluang baru di dalam bisnis dengan adanya Internet.

Masalah utama dengan banyak jaringan harus jelas: komputer yang terhubung ke jaringan tertentu hanya dapat berkomunikasi dengan komputer lain yang terhubung ke jaringan yang sama. Masalahnya menjadi jelas pada tahun 1970-an ketika organisasi besar mulai memperoleh banyak jaringan. Setiap jaringan dalam organisasi membentuk sebuah kelompok. Dalam banyak instalasi awal, setiap komputer terhubung ke satu jaringan, dan karyawan harus memilih komputer yang sesuai untuk setiap tugas. Artinya, seorang karyawan diberi akses ke beberapa layar dan keyboard, dan karyawan tersebut terpaksa berpindah dari satu komputer ke komputer lain untuk mengirim pesan melalui jaringan yang sesuai.

Pengguna tidak puas atau produktif ketika mereka harus menggunakan komputer terpisah untuk setiap jaringan. Akibatnya, sebagian besar sistem komunikasi komputer modern memungkinkan komunikasi antara dua komputer yang analog dengan cara sistem telepon menyediakan komunikasi antara dua telepon. Dikenal sebagai layanan universal, konsep ini merupakan bagian mendasar dari jaringan. Dengan layanan universal, pengguna di komputer mana pun di organisasi mana pun dapat mengirim pesan atau data ke pengguna lain. Selanjutnya, pengguna tidak perlu mengubah

sistem komputer saat mengubah tugas — semua informasi tersedia untuk semua komputer. Hasilnya, pengguna lebih produktif.

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung. Informasi dan data bergerak melalui kabel-kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama sama menggunakan hardware/software yang terhubung dengan jaringan. Tiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node.

Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir di setiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi di dalam perusahaan tersebut. Internet yang mulai populer saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan komputer yang terhubung dan dapat saling berinteraks

Poin Penting

Sistem komunikasi yang menyediakan layanan universal memungkinkan komputer yang saling berhubungan dapat berkomunikasi

Layanan Universal di Dunia yang Heterogen

Apakah layanan universal berarti bahwa setiap orang perlu mengadopsi teknologi jaringan tunggal, atau mungkinkah memiliki layanan universal di beberapa jaringan yang menggunakan banyak teknologi? Ketidakcocokan membuat tidak mungkin untuk membentuk jaringan besar hanya dengan menghubungkan kabel antar jaringan. Selanjutnya, teknik ekstensi seperti bridging tidak dapat digunakan dengan teknologi jaringan yang heterogen karena setiap teknologi menggunakan format paket dan skema pengalamatannya sendiri. Dengan demikian, frame yang dibuat untuk satu teknologi jaringan tidak dapat ditransmisikan pada jaringan yang menggunakan teknologi yang berbeda.

Poin Penting

Meskipun layanan universal sangat diinginkan, ketidakcocokan antara perangkat keras jaringan, bingkai, dan alamat mencegah jaringan yang dijembatani untuk memasukkan teknologi sewenang-wenang.

1.3 Internetworking

Meskipun tidak kompatibel antara teknologi jaringan, peneliti telah merancang skema yang menyediakan layanan universal di antara jaringan heterogen. Disebut internetworking, skema ini menggunakan perangkat keras dan perangkat lunak. Sistem perangkat keras tambahan digunakan untuk menghubungkan satu set jaringan fisik. Perangkat lunak pada komputer yang terpasang kemudian menyediakan layanan universal. Sistem yang dihasilkan dari jaringan fisik yang terhubung dikenal sebagai internetwork atau internet. Jaringan yang besar sebenarnya merupakan kumpulan dari jaringan yang kecil. Yang akan kita bahas disini adalah cara kita menghubungkan jaringan-jaringan kecil menjadi jaringan yang besar. Menghubungkan jaringan satu dengan jaringa yang lain inilah yang biasanya disebut dengan internetworking.

Internetworking cukup umum. Secara khusus, internet tidak dibatasi ukurannya — ada internet yang berisi beberapa jaringan dan Internet global berisi puluhan ribu jaringan. Demikian pula, jumlah

komputer yang terhubung ke setiap jaringan di internet dapat bervariasi — beberapa jaringan tidak memiliki komputer yang terhubung, sementara yang lain memiliki ratusan.

Internetwork adalah subsistem komunikasi di mana beberapa jaringan terhubung bersama-sama untuk menyediakan fasilitas komunikasi data umum serta membungkus (menyembunyikan) teknologi dan protokol jaringan komponen individu dan metode yang digunakan untuk interkoneksi mereka.

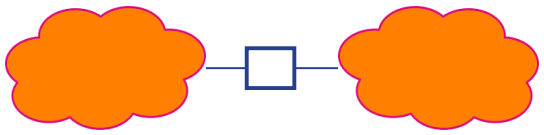
Berikut tipe-tipe jaringan secara umum :

	Range	*Bandwidth (Mbps)*	*Latency (ms)*
LAN	1-2 kms	10-1000	1-10
WAN	worldwide	0.010-600	100-500
MAN	2-50 kms	1-150	10
Wireless LAN	0.15-1.5 km	2-11	5-20
Wireless WAN	worldwide	0.010-2	100-500
Internet	worldwide	0.010-2	100-500

Jaringan perbandingan dari tabel di atas menunjukkan rentang dan karakteristik dari performance berbagai jenis jaringan yang telah kita bahas di atas. Titik tambahan perbandingan yang relevan bagi sistem terdistribusi adalah frekuensi dan jenis kegagalan yang dapat diharapkan pada berbagai jenis jaringan. Keandalan yang mendasarinya mekanisme transmisi data sangat tinggi di semua jenis kecuali jaringan nirkabel, di mana paket sering hilang karena gangguan eksternal. Dalam semua jenis paket jaringan mungkin hilang akibat keterlambatan pemrosesan atau buffer overflow di tempat tujuan. Ini jauh yang paling umum yang menyebabkan hilangnya paket.

1.4 Koneksi Jaringan Fisik dengan Router

Komponen perangkat keras dasar yang digunakan untuk menghubungkan jaringan heterogen adalah router. Secara fisik, router adalah sistem perangkat keras independen yang didedikasikan untuk tugas interkoneksi jaringan. Seperti jembatan, router berisi prosesor dan memori serta antarmuka I/O terpisah untuk setiap jaringan yang terhubung. Jaringan memperlakukan koneksi ke router sama seperti koneksi ke komputer lain. Gambar 20.1 mengilustrasikan bahwa koneksi fisik jaringan dengan router sangat mudah.



Gambar 20.1 Dua jaringan fisik yang dihubungkan oleh router, yang memiliki antarmuka terpisah untuk setiap koneksi jaringan. Komputer dapat terhubung ke setiap jaringan.

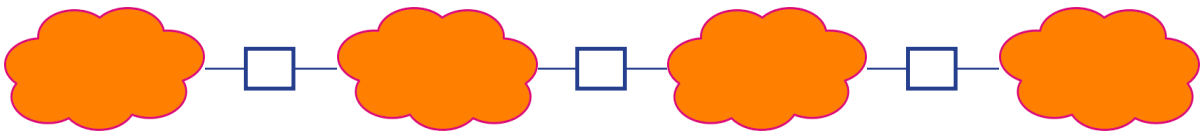
Gambar tersebut menggunakan awan untuk menggambarkan setiap jaringan karena koneksi router tidak terbatas pada teknologi jaringan tertentu. Router dapat menghubungkan dua LAN, LAN dan WAN, atau dua WAN. Selanjutnya, ketika router menghubungkan dua jaringan dalam kategori umum yang sama, jaringan tersebut tidak perlu menggunakan teknologi yang sama. Misalnya, router dapat menghubungkan Ethernet ke jaringan Wi-Fi. Dengan demikian, setiap cloud mewakili teknologi jaringan yang berubah-ubah.

Poin Penting

Router Internet adalah sistem perangkat keras tujuan khusus yang didedikasikan untuk tugas interkoneksi jaringan. Sebuah router dapat menghubungkan jaringan yang menggunakan teknologi yang berbeda, termasuk media yang berbeda, skema pengalamatan fisik, atau format frame.

1.5 Arsitektur Internet

Router memungkinkan organisasi untuk memilih teknologi jaringan yang sesuai untuk setiap kebutuhan dan menggunakan router untuk menghubungkan semua jaringan ke internet. Sebagai contoh, Gambar 20.2 mengilustrasikan bagaimana tiga router dapat digunakan untuk menghubungkan empat jaringan fisik arbitrer ke dalam internet.



Gambar 20.2 Internet dibentuk dengan menggunakan tiga router untuk menghubungkan empat jaringan fisik.

Meskipun gambar menunjukkan setiap router dengan tepat dua koneksi, router komersial dapat menghubungkan lebih dari dua jaringan. Jadi, satu router dapat menghubungkan keempat jaringan dalam contoh. Terlepas dari kelayakannya, sebuah organisasi jarang menggunakan satu router untuk menghubungkan semua jaringannya. Ada dua alasan:

- Karena router harus meneruskan setiap paket, prosesor di router yang diberikan tidak cukup untuk menangani lalu lintas yang lewat di antara sejumlah jaringan yang berubah-ubah.
- Redundansi meningkatkan keandalan internet. Untuk menghindari satu titik kegagalan, perangkat lunak protokol terus memantau koneksi internet dan menginstruksikan router untuk mengirim lalu lintas di sepanjang jalur alternatif ketika jaringan atau router gagal.

Jadi, ketika merencanakan internet, organisasi harus memilih desain yang memenuhi kebutuhan organisasi akan keandalan, kapasitas, dan biaya. Secara khusus, detail yang tepat dari topologi internet seringkali bergantung pada bandwidth jaringan fisik, lalu lintas yang diharapkan, persyaratan keandalan organisasi, dan biaya serta kinerja perangkat keras router yang tersedia.

Poin Penting

Internet terdiri dari sekumpulan jaringan yang saling terhubung oleh router. Skema internet memungkinkan setiap organisasi untuk memilih jumlah dan jenis jaringan, jumlah router yang akan digunakan untuk menghubungkannya, dan topologi interkoneksi yang tepat.

1.6 Mencapai Layanan Universal

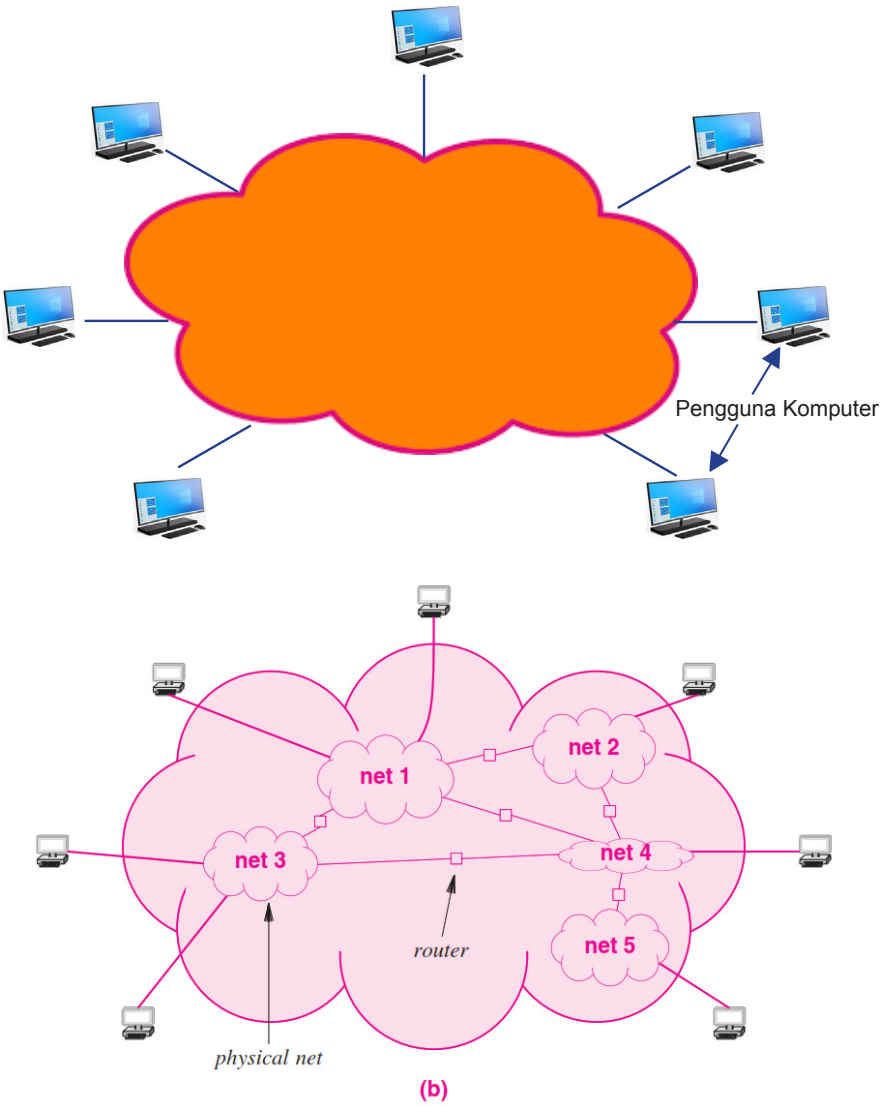
Tujuan dari internetworking adalah layanan universal di seluruh jaringan heterogen. Untuk menyediakan layanan universal di antara semua komputer di internet, router harus setuju untuk meneruskan informasi dari sumber di satu jaringan ke tujuan tertentu di jaringan lain. Tugasnya rumit karena format bingkai dan skema pengalamatan yang digunakan oleh jaringan yang mendasarinya bisa

berbeda. Akibatnya, perangkat lunak protokol diperlukan pada komputer dan router untuk memungkinkan layanan universal.

1.7 Jaringan Virtual

Secara umum, perangkat lunak Internet memberikan tampilan sistem komunikasi tunggal yang mulus yang dilampirkan oleh banyak komputer. Sistem menawarkan layanan universal: setiap komputer diberi alamat, dan komputer mana pun dapat mengirim paket ke komputer lain. Selain itu, perangkat lunak protokol Internet menyembunyikan detail koneksi jaringan fisik, alamat fisik, dan informasi perutean — baik pengguna maupun program aplikasi tidak mengetahui jaringan fisik yang mendasarinya atau router yang menghubungkannya.

Kami mengatakan bahwa internet adalah sistem jaringan virtual karena sistem komunikasi adalah abstraksi. Artinya, meskipun kombinasi perangkat keras dan perangkat lunak memberikan ilusi sistem jaringan yang seragam, tidak ada jaringan seperti itu. Gambar 20.3 mengilustrasikan konsep jaringan virtual serta struktur fisik yang sesuai.



Gambar 20.3 Konsep Internet. (a) Ilusi jaringan tunggal yang disediakan untuk pengguna dan aplikasi, dan (b) struktur fisik yang mendasari dengan router yang menghubungkan jaringan.

1.8 Protokol untuk Internetworking

TCP/IP adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (protocol suite). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (software) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP stack.

Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (IP Address) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini juga bersifat routable yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga UNIX) untuk membentuk jaringan yang heterogen.

Keunggulan TCP/IP adalah sebagai berikut:

- Open Protocol Standard, yaitu tersedia secara bebas dan dikembangkan independen terhadap komputer hardware ataupun sistem operasi apapun. Karena didukung secara meluas, TCP/IP sangat ideal untuk menyatukan bermacam hardware dan software, walaupun tidak berkomunikasi lewat internet.
- Independen dari physical network hardware. Ini menyebabkan TCP/IP dapat mengintegrasikan bermacam network, baik melalui ethernet, token ring, dial-up, X.25/AX.25 dan media transmisi fisik lainnya.
- Skema pengalamatan yang umum menyebabkan device yang menggunakan TCP/IP dapat menghubungi alamat device-device lain di seluruh network, bahkan Internet sekalipun.
- High level protocol standar, yang dapat melayani user secara luas

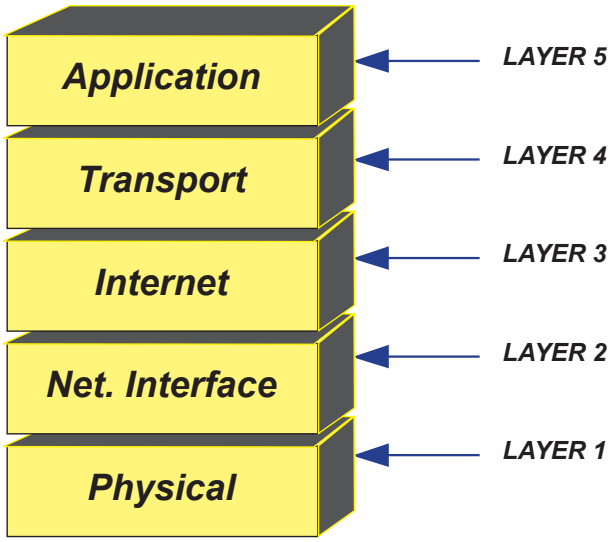
Cara Kerja TCP/IP

- Untuk memindahkan data antara dua komputer yang berbeda dalam suatu jaringan yang terdiri dari banyak komputer, dibutuhkan alamat tujuan dan perantara untuk memindahkan sinyal elektronik pembentuk data secara aman dan langsung.
- Internet menggunakan protokol untuk menjamin sampainya data secara aman di tempat tujuan.
- Saat seorang pengguna Internet mengirim sekelompok teks ke mesin lain, TCP/IP mulai bekerja. TCP membagi teks tersebut menjadi paket-paket data kecil, menambahkan beberapa informasi (dapat dianggap sebagai pengiriman barang), sehingga komputer penerima memastikan bahwa paket yang diterimanya tidak mengalami kerusakan sepanjang pengiriman. IP menambahkan label yang berisikan informasi alamat pada paket tersebut.
- Deretan paket-paket TCP/IP berjalan menuju tujuan yang sama dengan menggunakan berbagai jalur yang berbeda. Sebuah perangkat khusus yang disebut router dipasang di titik persimpangan antar jaringan dan memutuskan jalur mana yang paling efisien yang menjadi langkah berikut dari sebuah paket. Router membantu mengatur arus lalu lintas di Internet dengan membagi beban, sehingga menghindari kelebihan beban pada suatu bagian dari sistem yang ada.

- Saat paket-paket TCP/IP tiba di tempat tujuannya, komputer akan membuka label alamat IP lalu menggunakan daftar pengiriman yang ada pada paket TCP untuk memeriksa apakah ada kerusakan paket yang terjadi selama pengiriman, dan menyusun kembali paket-paket tsb menjadi susunan teks seperti aslinya. Saat komputer penerima menemukan paket yang rusak, komputer tsb akan meminta komputer pengirim untuk mengirim salinan baru dari paket yang rusak.
- Sebuah perangkat khusus yang disebut gateway memungkinkan beragam tipe jaringan yang ada di horison elektronik untuk berkomunikasi dengan Internet menggunakan TCP/IP. Gateway menerjemahkan protokol asli jaringan komputer tersebut menjadi TCP/IP dan sebaliknya.
- Bagi seorang pemakai, Internet hadir seperti jaringan global raksasa yang tidak terbatas, yang langsung merespon jika diminta. Komputer, gateway, router, dan protokol yang membuat ilusi ini bekerja.

1.9 Tinjauan Pelapisan TCP/IP

Protokol Internet menggunakan model referensi lima lapis seperti yang diilustrasikan Gambar 20.4.



Gambar 20.4 Lima lapisan model referensi TCP/IP.

Kami telah menjelajahi tiga lapisan dalam Buku Jilid 1. Bab di bagian 1 dari teks mempertimbangkan aplikasi; bab di bagian 2 dan 3 dari teks membahas protokol lapisan 1 dan lapisan 2. Bab-bab di bagian teks ini mempertimbangkan dua lapisan yang tersisa secara rinci:

Lapisan 3: Internet

Layer 3 (IP) menentukan format paket yang dikirim melalui Internet serta mekanisme yang digunakan untuk meneruskan paket dari komputer melalui satu atau lebih router ke tujuan akhir. Internet Protocol adalah jantung dari TCP/IP dan protokol paling penting pada Internet Layer (RFC 791). IP menyediakan layanan pengiriman paket dasar pada jaringan tempat TCP/IP network dibangun. Seluruh protokol, diatas dan dibawah Internet layer, menggunakan Internet Protokol untuk mengirimkan data. Semua data TCP/IP mengalir melalui IP, baik incoming maupun outgoing, dengan mengabaikan tujuan terakhirnya.

Lapisan 4: Transportasi

Layer 4 (TCP) menentukan pesan dan prosedur yang digunakan untuk memastikan transfer yang andal. Dua protokol utama pada layer ini adalah Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP). TCP menyediakan layanan pengiriman data handal dengan end-to-end deteksi dan koreksi kesalahan. UDP menyediakan layanan pengiriman datagram tanpa koneksi (connectionless) dan low-overhead. Kedua protokol ini mengirmkan data diantara Application Layer dan Internet Layer. Programmer untuk aplikasi dapat memilih layanan mana yang lebih dibutuhkan untuk aplikasi mereka.

Poin Penting

Protokol internet diatur ke dalam lima lapisan konseptual, dengan IP pada lapisan 3 dan TCP pada lapisan 4.

1.10 Komputer Host, Router, dan Lapisan Protokol

Kami menggunakan istilah komputer host untuk merujuk ke komputer yang terhubung ke Internet dan menjalankan aplikasi. Sebuah host bisa sekecil ponsel atau sebesar mainframe. Lebih jauh lagi, CPU host bisa lambat atau cepat, memori bisa besar atau kecil, dan jaringan yang terhubung dengan host dapat beroperasi pada kecepatan tinggi atau rendah. Protokol TCP/IP memungkinkan setiap pasangan host untuk berkomunikasi, meskipun ada perbedaan perangkat keras.

Baik host dan router memerlukan perangkat lunak protokol TCP/IP. Namun, router tidak menggunakan protokol dari semua lapisan. Secara khusus, router tidak memerlukan protokol layer 5 untuk aplikasi seperti transfer file karena router tidak menjalankan aplikasi konvensional. Bab-bab berikutnya membahas perangkat lunak protokol TCP/IP secara lebih rinci, dan menunjukkan cara kerja Internet layering.

1.11 Ringkasan

Logikanya, Internet tampaknya merupakan sistem komunikasi tunggal yang mulus. Sepasang komputer yang terhubung ke Internet dapat berkomunikasi seolah-olah mereka terhubung ke satu jaringan. Artinya, komputer dapat mengirim paket ke komputer lain yang terhubung ke Internet. Secara fisik, Internet adalah kumpulan jaringan yang saling terhubung oleh perangkat yang disebut router. Setiap router adalah perangkat tujuan khusus yang terhubung ke dua atau lebih jaringan dan didedikasikan untuk mentransfer paket Internet di antara jaringan.

Komputer yang terhubung ke Internet disebut host. Sebuah host mungkin komputer besar (misalnya, superkomputer) atau komputer kecil (misalnya, ponsel). Setiap host terhubung ke salah satu jaringan fisik di Internet.

Ilusi sistem komunikasi tunggal disediakan oleh perangkat lunak protokol Internet. Setiap host atau router di Internet harus menjalankan perangkat lunak, yang menyembunyikan detail koneksi fisik yang mendasarinya dan menangani pengiriman setiap paket ke tujuannya.

Protokol paling penting yang dikembangkan untuk internetworking dikenal sebagai Protokol Internet TCP/IP, biasanya disingkat TCP/IP. Selain digunakan di internet pribadi, TCP/IP telah digunakan di Internet global selama bertahun-tahun.

Latihan

1. Apakah Internet akan digantikan oleh teknologi jaringan tunggal? Mengapa atau mengapa tidak?
2. Apa kendala utama dalam menyediakan layanan universal?
3. Sebutkan dua alasan organisasi tidak menggunakan satu router untuk menghubungkan semua jaringannya?
4. Jika router tertentu dapat terhubung ke paling banyak jaringan K, berapa banyak router, R, yang diperlukan untuk menghubungkan jaringan N? Tulis persamaan yang memberikan R dalam bentuk N dan K.
5. Pengguna melihat Internet sebagai jaringan tunggal. Apa kenyataannya, dan apa yang dilampirkan komputer pengguna?
6. Dalam model referensi 5 lapis yang digunakan dengan protokol Internet TCP/IP, apa tujuan dari masing-masing dari lima lapisan?

Bab 2 Internet Protocol Address: Pengalamatan Internet

Bab ini akan membahas tentang:

- Deskripsi perangkat lunak protokol
- Skema pengalamatan yang digunakan oleh Internet Protocol (IPv4)
- Penggunaan masker alamat untuk pengalamatan tanpa kelas dan subnet

2.1 Alamat untuk Internet Virtual

Ingat dari Bab 1 dalam Buku Jilid 2 ini, bahwa tujuan *internetworking* adalah untuk menyediakan sistem komunikasi yang mulus. Untuk mencapai tujuan, perangkat lunak protokol harus menyembunyikan detail jaringan fisik dan menawarkan ilusi jaringan tunggal yang besar. Dari sudut pandang aplikasi, Internet virtual beroperasi seperti jaringan apa pun, memungkinkan komputer untuk mengirim dan menerima paket. Perbedaan utama antara Internet dan jaringan fisik adalah bahwa Internet adalah abstraksi yang dibayangkan oleh perancangnya dan dibuat seluruhnya oleh perangkat lunak protokol. Dengan demikian, perancang memilih alamat, format paket, dan teknik pengiriman yang tidak bergantung pada detail perangkat keras yang mendasarinya.

Pengalamatan (*addressing*) adalah komponen penting dari abstraksi Internet. Untuk memberikan tampilan jaringan tunggal, semua komputer host harus menggunakan skema pengalamatan yang seragam, dan setiap alamat harus unik. Meskipun setiap komputer memiliki alamat MAC, alamat tersebut tidak cukup karena Internet dapat mencakup beberapa teknologi jaringan dan setiap teknologi mendefinisikan alamat MAC-nya sendiri.

Untuk menjamin pengalamatan yang seragam, IP mendefinisikan skema pengalamatan yang independen dari alamat MAC yang mendasarinya. Alamat IP digunakan sebagai tujuan di Internet analog dengan cara alamat MAC digunakan sebagai tujuan di LAN. Untuk mengirim paket melalui Internet, pengirim menempatkan alamat IP tujuan dalam paket, dan meneruskan paket ke perangkat

lunak protokol IP untuk diteruskan. Perangkat lunak protokol IP menggunakan alamat IP tujuan saat meneruskan paket melalui Internet ke komputer tujuan.

Keuntungan dari pengalamatan IP terletak pada keseragaman: sepasang program aplikasi yang diprogram secara acak dapat berkomunikasi tanpa mengetahui jenis perangkat keras jaringan atau alamat MAC yang digunakan. Ilusi ini begitu lengkap sehingga beberapa pengguna terkejut mengetahui bahwa alamat IP disediakan oleh perangkat lunak protokol dan bukan bagian dari jaringan yang mendasarinya. Menariknya, kita akan mempelajari bahwa banyak lapisan perangkat lunak protokol menggunakan alamat IP.

Poin Penting

Untuk memberikan pengalamatan yang seragam di Internet, IP mendefinisikan skema pengalamatan abstrak yang memberikan setiap host alamat protokol yang unik; aplikasi menggunakan alamat IP untuk berkomunikasi.

2.2 Skema Pengalamatan IP

Standar IP menetapkan bahwa setiap host diberi nomor 32-bit unik yang dikenal sebagai alamat Protokol Internet host, alamat IP, atau alamat Internet. Saat mengirim paket melalui Internet, pengirim harus menentukan alamat IP 32-bitnya sendiri (alamat sumber) serta alamat penerima yang dituju (alamat tujuan). Pengalamatan IP adalah pengidentifikasian dengan angka yang diberikan setiap mesin di dalam jaringan IP. Pengalamatan IP digunakan untuk menunjukkan lokasi spesifik dari alat di dalam jaringan. Alamat IP adalah alamat software, bukan alamat hardware yang terpatri ke dalam Network Interface Card (NIC) dan digunakan untuk menemukan host pada jaringan lokal. Pengalamatan IP ditujukan untuk memungkinkan host di dalam sebuah jaringan bisa berkomunikasi dengan host pada jaringan yang berbeda, tanpa mempedulikan tipe dari LAN yang digunakan oleh host yang berpartisipasi.

Untuk mempelajari pengertian tentang internet protocol, berikut ini ada beberapa istilah yaitu:

- Bit, satu bit sama dengan satu digit yang bernilai 1 atau 0.
- Byte, satu byte sama dengan 7 atau 8 bit yanng bergantung apakah menggunakan parity. 3.
- Octet, terdiri atas 8 bit yang merupakan bilangan biner 8 bit umumnya.
- Alamat Network, digunakan dalam routing untuk menunjukkan pengiriman paket ke remote network.
- Alamat broadcast, di digunakan oleh aplikasi dan host untuk mengirim informasi ke semua titik di dalam jaringan.

Poin Penting

Alamat Internet (alamat IP) adalah nomor biner 32-bit unik yang ditetapkan ke host dan digunakan untuk semua komunikasi dengan host.

2.3 Hirarki Alamat IP

Analog dengan pengalamatan hierarkis yang digunakan dengan WAN, setiap alamat IP 32-bit dibagi menjadi dua bagian: prefiks dan sufiks. Prefiks IP tidak hanya mengidentifikasi switch paket tapi justru mengidentifikasi jaringan fisik tempat host terpasang. Sufiks IP mengidentifikasi komputer tertentu di jaringan. Artinya, setiap jaringan fisik di Internet diberi nomor jaringan yang unik. Nomor jaringan muncul sebagai awalan di alamat IP setiap komputer yang terhubung ke jaringan, dan setiap komputer di jaringan fisik tertentu diberi akhiran unik.

Untuk menjamin keunikan, tidak ada dua jaringan di Internet yang dapat diberi nomor jaringan yang sama dan tidak ada dua komputer di jaringan tertentu yang dapat diberi akhiran (sufiks) yang sama. Misalnya, jika internet berisi tiga jaringan, mereka mungkin diberi nomor jaringan 1, 2, dan 3. Tiga komputer yang terhubung ke jaringan 1 dapat diberi sufiks 1, 3, dan 5, sedangkan tiga komputer yang terhubung ke jaringan 2 dapat diberi sufiks 1, 2, dan 3. Nilai yang ditetapkan tidak perlu bersebelahan.

Poin penting adalah bahwa skema alamat IP menjamin dua properti:

- Setiap komputer diberi alamat unik (yaitu, satu alamat tidak pernah diberikan ke lebih dari satu komputer).
- Meskipun penetapan nomor jaringan harus dikoordinasikan secara global, sufiks dapat ditetapkan secara lokal tanpa koordinasi global.

Properti pertama dijamin karena alamat IP berisi awalan dan akhiran. Jika dua komputer terhubung ke jaringan fisik yang berbeda, prefiks yang diberikan ke alamat mereka akan berbeda. Jika dua komputer terhubung ke jaringan fisik yang sama, alamat mereka memiliki akhiran yang berbeda. Dengan demikian, alamat yang diberikan ke komputer adalah unik.

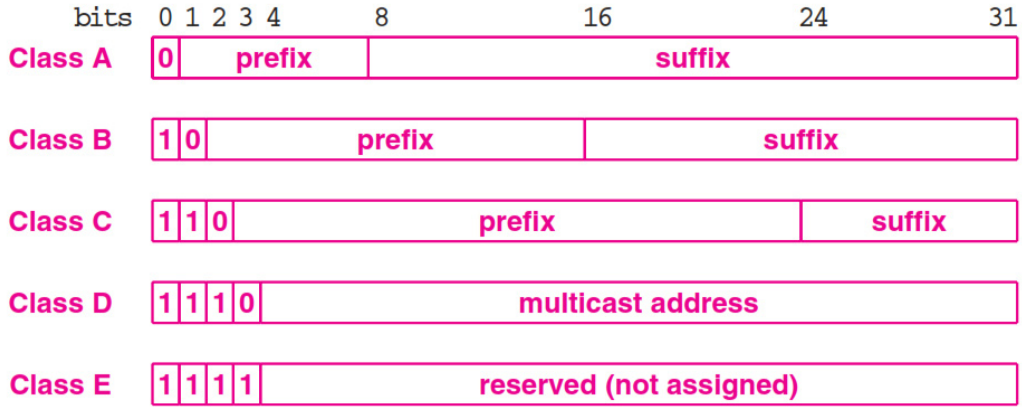
2.4 Jenis Kelas Alamat IP

Setelah mereka memilih ukuran untuk alamat IP dan memutuskan untuk membagi setiap alamat menjadi dua bagian, perancang IP harus menentukan berapa banyak bit yang akan ditempatkan di setiap bagian. Prefiks membutuhkan bit yang cukup untuk memungkinkan nomor jaringan unik ditetapkan ke setiap jaringan fisik di Internet. Sufiks membutuhkan bit yang cukup untuk mengizinkan setiap komputer yang terhubung ke jaringan untuk diberi sufiks unik. Tidak ada pilihan sederhana yang mungkin karena menambahkan bit ke satu bagian berarti mengurangi bit dari yang lain. Memilih awalan yang besar mengakomodasi banyak jaringan, tetapi membatasi ukuran setiap jaringan; memilih akhiran besar berarti setiap jaringan fisik dapat berisi banyak komputer, tetapi membatasi jumlah jaringan.

Karena Internet mencakup teknologi jaringan arbitrer, ia berisi beberapa jaringan fisik besar dan banyak jaringan kecil. Akibatnya, perancang memilih skema pengalamatan untuk mengakomodasi kombinasi jaringan besar dan kecil. Skema asli, yang dikenal sebagai pengalamatan IP *classful*, membagi ruang alamat IP menjadi tiga kelas utama, di mana setiap kelas memiliki ukuran awalan dan akhiran yang berbeda.

Empat bit pertama dari sebuah alamat menentukan kelas tempat alamat itu berada, dan menentukan bagaimana sisa alamat dibagi menjadi awalan dan akhiran. Gambar 2.1 mengilustrasikan lima kelas alamat, bit utama yang digunakan untuk mengidentifikasi setiap kelas, dan pembagian

menjadi awalan dan akhiran. Gambar mengikuti konvensi yang digunakan dalam protokol TCP/IP penomoran bit dari kiri ke kanan dan menggunakan nol untuk bit pertama.



Gambar 2.1 Lima kelas alamat IP dalam skema classful asli.

Meskipun skema *classful* telah digantikan, alamat kelas D masih digunakan untuk multicasting, yang memungkinkan pengiriman ke satu set komputer. Setiap alamat multicast sesuai dengan sekelompok komputer. Setelah grup multicast dibuat, salinan paket apa pun yang dikirim ke alamat multicast akan dikirimkan ke setiap host dalam grup. Dalam prakteknya, multicasting Internet tidak pernah tersedia secara global, yang berarti bahwa multicasting dibatasi untuk situs individu.

Poin Penting

Skema pengalamatan IP asli membagi alamat ke dalam kelas-kelas. Alamat kelas D masih digunakan untuk multicasting, tetapi multicasting tidak bekerja secara global.

2.5 Notasi Desimal Bertitik

Meskipun alamat IP adalah angka 32-bit, pengguna tidak memasukkan atau membaca nilai dalam biner. Sebaliknya, ketika berinteraksi dengan pengguna, perangkat lunak menggunakan notasi yang lebih mudah dipahami manusia. Disebut Notasi Desimal Bertitik (*Dotted Decimal Notation*), formulir tersebut menyatakan setiap bagian 8-bit dari angka 32-bit sebagai nilai desimal dan menggunakan titik untuk memisahkan bagian-bagian tersebut. Gambar 2.2 mengilustrasikan contoh bilangan biner dan notasi desimal bertitik yang setara. Detik. 1.6 Notasi Desimal Bertitik

32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129.52.6.0
11000000 00000101 00110000 00000011	192.5.48.3
00001010 00000010 00000000 00100101	10.2.0.37
10000000 00001010 00000010 00000011	128.10.2.3
10000000 10000000 11111111 00000000	128.128.255.0

Gambar 2.2 Contoh bilangan biner 32-bit dan ekuivalennya dalam notasi desimal bertitik.

Desimal Bertitik memperlakukan setiap oktet (setiap nilai 8-bit) sebagai bilangan bulat biner tak bertanda†. Sebagai contoh terakhir pada gambar menunjukkan, nilai terkecil yang mungkin, 0, terjadi ketika semua bit dari sebuah oktet adalah nol, dan nilai terbesar yang mungkin, 255, terjadi ketika semua bit dari sebuah oktet adalah satu. Jadi, alamat desimal bertitik berkisar dari 0.0.0.0 hingga 255.255.255.255. Alamat multicast, kelas D, menempati rentang dari 224.0.0.0 hingga 239.255.255.255.

Poin Penting

Notasi Desimal Bertitik adalah bentuk sintaksis yang digunakan perangkat lunak IP untuk mengekspresikan nilai biner 32-bit saat berinteraksi dengan manusia. Desimal bertitik mewakili setiap oktet dalam desimal dan menggunakan titik untuk memisahkan oktet.

2.6 Pembagian Ruang Alamat

Skema classful asli, yang dirancang sebelum PC ditemukan, sebelum LAN tersedia secara luas, dan sebelum sebagian besar perusahaan memiliki jaringan komputer, membagi ruang alamat menjadi ukuran yang tidak sama. Para desainer memilih divisi yang tidak seimbang untuk mengakomodasi berbagai skenario. Misalnya, meskipun terbatas pada 128 jaringan, kelas A berisi setengah dari semua alamat. Motivasinya adalah untuk memungkinkan ISP utama masing-masing menyebarkan jaringan besar yang menghubungkan jutaan komputer. Demikian pula, motivasi untuk kelas C adalah untuk memungkinkan sebuah organisasi untuk memiliki beberapa komputer yang terhubung pada LAN. Gambar 2.3 merangkum jumlah maksimum jaringan yang tersedia di setiap kelas dan jumlah maksimum host per jaringan.

Gambar 2.3 Jumlah jaringan dan host per jaringan di masing-masing dari tiga kelas alamat IP primer.

Kelas Alamat	Bit Dalam Awalan	Jumlah Jaringan Maksimum	Bit Dalam Sufiks	Jumlah Maksimum Host Per Jaringan
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

Setiap awalan yang ditetapkan ke jaringan individu di Internet harus unik. Oleh karena itu, sebuah organisasi pusat, *Internet Corporation for Assigned Names and Numbers* (ICANN), telah dibentuk untuk menangani penugasan alamat dan mengadili perselisihan. ICANN tidak menetapkan awalan individu. Sebagai gantinya, ICANN mengizinkan sekumpulan registrar untuk melakukannya. Pendaftar membuat blok alamat tersedia untuk ISP, yang memberikan alamat kepada pelanggan. Jadi, untuk mendapatkan awalan, perusahaan biasanya menghubungi ISP.

2.7 Pengalamatan Subnet dan Tanpa Kelas

Sebagai Internet tumbuh, skema pengalamatan classful asli menjadi batasan. Setiap orang menuntut alamat kelas A atau B sehingga mereka memiliki alamat yang cukup untuk pertumbuhan di masa depan; banyak alamat yang tidak digunakan. Meskipun banyak alamat kelas C yang tersisa, beberapa grup menginginkannya.

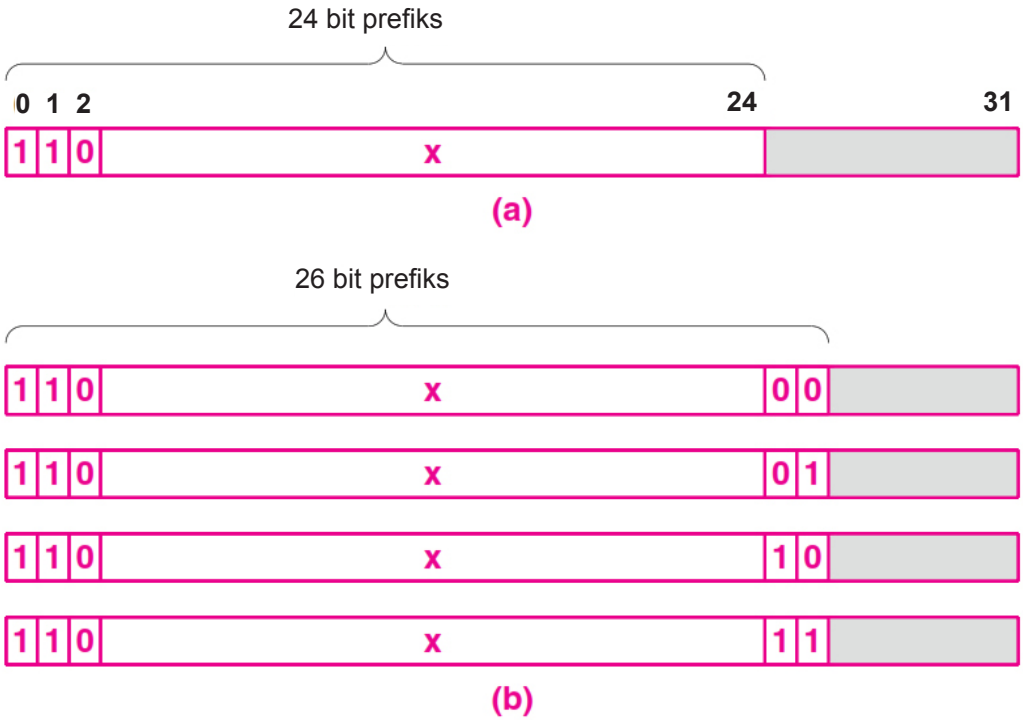
Dua mekanisme baru diciptakan untuk mengatasi keterbatasan:

- Pengalamatan subnet
- Pengalamatan tanpa kelas

Kedua mekanisme tersebut sangat erat hubungannya sehingga dapat dianggap sebagai bagian dari abstraksi tunggal: alih-alih memiliki tiga kelas alamat yang berbeda, memungkinkan pembagian antara awalan dan akhiran terjadi pada batas bit yang berubah-ubah. Pengalamatan subnet awalnya digunakan dalam organisasi besar yang terhubung ke Internet global, dan pengalamatan tanpa kelas memperluas pendekatan ke seluruh Internet.

Untuk memahami motivasi menggunakan batasan sembarang, pertimbangkan ISP yang membagikan awalan. Misalkan pelanggan ISP meminta awalan untuk jaringan yang berisi tiga puluh lima host. Ketika pengalamatan classful digunakan, ISP akan menetapkan awalan kelas C. Faktanya, hanya empat bit akhiran host yang diperlukan untuk mewakili semua nilai host yang mungkin, yang berarti bahwa 219 dari 254 akhiran yang mungkin tidak akan pernah ditetapkan ke host†. Dengan kata lain, sebagian besar ruang alamat kelas C terbuang percuma. Pengalamatan tanpa kelas memberikan solusi yang lebih baik dengan mengizinkan ISP untuk menetapkan awalan yang panjangnya dua puluh enam bit. Jadi, sufiksnya panjangnya enam bit, artinya hanya dua puluh tujuh alamat yang tidak akan digunakan.

Cara lain untuk melihat situasi ini adalah dengan menganggap ISP memiliki awalan kelas C. Pengalamatan classful menetapkan seluruh awalan ke satu organisasi. Namun, dengan pengalamatan tanpa kelas, ISP dapat membagi prefiks menjadi beberapa prefiks yang lebih panjang, dan menetapkan masing-masing ke pelanggan. Gambar 2.4 mengilustrasikan bagaimana pengalamatan tanpa kelas memungkinkan ISP untuk membagi prefiks kelas C menjadi empat prefiks yang lebih panjang yang masing-masing mengakomodasi jaringan hingga enam puluh dua host.



Gambar 2.4 (a) Awalan kelas C, dan (b) awalan yang sama dibagi menjadi empat awalan tanpa kelas.

Pada gambar, bagian host dari setiap awalan ditampilkan dalam warna abu-abu. Alamat kelas C asli memiliki delapan bit akhiran, dan masing-masing alamat tanpa kelas memiliki enam bit akhiran. Dengan asumsi bahwa awalan kelas C asli adalah unik, setiap awalan tanpa kelas juga akan unik. Jadi, alih-alih membuang alamat, ISP dapat menetapkan masing-masing dari empat prefiks tanpa kelas ke pelanggan.

2.8 Subnet Mask (Masker Subjaringan)

Bagaimana alamat IP dapat dibagi pada batas yang acak ? Skema pengalamatan tanpa kelas dan subnet memerlukan host dan router yang memproses alamat untuk menyimpan informasi tambahan: nilai yang menentukan batas yang tepat antara awalan jaringan dan akhiran host. Untuk menandai batas, IP menggunakan nilai 32-bit yang dikenal sebagai *address mask*, yang pada awalnya disebut subnet mask. Sebuah *address mask* memiliki satu bit untuk menandai awalan jaringan dan nol bit untuk menandai bagian host.

Subnet mask merupakan sebuah teknik khusus untuk memecah atau membagi jaringan komputer sehingga menjadi subnetwork-subnetwork dengan ukuran yang lebih kecil. Kegiatan pemecahan ini dinamakan subnetting dan hanya bisa dilakukan terhadap IP Address yang terdiri dari kelas A, B dan C saja. Dengan teknik subnetting, maka suatu network dapat menciptakan beberapa network tambahan, tetapi hal itu sayangnya bisa mengurangi jumlah maksimum host yang ada dalam tiap network tersebut.

Mengapa menyimpan ukuran batas sebagai *bit-mask*? Sebuah *mask* membuat pemrosesan menjadi efisien. Secara khusus, kita akan melihat bahwa ketika mereka menangani paket IP, host dan router perlu membandingkan bagian awalan jaringan dari alamat dengan nilai dalam tabel penerusan mereka. Representasi *bit-mask* membuat perbandingan menjadi efisien. Untuk melihat caranya, misalkan router diberi alamat tujuan, D, awalan jaringan yang direpresentasikan sebagai nilai 32-bit, N, dan mask alamat 32-bit, M. Artinya, asumsikan bit teratas dari N berisi jaringan awalan, dan bit yang tersisa telah disetel ke nol. Untuk menguji apakah tujuan terletak pada jaringan yang ditentukan, router menguji kondisi:

$$T == (D \& M)$$

Artinya, router menggunakan *mask* dengan operasi "logis dan" untuk mengatur bit host alamat D ke nol, dan kemudian membandingkan hasilnya dengan awalan jaringan N.
Sebagai contoh, pertimbangkan awalan jaringan 32-bit berikut:

10000000 00001010 00000000 00000000

yang memiliki nilai desimal bertitik 128.10.0.0. Juga pertimbangkan mask 32-bit yang memiliki enam belas satu bit diikuti oleh 16 bit nol, yang dapat dilambangkan dalam desimal bertitik sebagai 255.255.0.0:

11111111 11111111 00000000 00000000

Sekarang pertimbangkan alamat tujuan 32-bit 128.10.2.3, yang memiliki ekuivalen biner dari:

10000000 00001010 00000010 00000011

Logika dan antara alamat tujuan dan mask alamat mengekstrak enam belas bit orde tinggi, yang menghasilkan hasil biner:

10000000 00001010 00000000 00000000

yang sama dengan awalan jaringan 128.10.0.0.

2.9 Notasi CIDR

Skema pengalamatan tanpa kelas secara resmi dikenal sebagai *Classless Inter-Domain Routing* (CIDR). Nama ini disayangkan karena CIDR hanya menentukan pengalamatan dan penerusan. Ketika skema pengalamatan CIDR dibuat, perancang ingin memudahkan manusia untuk menentukan mask. Untuk memahami kesulitannya, perhatikan mask yang diperlukan untuk contoh pada Gambar 2.4b, yang memiliki dua puluh enam bit 1 diikuti oleh enam bit 0. Dalam desimal bertitik, *mask*-nya adalah:

255.255.255.192

Untuk memudahkan manusia menentukan dan menafsirkan nilai mask, notasi desimal bertitik diperluas. Dalam versi yang diperluas, yang dikenal sebagai notasi CIDR, *address* dan *mask* dapat ditentukan dengan memberikan alamat desimal bertitik diikuti oleh garis miring dan angka desimal yang menentukan jumlah bit yang berdekatan dan rata kiri di mask. Artinya, bentuk umumnya adalah:

ddd.ddd.ddd.ddd / m

di mana *ddd* adalah nilai desimal untuk oktet alamat, dan m adalah jumlah satu bit dalam mask. Dengan demikian, seseorang dapat menulis yang berikut:

192.5.48.69 / 26

yang menentukan mask 26 bit. Gambar 2.5 mencantumkan mask alamat dalam notasi CIDR bersama dengan ekuivalen desimal bertitik masing-masing. Perhatikan bahwa beberapa mask alamat CIDR sesuai dengan tugas classful asli.

1.12 Contoh CIDR

Sebagai contoh CIDR, asumsikan ISP memiliki blok alamat berikut yang tersedia untuk ditetapkan:

128.211.0.0 / 16

Selanjutnya misalkan ISP memiliki dua pelanggan, satu pelanggan membutuhkan dua belas alamat IP dan pelanggan lainnya membutuhkan sembilan. ISP dapat menetapkan satu awalan CIDR pelanggan:

128.211.0.16 / 28 dan dapat menetapkan pelanggan lain:

128.211.0.32 / 28

Panjang (CIDR)	Subnet Mask	Keterangan
/0	0 . 0 . 0 . 0	Semua 0s (setara dengan tidak ada mask)
/ 1	128 . 0 . 0 . 0	
/ 2	192 . 0 . 0 . 0	
/ 3	224 . 0 . 0 . 0	
/ 4	240 . 0 . 0 . 0	
/ 5	248 . 0 . 0 . 0	
/ 6	252 . 0 . 0 . 0	
/ 7	254 . 0 . 0 . 0	
/ 8	255 . 0 . 0 . 0	Subnet-mask Kelas A asli
/ 9	225 . 128 . 0 . 0	
/ 10	225 . 192 . 0 . 0	
/ 11	225 . 224 . 0 . 0	
/ 12	225 . 240 . 0 . 0	
/ 13	225 . 248 . 0 . 0	
/ 14	225 . 252 . 0 . 0	
/ 15	225 . 254 . 0 . 0	
/ 16	225 . 255 . 0 . 0	Subnet-mask Kelas B asli
/ 17	225 . 255 . 128 . 0	
/ 18	225 . 255 . 192 . 0	
/ 19	225 . 255 . 224 . 0	
/ 20	225 . 255 . 240 . 0	
/ 21	225 . 255 . 248 . 0	
/ 22	225 . 255 . 252 . 0	
/ 23	225 . 255 . 254 . 0	
/ 24	225 . 255 . 255 . 0	Subnet-mask Kelas C asli
/ 25	225 . 255 . 255 . 128	
/ 26	225 . 255 . 255 . 192	
/ 27	225 . 255 . 255 . 224	
/ 28	225 . 255 . 255 . 240	
/ 29	225 . 255 . 255 . 248	
/ 30	225 . 255 . 255 . 242	
/ 31	225 . 255 . 255 . 254	
/ 32	225 . 255 . 255 . 255	Semua 1 (Subnet-mask khusus host)

Gambar 2.5 Daftar Subnet Mask dalam notasi CIDR dan desimal bertitik.

Meskipun kedua pelanggan memiliki ukuran mask yang sama (28 bit), prefiksnya berbeda. Nilai biner yang ditetapkan untuk satu pelanggan adalah:

10000000 11010011 00000000 0001 0000

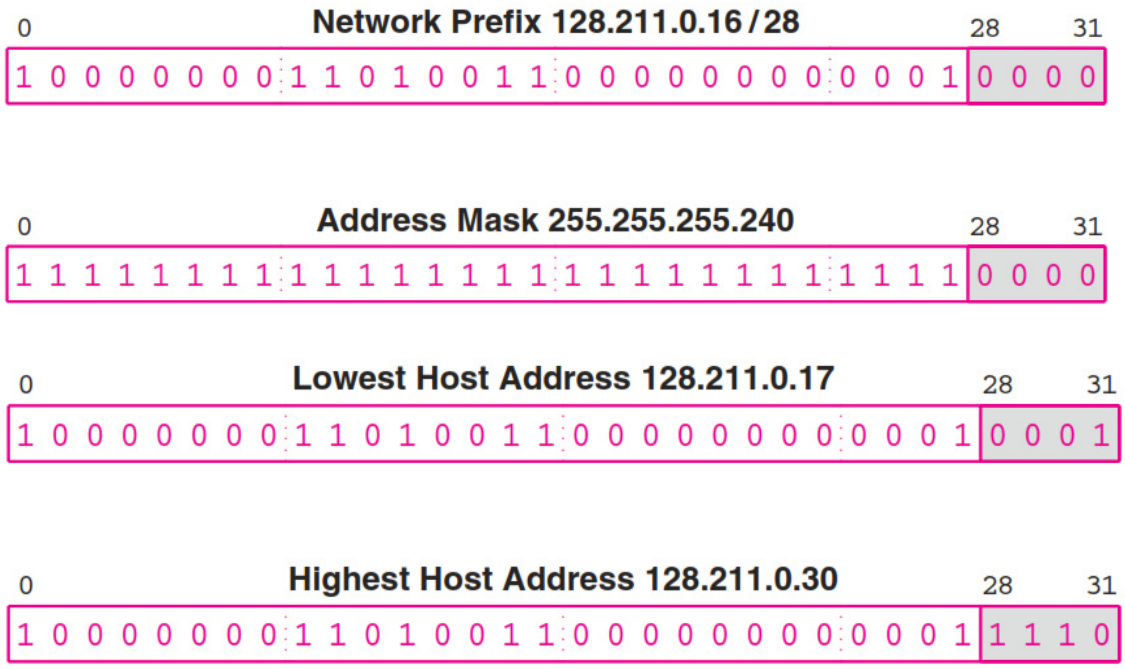
dan nilai biner yang diberikan ke pelanggan lain adalah:

10000000 11010011 00000000 0010 0000

Dengan demikian, tidak ada ambiguitas — setiap pelanggan memiliki awalan yang unik. Lebih penting lagi, ISP mempertahankan sebagian besar blok alamat asli, yang dapat dialokasikan ke pelanggan lain.

2.10 Alamat Host CIDR

Pertimbangkan untuk menghitung rentang alamat dalam blok CIDR. Setelah ISP memberikan pelanggan awalan CIDR, pelanggan dapat menetapkan alamat host. Misalnya, anggaplah sebuah organisasi ditugaskan 128.211.0.16 / 28 seperti dijelaskan di atas. Gambar 2.6 mengilustrasikan bahwa organisasi akan memiliki empat bit untuk digunakan sebagai bidang alamat host, dan menunjukkan alamat tertinggi dan terendah dalam biner dan desimal bertitik. Contoh menghindari menetapkan semua 1s dan semua 0s alamat host.



Gambar 2.6 Ilustrasi pengalamatan CIDR sebagai contoh / 28 prefix.

Gambar 2.6 mengilustrasikan kelemahan pengalamatan tanpa kelas — karena akhiran host dapat dimulai pada batas yang berubah-ubah, nilai tidak mudah dibaca dalam desimal bertitik. Misalnya, ketika digabungkan dengan awalan jaringan, empat belas kemungkinan akhiran host menghasilkan nilai desimal bertitik dari 128.211.0.17 hingga 128.211.0.30.

2.11 Alamat IP Khusus

Selain menetapkan alamat untuk setiap komputer, akan lebih mudah untuk memiliki alamat yang dapat digunakan untuk menunjukkan jaringan atau set komputer. IP mendefinisikan satu set bentuk alamat khusus yang dicadangkan. Artinya, alamat khusus tidak pernah ditetapkan ke host. Bagian ini menjelaskan sintaks dan semantik dari setiap formulir alamat khusus.

Alamat Jaringan

Salah satu motivasi untuk mendefinisikan formulir alamat khusus dapat dilihat pada Gambar 2.6 — akan lebih mudah untuk memiliki alamat yang dapat digunakan untuk menunjukkan awalan yang ditetapkan ke jaringan tertentu. IP cadangan alamat host nol, dan menggunakannya untuk menunjukkan jaringan. Jadi, alamat 128.211.0.16 / 28 menunjukkan jaringan karena bit di luar tanggal 28 adalah nol. Alamat jaringan tidak boleh muncul sebagai alamat tujuan dalam sebuah paket.

Directed Broadcast Address

Terkadang, akan lebih mudah untuk mengirim salinan paket ke semua host di jaringan fisik. Untuk menyederhanakan penyiaran, IP mendefinisikan alamat *directed broadcast* untuk setiap jaringan fisik. Ketika sebuah paket dikirim ke alamat broadcast jaringan yang diarahkan, satu salinan dari paket tersebut berjalan melintasi Internet hingga mencapai jaringan yang ditentukan. Paket tersebut kemudian dikirimkan ke semua host di jaringan.

Alamat broadcast diarahkan untuk jaringan dibentuk dengan menambahkan sufiks yang terdiri dari semua 1 bit ke awalan jaringan. Jadi, sufiks host yang terdiri dari semua 1 bit dicadangkan — jika administrator secara tidak sengaja memberikan sufiks all-one ke komputer tertentu, perangkat lunak mungkin tidak berfungsi.

Bagaimana cara kerja broadcast? Jika perangkat keras jaringan mendukung siaran, siaran langsung akan dikirimkan menggunakan kemampuan siaran perangkat keras. Jika jaringan tertentu tidak memiliki dukungan perangkat keras untuk siaran, perangkat lunak harus mengirim salinan paket yang terpisah ke setiap host di jaringan.

Limited Broadcast Address

Istilah siaran terbatas (*limited broadcast*) mengacu pada siaran di jaringan yang terhubung langsung; secara informal, kami mengatakan bahwa siaran terbatas pada "kabel tunggal". Siaran terbatas digunakan selama startup sistem oleh komputer yang belum mengetahui nomor jaringan.

IP mencadangkan alamat yang terdiri dari tiga puluh dua 1 bit untuk merujuk ke siaran terbatas. Dengan demikian, IP akan menyiarkan paket apa pun yang dikirim ke alamat all-ones di jaringan lokal.

This Computer Address

Karena setiap paket Internet berisi alamat sumber dan juga tujuan, komputer perlu mengetahui alamat IP-nya sebelum dapat mengirim atau menerima paket Internet. Pada Bab 23, kita akan mempelajari bahwa TCP/IP berisi protokol yang dapat digunakan komputer untuk mendapatkan alamat IP-nya secara otomatis saat komputer melakukan booting. Menariknya, protokol startup menggunakan IP untuk berkomunikasi. Saat menggunakan protokol pengaktifan seperti itu, komputer tidak dapat menyediakan alamat sumber IP yang benar. Untuk menangani kasus seperti itu, IP mencadangkan alamat yang terdiri dari semua nol yang berarti komputer ini.

Loopback Address

IP mendefinisikan alamat loopback yang digunakan untuk menguji aplikasi jaringan. Pemrogram sering menggunakan loopback untuk debugging awal setelah aplikasi jaringan dibuat. Untuk melakukan tes loopback, seorang programmer harus memiliki dua program aplikasi yang dimaksudkan untuk berkomunikasi melalui jaringan. Setiap aplikasi menyertakan kode yang diperlukan untuk

berinteraksi dengan perangkat lunak protokol TCP/IP. Alih-alih mengeksekusi setiap program pada komputer yang terpisah, programmer menjalankan kedua program pada satu komputer dan menginstruksikan mereka untuk menggunakan alamat loopback saat berkomunikasi. Ketika satu aplikasi mengirim data ke yang lain, data berjalan menuruni tumpukan protokol ke perangkat lunak IP, yang meneruskannya kembali melalui tumpukan protokol ke program kedua. Dengan demikian, programmer dapat menguji logika program dengan cepat tanpa memerlukan dua komputer dan tanpa mengirim paket melalui jaringan.

IP mencadangkan awalan jaringan 127/8 untuk digunakan dengan loopback. Alamat host yang digunakan dengan 127 tidak relevan — semua alamat host diperlakukan sama. Secara konvensional, pemrogram sering menggunakan host nomor 1, menjadikan 127.0.0.1 alamat loopback paling populer.

Selama pengujian loopback tidak ada paket yang pernah meninggalkan komputer — perangkat lunak IP meneruskan paket dari satu program aplikasi ke program aplikasi lainnya. Akibatnya, alamat loopback tidak pernah muncul dalam paket yang melintasi jaringan.

2.12 Ringkasan Alamat IP Khusus

Tabel pada Gambar 2.7 merangkum formulir alamat IP khusus.

Gambar 2.7 Ringkasan formulir alamat IP khusus.

Prefix	Suffix	Jenis Alamat	Tujuan
semua-0s	semua-0s	komputer ini	digunakan selama bootstrap
jaringan	semua-0s	jaringan	mengidentifikasi jaringan
jaringan	all-1s	siaran langsung	siaran di jaringan tertentu
all-1s	all-1s	siaran terbatas	siaran terbatas di jaringan lokal
127/8	apa pun	loopback	pengujian

Kami mengatakan bahwa alamat khusus dicadangkan dan tidak boleh diberikan ke komputer host. Selanjutnya, setiap alamat khusus dibatasi untuk penggunaan tertentu. Misalnya, alamat broadcast tidak boleh muncul sebagai alamat sumber, dan alamat all-0s tidak boleh digunakan setelah host menyelesaikan prosedur startup dan telah memperoleh alamat IP.

2.13 Formulir Alamat Berkeley Broadcast

University of California di Berkeley mengembangkan dan mendistribusikan implementasi awal protokol TCP/IP sebagai bagian dari BSD UNIX. Implementasi BSD berisi fitur tidak standar yang telah mempengaruhi banyak implementasi selanjutnya. Alih-alih menggunakan akhiran host dari semua yang mewakili alamat *directed broadcast* implementasi Berkeley menggunakan akhiran host yang berisi semua nol (yaitu, identik dengan alamat jaringan). Formulir alamat dikenal secara informal sebagai *Berkeley Broadcast*.

Sayangnya, banyak produsen komputer memperoleh perangkat lunak TCP/IP awal mereka dari implementasi Berkeley, dan beberapa situs masih menggunakan *Berkeley Broadcas*. Implementasi TCP/IP sering kali menyertakan parameter konfigurasi yang dapat memilih antara standar TCP/IP dan format Berkeley; banyak implementasi dibangun untuk menerima baik bentuk alamat broadcast standar

maupun Berkeley. Dengan demikian, manajer jaringan harus memilih formulir yang akan digunakan pada setiap jaringan (jika *directed broadcast* diperbolehkan).

2.14 Router dan Prinsip Pengalamatan IP

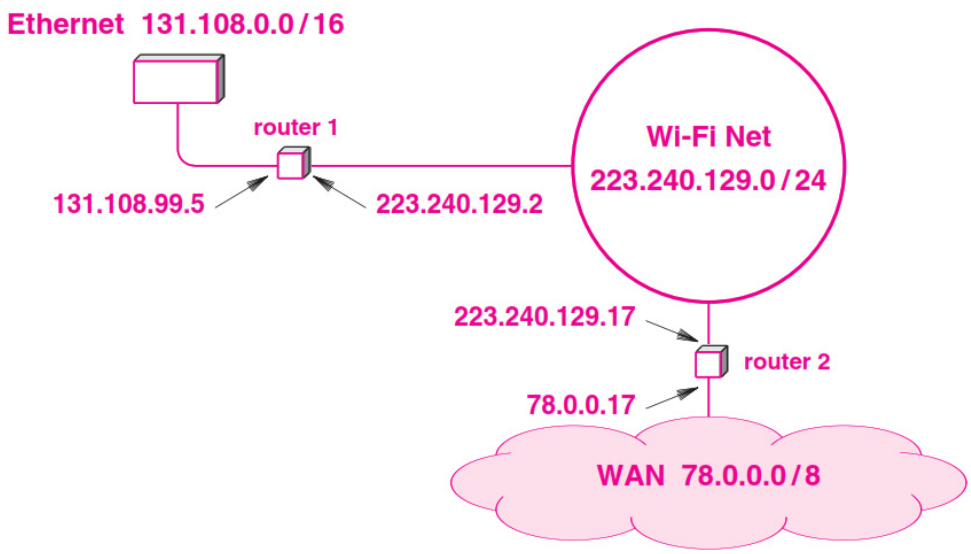
Selain menetapkan alamat Internet untuk setiap host, Protokol Internet menetapkan bahwa router juga harus diberikan alamat IP. Faktanya, setiap router diberikan dua atau lebih alamat IP, satu untuk setiap jaringan yang terhubung dengan router. Untuk memahami alasannya, ingat dua fakta:

- Sebuah router memiliki koneksi ke beberapa jaringan fisik.
- Setiap alamat IP berisi prefiks yang menentukan jaringan fisik.

Jadi, satu alamat IP tidak cukup untuk router karena setiap router terhubung ke beberapa jaringan dan setiap jaringan memiliki awalan yang unik. Skema IP dapat dijelaskan dengan prinsip dasar:

> *Alamat IP tidak mengidentifikasi komputer tertentu. Sebaliknya, setiap alamat IP mengidentifikasi koneksi antara komputer dan jaringan. Komputer dengan beberapa koneksi jaringan (mis., Router) harus diberi satu alamat IP untuk setiap koneksi.*

Gambar 2.8 mengilustrasikan ide dengan contoh yang menunjukkan alamat IP yang ditetapkan untuk dua router yang menghubungkan tiga jaringan.



Gambar 2.8 Contoh alamat IP yang ditetapkan untuk dua router.

IP tidak mengharuskan sufiks yang sama diberikan ke semua antarmuka router. Pada gambar, misalnya, router yang menghubungkan Ethernet dan jaringan Wi-Fi memiliki sufiks 99,5 (koneksi ke Ethernet) dan 2 (koneksi ke jaringan Wi-Fi). Namun, IP tidak mencegah penggunaan akhiran yang sama untuk semua koneksi. Jadi, contoh menunjukkan bahwa administrator telah memilih untuk menggunakan sufiks yang sama, 17, untuk kedua antarmuka router yang menghubungkan jaringan Wi-Fi ke WAN. Secara praktis, penggunaan akhiran yang sama dapat membantu manusia yang mengelola jaringan karena satu nomor lebih mudah diingat.

2.15 Skema Host sebagai Multi Host

Bisakah sebuah host terhubung ke beberapa jaringan? Ya. Komputer host dengan beberapa koneksi jaringan dikatakan multi-homed. Multi-homing terkadang digunakan untuk meningkatkan keandalan — jika satu jaringan gagal, host masih dapat menjangkau Internet melalui koneksi kedua. Atau, multi-homing digunakan untuk meningkatkan kinerja — koneksi ke beberapa jaringan dapat memungkinkan untuk mengirim lalu lintas secara langsung dan menghindari router, yang terkadang macet. Seperti router, host multi-homed memiliki beberapa alamat protokol, satu untuk setiap koneksi jaringan.

2.16 Ringkasan

Untuk memberikan tampilan jaringan yang besar dan mulus, Internet menggunakan skema pengalamatan yang seragam. Setiap komputer diberi alamat IP yang unik; semua aplikasi Internet menggunakan alamat tersebut saat berkomunikasi dengan komputer.

Protokol Internet menentukan pengalamatan. IP membagi setiap alamat Internet menjadi hierarki dua tingkat: awalan mengidentifikasi jaringan tempat komputer terhubung, dan akhiran mengidentifikasi komputer tertentu di jaringan. Untuk memastikan bahwa alamat tetap unik di seluruh internet yang diberikan, otoritas pusat memberikan awalan jaringan. Setelah awalan telah ditetapkan, administrator jaringan lokal memberikan setiap host di jaringan akhiran yang unik.

Alamat IP adalah angka 32 bit. Skema pengalamatan asli membagi alamat ke dalam kelas-kelas; kelas multicast masih digunakan. Pengalamatan tanpa kelas dan subnet memungkinkan batas antara awalan dan akhiran terjadi pada batas bit yang berubah-ubah. Untuk melakukannya, subnet dan pengalamatan tanpa kelas (CIDR) menyimpan mask 32-bit bersama dengan setiap alamat. Mask memiliki nilai 1 untuk setiap bit di awalan, dan nilai 0 untuk setiap bit di akhiran.

Standar IP menentukan satu set alamat yang dicadangkan yang memiliki arti khusus. Alamat khusus dapat digunakan untuk menentukan loopback (digunakan untuk pengujian), alamat jaringan, siaran di jaringan fisik lokal, dan siaran di jaringan jarak jauh.

Meskipun lebih mudah untuk menganggap alamat IP sebagai menentukan komputer, setiap host multi-rumah, yang memiliki koneksi ke beberapa jaringan fisik, masing-masing memiliki beberapa alamat IP.

Latihan

1. Bisakah IP didesain ulang untuk menggunakan alamat perangkat keras alih-alih alamat 32-bit yang saat ini digunakan? Mengapa atau mengapa tidak?
2. Apa yang dapat dilakukan oleh hierarki alamat Internet oleh manajer lokal?
3. Dalam skema alamat classful asli, apakah mungkin untuk menentukan kelas alamat dari alamat itu sendiri? Jelaskan.

4. Tulis program komputer yang menerima alamat desimal bertitik sebagai input dan menampilkan string 32 bit.
5. Tulis program komputer yang membaca alamat IP dalam bentuk desimal bertitik dan menentukan apakah alamat tersebut merupakan alamat multicast.
6. Tulis program komputer yang menerjemahkan antara notasi garis miring CIDR dan nilai desimal bertitik yang setara.
7. Jika ISP memberi Anda blok alamat / 28, berapa banyak komputer yang dapat Anda berikan alamatnya?
8. Jika ISP menawarkan blok alamat / 17 seharga N rupiah per bulan dan blok alamat / 16 untuk 1,5 N rupiah per bulan, yang memiliki biaya termurah per komputer?
10. Apakah awalan CIDR 1.2.3.4 / 29 valid? Mengapa atau mengapa tidak?
11. Misalkan Anda adalah ISP dengan blok alamat / 24. Jelaskan apakah Anda mengakomodasi permintaan dari pelanggan yang membutuhkan alamat untuk 255 komputer. (Petunjuk: pertimbangkan alamat khusus.)
12. Misalkan Anda adalah ISP yang memiliki blok alamat / 22. Tunjukkan alokasi CIDR yang akan Anda gunakan untuk mengalokasikan blok alamat ke empat pelanggan yang membutuhkan alamat untuk masing-masing 60 komputer.
13. Misalkan Anda adalah ISP yang memiliki blok alamat / 22. Dapatkah Anda mengakomodasi permintaan dari enam pelanggan yang membutuhkan alamat untuk masing-masing 9, 15, 20, 41, 128, dan 260 komputer? Jika demikian, bagaimana? Jika tidak, jelaskan mengapa.
14. Tulis program komputer yang membaca alamat dalam notasi CIDR dan mencetak alamat dan mask yang dihasilkan dalam biner.
15. Tulis program komputer yang membaca sebagai input awalan jaringan dalam notasi CIDR dan permintaan untuk sejumlah host. Asumsikan permintaan telah diberikan kepada ISP yang memiliki awalan, dan tetapkan awalan CIDR yang mengakomodasi permintaan tanpa membuang alamat.
16. Tulis program komputer yang membaca alamat host 32-bit dan mask 32-bit di CIDR
17. notasi dan memberitahukan apakah alamat tersebut merupakan salah satu alamat khusus.
18. Apa yang dimaksud dengan alamat siaran Berkeley?
19. Berapa banyak alamat IP yang ditetapkan ke router? Jelaskan.
20. Bisakah sebuah host memiliki lebih dari satu alamat IP? Jelaskan.

Bab 3 Penerusan Datagram

Bab ini akan membahas tentang:

- Layanan komunikasi mendasar di Internet.
- Format paket yang dikirim melalui Internetl
- Konsep kunci enkapsulasi datagram, penerusan, dan fragmentasi dan perakitan kembali

3.1 Layanan Tanpa Koneksi

Tujuan dari internetworking adalah untuk menyediakan sistem komunikasi paket yang memungkinkan program yang berjalan di satu komputer untuk mengirim data ke program yang berjalan di komputer lain. Dalam internet yang dirancang dengan baik, program aplikasi tetap tidak menyadari jaringan fisik yang mendasari — mereka dapat mengirim dan menerima data tanpa mengetahui detail jaringan lokal yang terhubung dengan komputer, jaringan jarak jauh yang terhubung dengan tujuan, atau interkoneksi antara dua.

Salah satu pertanyaan mendasar yang harus dipertimbangkan ketika merancang sebuah internet menyangkut layanan yang akan ditawarkan. Secara khusus, desainer harus memutuskan apakah akan menawarkan layanan berorientasi koneksi, layanan tanpa koneksi, atau keduanya.

Perancang TCP/IP memilih untuk menyertakan protokol baik untuk layanan connectionless maupun connection-oriented. Mereka memilih untuk membuat layanan pengiriman dasar tanpa koneksi, dan menambahkan layanan berorientasi koneksi andal yang menggunakan layanan tanpa koneksi yang mendasarinya. Desainnya berhasil, dan menjadi dasar untuk semua komunikasi Internet.

3.2 Paket Virtual

Layanan tanpa koneksi adalah perpanjangan langsung dari packet switching — layanan ini memungkinkan pengirim untuk mengirimkan paket data individual di Internet. Setiap paket berjalan secara independen, dan berisi informasi yang mengidentifikasi penerima yang dituju.

Bagaimana sebuah paket melewati Internet? Secara umum, jawabannya adalah bahwa router menangani sebagian besar penerusan. Sebuah host membuat sebuah paket, menempatkan alamat tujuan di header paket, dan kemudian mengirimkan paket ke router terdekat. Ketika router menerima paket, router menggunakan alamat tujuan untuk memilih router berikutnya di jalur ke tujuan, dan kemudian meneruskan paket. Akhirnya, paket mencapai router yang dapat mengirimkan paket ke tujuan akhirnya.

Format apa yang digunakan untuk paket Internet? Karena Internet terdiri dari jaringan heterogen yang menggunakan format bingkai yang tidak kompatibel, Internet tidak dapat mengadopsi salah satu format bingkai perangkat keras. Lebih penting lagi, router tidak bisa begitu saja memformat ulang frame header karena dua jaringan mungkin menggunakan pengalamatan yang tidak kompatibel (misalnya, alamat dalam frame yang masuk mungkin tidak masuk akal di jaringan lain).
Untuk mengatasi heterogenitas, Internet Protocol mendefinisikan format paket yang tidak bergantung pada perangkat keras yang mendasarinya. Hasilnya adalah paket virtual universal yang dapat ditransfer melintasi perangkat keras yang mendasarinya secara utuh. Seperti yang tersirat dalam istilah virtual, format paket Internet tidak terikat langsung ke perangkat keras apa pun. Faktanya, perangkat keras yang mendasarinya tidak memahami atau mengenali paket Internet. Seperti yang tersirat dari istilah universal, setiap host atau router di Internet berisi perangkat lunak protokol yang mengenali paket Internet.

Poin Penting

Karena mencakup jaringan yang tidak kompatibel, Internet tidak dapat mengadopsi format paket perangkat keras tertentu. Untuk mengakomodasi heterogenitas, Protokol Internet mendefinisikan format paket yang tidak bergantung pada perangkat keras.

3.3 Datagram IP

Protokol TCP/IP menggunakan nama datagram IP untuk merujuk ke paket Internet. Anehnya, datagram IP memiliki format umum yang sama dengan kerangka perangkat keras: datagram dimulai dengan header diikuti oleh area data (atau payload). Gambar 3.1 mengilustrasikan format datagram.

Gambar 3.1 Bentuk umum dari datagram IP dengan header diikuti dengan payload

Poin Penting

Paket yang dikirim melalui internet TCP/IP disebut IP datagram. Setiap datagram terdiri dari header diikuti oleh area data, yang dikenal sebagai payload.

Jumlah data yang dibawa dalam datagram tidak tetap. Pengirim memilih sejumlah data yang sesuai untuk tujuan tertentu. Misalnya, aplikasi yang mengirimkan penekanan tombol di seluruh jaringan dapat menempatkan setiap penekanan tombol dalam datagram terpisah, sedangkan aplikasi yang mentransfer file besar dapat mengirim datagram besar.

Poin Penting

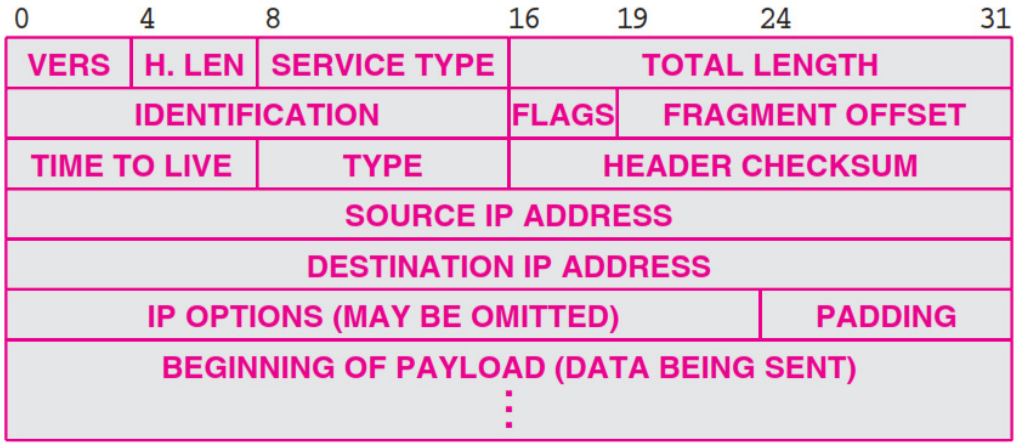
Ukuran datagram ditentukan oleh aplikasi yang mengirimkan data. Membiarkan ukuran datagram bervariasi membuat IP dapat beradaptasi dengan berbagai aplikasi.

Dalam versi Internet Protocol (IP versi 4) saat ini, datagram dapat berisi sesedikit satu oktet data atau paling banyak 64K oktet, termasuk header. Di sebagian besar datagram, header jauh lebih kecil daripada payload. Header mewakili overhead — karena ukuran header datagram tetap, pengiriman datagram besar menghasilkan lebih banyak oktet data yang ditransmisikan per unit waktu (yaitu, throughput yang lebih tinggi).

3.4 Format Header Datagram IP

Apa isi header datagram? Mirip dengan header frame, header datagram berisi informasi yang digunakan untuk meneruskan datagram. Secara khusus, header berisi alamat sumber (pengirim asli), alamat tujuan (penerima akhir), dan bidang yang menentukan jenis data yang dibawa di area muatan. Setiap alamat di header adalah alamat IP; Alamat MAC untuk pengirim dan penerima tidak muncul di datagram.

Setiap bidang dalam header datagram IP memiliki ukuran tetap, yang membuat pemrosesan header menjadi efisien. Gambar 3.2 menunjukkan bidang dari header datagram IP, dan teks selanjutnya menjelaskan setiap bidang.



Gambar 3.2 Field pada header datagram versi 4 IP.

- VERS. Setiap datagram dimulai dengan nomor versi protokol 4-bit (gambar menunjukkan header versi 4).
- H.LEN. Bidang panjang header 4-bit menentukan jumlah kuantitas 32-bit di header. Jika tidak ada opsi, nilainya adalah 5.

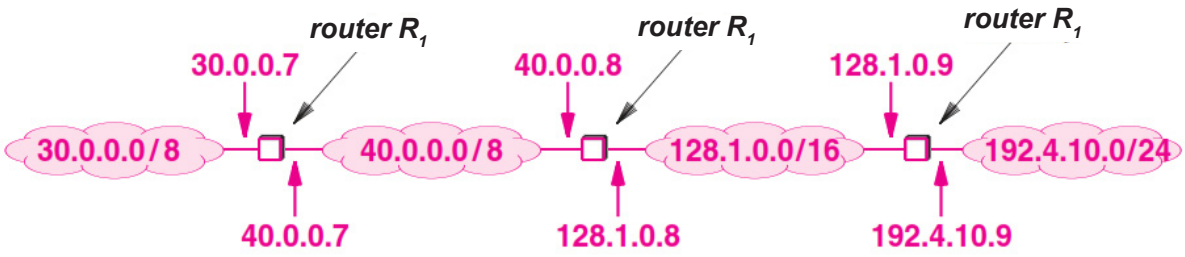
- SERVICE TYPE. Bidang 8-bit yang membawa kelas layanan untuk datagram (jarang digunakan dalam praktik). Bab 28 menjelaskan interpretasi DiffServ dari bidang jenis layanan.
- TOTAL LENGTH. Integer 16-bit yang menentukan jumlah total byte dalam datagram, termasuk header dan data.
- IDENTIFICATION. Nomor 16-bit unik (biasanya berurutan) yang ditetapkan ke datagram yang digunakan untuk mengumpulkan semua fragmen untuk dipasang kembali.
- FLAGS. Bidang 3-bit dengan bit individu yang menentukan apakah datagram adalah fragmen dan jika demikian, apakah fragmen sesuai dengan bagian paling kanan dari datagram asli.
- FRAGMENT OFFSET. Bidang 13-bit yang menentukan di mana dalam datagram asli data dalam fragmen ini berada. Nilai bidang dikalikan dengan delapan untuk mendapatkan offset.
- TIME TO LIVE . Integer 8-bit yang diinisialisasi oleh pengirim asli dan dikurangi oleh setiap router yang memproses datagram. Jika nilainya mencapai nol, datagram dibuang dan pesan kesalahan dikirim kembali ke sumbernya.
- TYPE. Bidang 8-bit yang menentukan jenis muatan.
- HEADER CHECKSUM. checksum one-complement 16-bit dari bidang header yang dihitung menurut Algoritma 8.1†.
- SOURCE IP ADDRESS. Alamat Internet 32-bit pengirim asli (alamat router perantara tidak muncul di header).
- DESTINATION IP ADDRESS. Alamat Internet 32-bit dari tujuan akhir. Alamat router perantara tidak muncul di header.
- IP OPTIONS. Bidang header opsional yang digunakan untuk mengontrol perutean dan pemrosesan datagram. Sebagian besar datagram tidak mengandung opsi apa pun, yang berarti bidang IP OPTIONS dihilangkan dari header.
- PADDING. Jika opsi tidak berakhir pada batas 32-bit, nol bit padding ditambahkan untuk membuat header kelipatan 32 bit.

3.5 Meneruskan Datagram IP

Kami mengatakan bahwa datagram melintasi Internet dengan mengikuti jalur dari sumber awalnya melalui router ke tujuan akhir. Internet menggunakan penerusan hop berikutnya. Setiap router di sepanjang jalur menerima datagram, mengekstrak alamat tujuan dari header, dan menggunakan alamat tujuan untuk menentukan hop berikutnya ke mana datagram harus dikirim. Router kemudian meneruskan datagram ke hop berikutnya, baik tujuan akhir atau router lain.

Untuk membuat pemilihan hop berikutnya efisien, router IP menggunakan tabel penerusan. Tabel penerusan diinisialisasi saat router melakukan booting, dan harus diperbarui jika topologi berubah atau perangkat keras gagal.

Secara konseptual, tabel penerusan berisi satu set entri yang masing-masing menentukan tujuan dan hop berikutnya yang digunakan untuk mencapai tujuan itu. Gambar 3.3 menunjukkan contoh internet dan isi tabel penerusan di salah satu dari tiga router yang digunakan untuk menghubungkan jaringan.



(a)

Destination	Mask	Hop Selanjutnya
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	deliver direct
128.1.0.0	255.255.0.0	deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

(b)

Gambar 3.3 (a) Contoh internet dengan empat jaringan, dan (b) tabel penerusan yang terdapat pada router R2.

Pada gambar, setiap router telah diberikan dua alamat IP, satu untuk setiap antarmuka. Router R2, yang terhubung langsung ke jaringan 40.0.0.0 / 8 dan 128.1.0.0 / 16, telah diberikan alamat 40.0.0.8 dan 128.1.0.8. Ingatlah bahwa IP tidak memerlukan sufiks yang sama di semua antarmuka — administrator jaringan telah memilih sufiks yang sama untuk setiap antarmuka untuk memudahkan manusia yang mengelola jaringan.

Poin penting yang perlu diperhatikan adalah ukuran tabel penerusan, yang sangat penting di Internet global bahwa karena setiap tujuan dalam tabel penerusan sesuai dengan jaringan, jumlah entri dalam tabel penerusan sebanding dengan jumlah jaringan di Internet, bukan jumlah host.

3.6 Ekstraksi Prefiks Jaringan dan Penerusan Datagram

Proses menggunakan tabel penerusan untuk memilih hop berikutnya untuk datagram yang diberikan disebut penerusan (*forwarding*). Ingat dari Bab 2 bahwa subnet-mask dalam entri tabel penerusan digunakan untuk mengekstrak bagian jaringan dari sebuah alamat selama pencarian. Ketika router menemukan datagram dengan alamat IP tujuan D, fungsi penerusan harus menemukan entri di tabel penerusan yang menentukan hop berikutnya untuk D. Untuk melakukannya, perangkat lunak memeriksa setiap entri dalam tabel dengan menggunakan mask di entri untuk mengekstrak awalan alamat D dan membandingkan awalan yang dihasilkan dengan bidang Tujuan entri. Jika keduanya sama, datagram akan diteruskan ke Next Hop di entri.

Representasi bit mask membuat ekstraksi menjadi efisien — perhitungan terdiri dari Boolean dan antara mask dan alamat tujuan, D. Dengan demikian, komputasi untuk memeriksa entri ke-i dalam tabel dapat dinyatakan sebagai:

```
if ( (Mask[i] & D) == Destination[i] ) teruskan ke NextHop[i];
```

Sebagai contoh, perhatikan sebuah datagram yang ditujukan untuk alamat 192.4.10.3, dan asumsikan datagram tersebut tiba di router pusat, R2, pada Gambar 3.3. Selanjutnya asumsikan prosedur penerusan mencari entri tabel secara berurutan. Entri pertama gagal karena 255.0.0.0 & 192.4.10.3 tidak sama dengan 30.0.0.0. Setelah menolak entri kedua dan ketiga dalam tabel, perangkat lunak perutean akhirnya memilih hop berikutnya 128.1.0.9 karena

255.255.255.0 & 192.4.10.3 == 192.4.10.

3.7 Pencocokan Prefiks yang Panjang

Gambar 3.3 berisi contoh sepele. Dalam praktiknya, tabel penerusan Internet bisa sangat besar, dan algoritme penerusannya rumit. Misalnya, analog dengan penerusan WAN yang dijelaskan dalam Bab 18 pada Buku Jilid 1, tabel penerusan Internet dapat berisi entri default yang menyediakan jalur untuk semua tujuan yang tidak dicantumkan secara eksplisit. Selain itu, penerusan Internet memungkinkan manajer untuk menentukan rute khusus host yang mengarahkan lalu lintas yang ditujukan ke host tertentu di sepanjang jalur yang berbeda dari lalu lintas untuk host lain di jaringan yang sama (yaitu, untuk menentukan entri tabel penerusan dengan entri tabel penerusan 32-bit). mask, yang membutuhkan kecocokan seluruh alamat host).

Fitur penting dari penerusan Internet muncul karena subnet-mask dapat tumpang tindih. Misalnya, tabel penerusan router berisi entri untuk dua prefiks jaringan berikut:

128.10.0.0 / 16

128.10.2.0 / 24

Pertimbangkan apa yang terjadi jika datagram tiba dengan tujuan 128.10.2.3. Anehnya, prosedur pencocokan yang dijelaskan di atas berhasil untuk kedua entri. Artinya, Boolean dan topeng 16-bit akan menghasilkan 128.10.0.0, dan Boolean dan dengan topeng 24-bit akan menghasilkan 128.10.2.0. Entri mana yang harus digunakan?

Untuk menangani ambiguitas yang muncul dari topeng alamat yang tumpang tindih, penerusan Internet menggunakan kecocokan awalan terpanjang. Artinya, alih-alih memeriksa entri dalam urutan sewenang-wenang, perangkat lunak penerusan mengatur untuk memeriksa entri dengan awalan terpanjang terlebih dahulu. Dalam contoh di atas, penerusan Internet akan memilih entri yang sesuai dengan 128.10.2.0 / 24.

Poin Penting

Untuk mengatasi ambiguitas yang dapat muncul ketika lebih dari satu entri cocok dengan tujuan, penerusan Internet memeriksa entri dengan prefiks terpanjang terlebih dahulu.

3.8 Alamat Tujuan dan Alamat Next-Hop

Apa hubungan antara alamat tujuan di header datagram dan alamat hop berikutnya ke mana datagram diteruskan? Bidang ALAMAT IP TUJUAN dalam datagram berisi alamat tujuan akhir; itu tidak berubah ketika datagram melewati Internet. Ketika router menerima datagram, router menggunakan tujuan akhir, D, untuk menghitung alamat router berikutnya ke mana datagram harus dikirim, N. Meskipun router meneruskan datagram ke hop berikutnya, N, header di datagram mempertahankan alamat tujuan D.

Poin Penting

Alamat tujuan dalam header datagram selalu mengacu pada tujuan akhir; pada setiap titik, hop berikutnya dihitung, tetapi alamat hop berikutnya tidak muncul di header datagram.

3.9 Pelayanan Terbaik IP

Selain mendefinisikan format datagram Internet, Protokol Internet mendefinisikan semantik komunikasi, dan menggunakan istilah *best-effort* (upaya terbaik) untuk menggambarkan layanan yang ditawarkannya. Intinya, standar tersebut menetapkan bahwa meskipun IP melakukan upaya terbaik untuk mengirimkan setiap datagram, IP tidak menjamin bahwa ia akan menangani semua masalah. Secara khusus, standar IP mengakui bahwa masalah berikut dapat terjadi:

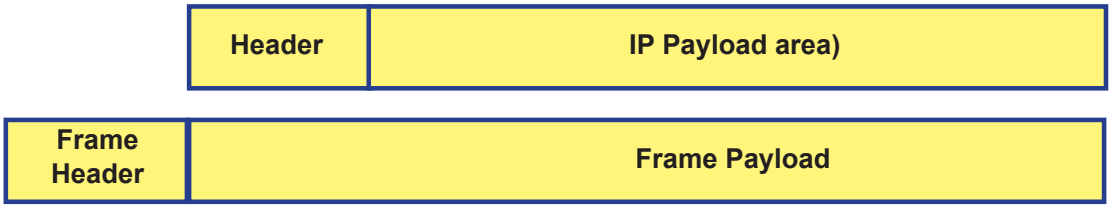
- duplikasi datagram
- Pengiriman tertunda atau tidak sesuai pesanan
- korupsi data
- kehilangan datagram

Mungkin aneh bagi IP untuk menentukan bahwa kesalahan dapat terjadi. Namun, ada alasan penting: IP dirancang untuk berjalan di semua jenis jaringan. Kita tahu dari bab sebelumnya bahwa peralatan jaringan dapat mengalami gangguan dari kebisingan, yang dapat mengakibatkan kerusakan atau kehilangan. Dalam sistem di mana rute dapat berubah, paket yang mengikuti satu jalur mungkin memakan waktu lebih lama daripada yang mengikuti jalur lain, yang dapat mengakibatkan pengiriman yang tidak sesuai pesanan.

Karena IP dirancang untuk beroperasi pada semua jenis perangkat keras jaringan, termasuk perangkat keras yang mengalami masalah, datagram IP dapat hilang, terduplikasi, tertunda, rusak, atau dikirimkan dengan data yang rusak. Untungnya, kita akan melihat bahwa paket protokol TCP/IP menyertakan protokol tambahan yang menangani banyak masalah. Kami juga akan mempelajari bahwa beberapa aplikasi lebih memilih untuk menggunakan layanan upaya terbaik daripada layanan yang mendeteksi dan memperbaiki masalah.

3.10 Enkapsulasi IP

Bagaimana datagram dapat ditransmisikan melalui jaringan fisik yang tidak memahami format datagram? Jawabannya terletak pada teknik yang dikenal sebagai enkapsulasi. Ketika datagram IP dienkapsulasi dalam bingkai, seluruh datagram ditempatkan di area muatan bingkai. Perangkat keras jaringan memperlakukan bingkai yang berisi datagram persis seperti bingkai lainnya. Faktanya, perangkat keras tidak memeriksa atau mengubah isi muatan. Gambar 3.4 mengilustrasikan konsep tersebut.



Gambar 3.4 Ilustrasi datagram IP yang dienkapsulasi dalam bingkai.

Bagaimana penerima mengetahui apakah muatan bingkai yang masuk berisi datagram IP atau data lain? Pengirim dan penerima harus menyetujui nilai yang digunakan dalam bidang jenis bingkai. Ketika menempatkan datagram dalam bingkai, perangkat lunak pada komputer pengirim memberikan bidang jenis bingkai nilai khusus yang disediakan untuk IP. Ketika sebuah frame tiba dengan nilai IP di bidang tipenya, penerima tahu bahwa area muatan berisi datagram IP. Misalnya, standar Ethernet menetapkan bahwa bidang jenis bingkai Ethernet yang membawa datagram IP ditetapkan 0x0800.

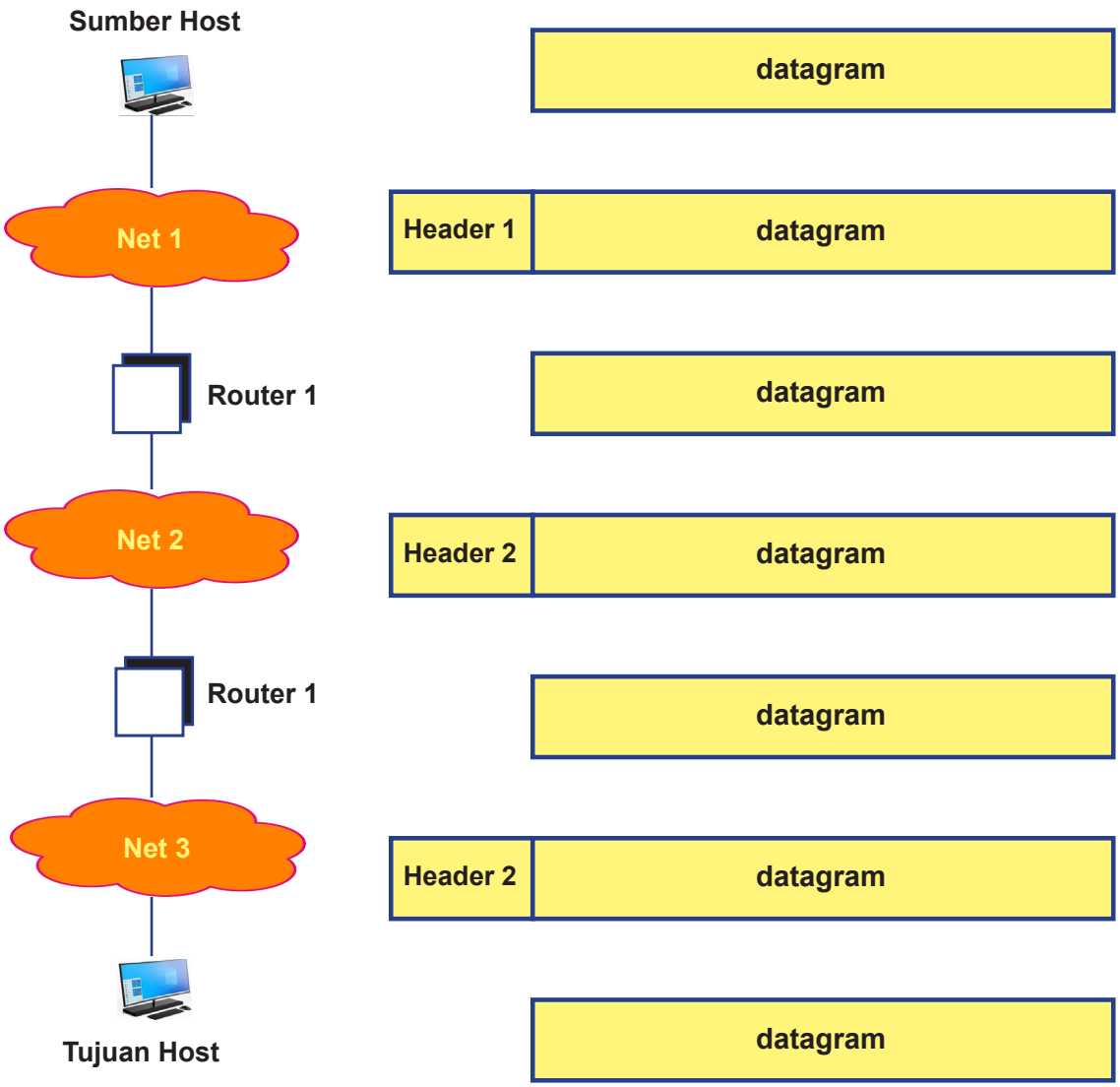
Sebuah frame yang membawa IP datagram harus memiliki alamat tujuan. Oleh karena itu, selain menempatkan datagram di area payload dari sebuah frame, enkapsulasi membutuhkan pengirim untuk memberikan alamat MAC dari komputer berikutnya ke mana datagram harus dikirim. Untuk menghitung alamat yang sesuai, IP pada komputer pengirim harus mengikat alamat IP next-hop ke alamat MAC yang setara, yang merupakan tujuan di header frame. Bab berikutnya menjelaskan protokol ARP yang digunakan untuk melakukan pengikatan.

Poin Penting

Datagram dienkapsulasi dalam bingkai untuk transmisi melalui jaringan fisik. Alamat tujuan dalam frame adalah alamat MAC dari hop berikutnya ke mana datagram sedang dikirim; alamat diperoleh dengan menerjemahkan alamat IP dari hop berikutnya ke alamat MAC yang setara.

3.11 Transmisi Melalui Internet

Enkapsulasi berlaku untuk satu transmisi pada satu waktu. Setelah pengirim memilih hop berikutnya, pengirim merangkum datagram dalam bingkai dan mengirimkan hasilnya melalui jaringan fisik. Ketika frame mencapai hop berikutnya, perangkat lunak penerima menghapus datagram IP dan membuang frame. Jika datagram harus diteruskan melalui jaringan lain, bingkai baru dibuat. Gambar 3.5 mengilustrasikan bagaimana datagram dienkapsulasi dan tidak dienkapsulasi saat berjalan dari host sumber ke host tujuan melalui tiga jaringan dan dua router. Setiap jaringan dapat menggunakan teknologi perangkat keras yang berbeda dari yang lain, artinya format bingkai dan ukuran header bingkai dapat berbeda.



Gambar 3.5 Sebuah datagram IP saat melintasi Internet.

Seperti yang ditunjukkan gambar, host dan router menyimpan datagram dalam memori tanpa header tambahan. Ketika datagram melewati jaringan fisik, datagram dienkapsulasi dalam bingkai yang sesuai untuk jaringan. Ukuran header frame yang muncul sebelum datagram tergantung pada teknologi jaringan. Misalnya, jika Net 1 mewakili Ethernet, header di frame 1 adalah header Ethernet. Demikian pula, jika Net 2 mewakili jaringan Wi-Fi, header di frame 2 sesuai dengan header Wi-Fi.

Penting untuk diperhatikan bahwa header frame tidak menumpuk selama perjalanan melalui Internet. Ketika datagram tiba, datagram dihapus dari frame masuk sebelum dienkapsulasi dalam frame keluar. Jadi, ketika datagram mencapai tujuan akhirnya, satu-satunya header frame pada datagram adalah header dari jaringan terakhir tempat datagram tiba. Setelah header dihapus, hasilnya adalah datagram asli.

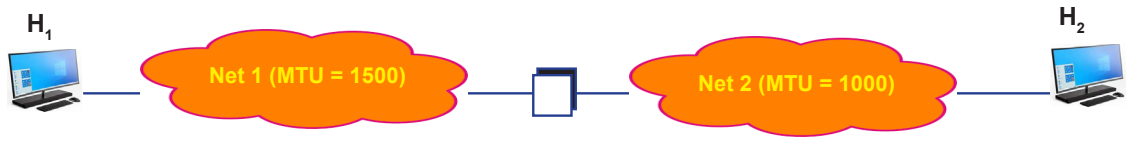
Poin Penting

Ketika datagram tiba dalam bingkai jaringan, penerima mengekstrak datagram dari area muatan bingkai dan membuang header bingkai.

3.12 MTU dan Fragmentasi Datagram

Setiap teknologi perangkat keras menentukan jumlah maksimum data yang dapat dibawa oleh bingkai. Batas tersebut dikenal sebagai *Maximum Transmission Unit* (MTU). Tidak ada pengecualian untuk batas MTU — perangkat keras jaringan tidak dirancang untuk menerima atau mentransfer bingkai yang membawa lebih banyak data daripada yang diizinkan MTU. Dengan demikian, datagram harus lebih kecil atau sama dengan jaringan MTU, atau tidak dapat dienkapsulasi untuk transmisi.

Di internet yang memiliki jaringan heterogen, pembatasan MTU menimbulkan masalah. Secara khusus, karena router dapat menghubungkan jaringan dengan nilai MTU yang berbeda, datagram yang diterima router melalui satu jaringan bisa terlalu besar untuk dikirim melalui jaringan lain. Misalnya, Gambar 3.6 mengilustrasikan router yang menghubungkan dua jaringan dengan nilai MTU 1500 dan 1000.



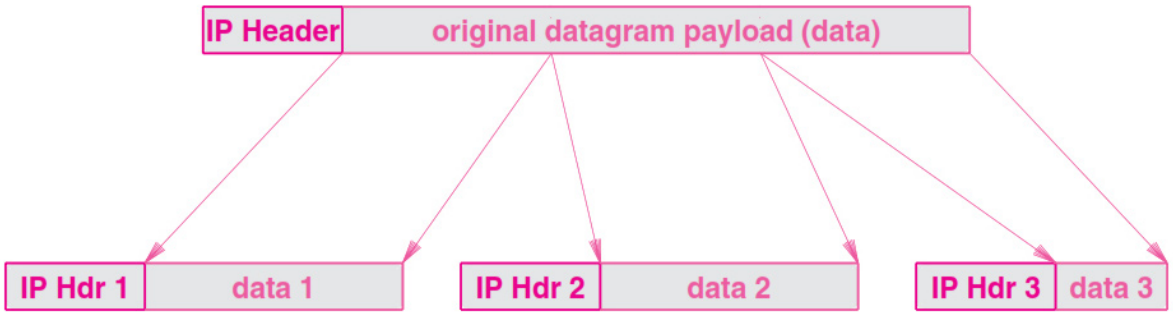
Gambar 3.6 Ilustrasi router yang menghubungkan dua jaringan dengan MTU yang berbeda.

Pada gambar, host H1 terhubung ke jaringan dengan MTU 1500, dan dapat mengirim datagram hingga 1500 oktet. Host H2 terhubung ke jaringan yang memiliki MTU 1000, yang berarti tidak dapat mengirim atau menerima datagram yang lebih besar dari 1000 oktet. Jika host H1 mengirimkan datagram 1500 oktet ke host H2, router R tidak akan dapat merangkum datagram untuk transmisi melalui jaringan 2.

Untuk mengatasi masalah MTU yang heterogen, router menggunakan teknik yang dikenal sebagai fragmentasi. Ketika datagram lebih besar dari MTU jaringan yang harus dikirim, router membagi datagram menjadi bagian-bagian yang lebih kecil yang disebut fragmen, dan mengirimkan setiap fragmen secara independen.

Anehnya, sebuah fragmen memiliki format yang sama dengan datagram lain — sedikit di bidang FLAGS pada header menunjukkan apakah datagram adalah fragmen atau datagram lengkap. Bidang lain di header diberi informasi yang digunakan tujuan akhir untuk menyusun kembali fragmen untuk mereproduksi datagram asli. Secara khusus, bidang FRAGMENT OFFSET di header sebuah fragmen menentukan di mana dalam datagram asli fragmen tersebut berada.

Untuk memecah datagram untuk transmisi di seluruh jaringan, router menggunakan jaringan MTU dan ukuran header untuk menghitung jumlah maksimum data yang dapat dikirim di setiap fragmen dan jumlah fragmen yang akan dibutuhkan. Router kemudian membuat fragmen. Ini menggunakan bidang dari header asli untuk membuat header fragmen. Misalnya, router menyalin bidang IP SOURCE dan IP DESTINATION dari datagram ke header fragmen. Terakhir, router menyalin data yang sesuai dari datagram asli ke dalam fragmen, dan mengirimkan hasilnya. Gambar 3.7 mengilustrasikan pembagian.



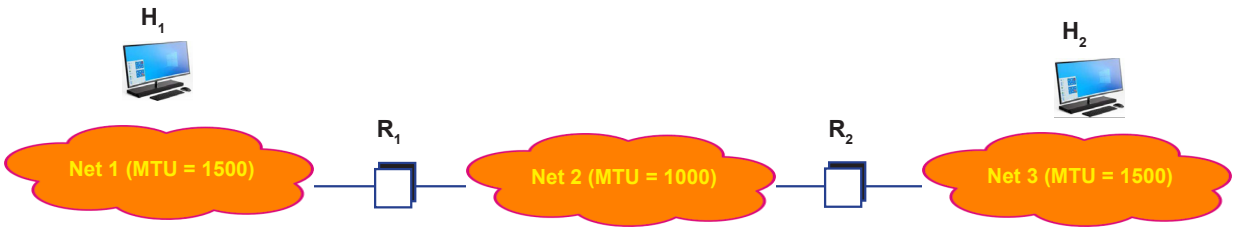
Gambar 3.7 Sebuah datagram IP dibagi menjadi tiga fragmen, dengan fragmen terakhir lebih kecil dari yang lain.

Poin Penting

Setiap jaringan memiliki MTU yang menentukan jumlah maksimum data yang dapat dibawa oleh frame. Ketika router menerima datagram yang lebih besar dari MTU jaringan yang akan dikirim, router membagi datagram menjadi bagian-bagian yang lebih kecil yang disebut fragmen. Setiap fragmen menggunakan format datagram IP, tetapi hanya membawa sebagian dari muatan aslinya.

3.13 Perakitan Kembali Datagram dari Fragmen

Proses membuat kembali salinan datagram asli dari fragmen disebut reassembly. Karena setiap fragmen dimulai dengan salinan header datagram asli†, semua fragmen memiliki alamat tujuan yang sama dengan datagram asli tempat mereka diturunkan. Fragmen yang membawa potongan data terakhir memiliki bit tambahan yang ditetapkan di header. Dengan demikian, host yang melakukan reassembly dapat mengetahui apakah semua fragmen telah berhasil tiba. Menariknya, IP menetapkan bahwa tujuan akhir harus merakit kembali fragmen. Sebagai contoh, perhatikan konfigurasi pada Gambar 3.8.



Gambar 3.8 Ilustrasi tiga jaringan yang dihubungkan oleh dua router.

Pada gambar, jika host H1 mengirimkan datagram 1500 oktet ke host H2, router R1 akan membagi datagram menjadi dua fragmen, yang akan diteruskan ke R2. Router R2 tidak memasang kembali fragmen. Sebaliknya R2 menggunakan alamat tujuan dalam sebuah fragmen untuk meneruskan fragmen seperti biasa. Host tujuan akhir, H2, mengumpulkan fragmen, dan menyusunnya kembali untuk menghasilkan datagram asli.

Memerlukan tujuan akhir untuk merakit kembali fragmen memiliki dua keuntungan.

- Pertama, ini mengurangi jumlah informasi status di router. Saat meneruskan datagram, router tidak perlu mengetahui apakah datagram tersebut merupakan fragmen.

- Kedua, memungkinkan rute berubah secara dinamis. Jika router perantara ingin merakit kembali fragmen, semua fragmen perlu mencapai router.

Dengan menunda reassembly sampai tujuan akhir, IP bebas untuk melewatkan beberapa fragmen dari datagram sepanjang rute yang berbeda dari fragmen lainnya. Artinya, Internet dapat mengubah rute kapan saja (misalnya, untuk merutekan di sekitar kegagalan perangkat keras).

3.14 Mengumpulkan Fragmen Datagram

Ingatlah bahwa IP tidak menjamin pengiriman. Dengan demikian, fragmen individu, yang diteruskan persis seperti datagram lainnya, dapat hilang atau rusak. Lebih penting lagi, jika sumber tertentu mengirimkan beberapa datagram ke tujuan yang sama, fragmen dari beberapa datagram dapat tiba dalam urutan yang berubah-ubah.

Bagaimana perangkat lunak IP memasang kembali fragmen yang tiba tidak sesuai pesanan? Pengirim menempatkan nomor identifikasi unik di bidang IDENTIFIKASI setiap datagram keluar. Ketika router memecah datagram, router menyalin nomor identifikasi ke dalam setiap fragmen. Penerima menggunakan nomor identifikasi dan alamat sumber IP dalam fragmen yang masuk untuk menentukan datagram yang menjadi milik fragmen. Selain itu, bidang FRAGMENT OFFSET memberi tahu penerima di mana data dalam fragmen termasuk dalam datagram asli.

3.15 Konsekuensi Kehilangan Fragmen

Kami mengatakan bahwa IP tidak menjamin pengiriman fragmen — jika jaringan yang mendasari menjatuhkan paket, baik datagram atau fragmen yang dienkapsulasi dapat hilang. Datagram tidak dapat dipasang kembali sampai semua fragmen tiba. Jadi, masalah muncul ketika satu atau lebih fragmen dari datagram tiba, dan fragmen lain tertunda atau hilang. Meskipun datagram tidak dapat dipasang kembali, penerima harus menyimpan fragmen yang telah tiba jika fragmen yang hilang hanya tertunda.

Penerima tidak dapat menyimpan fragmen dalam waktu lama karena fragmen menempati ruang dalam memori. Untuk menghindari kehabisan memori, IP menentukan waktu maksimum untuk menyimpan fragmen. Ketika fragmen pertama tiba dari datagram yang diberikan, penerima memulai pengatur waktu reassembly. Jika semua fragmen datagram tiba sebelum timer berakhir, penerima membatalkan timer dan memasang kembali datagram. Namun, jika penghitung waktu berakhir sebelum semua fragmen tiba, penerima membuang fragmen yang telah tiba.

Hasil dari timer reassembly IP adalah semua atau tidak sama sekali: baik semua fragmen tiba dan IP memasang kembali datagram, atau IP membuang datagram yang tidak lengkap. Secara khusus, tidak ada mekanisme bagi penerima untuk memberi tahu pengirim fragmen mana yang telah tiba. Desainnya masuk akal karena pengirim tidak tahu tentang fragmentasi. Selanjutnya, jika pengirim melakukan retransmit datagram, rute mungkin berbeda, yang berarti pengiriman ulang tidak harus melintasi router yang sama. Oleh karena itu, tidak ada jaminan bahwa datagram yang ditransmisikan ulang akan terfragmentasi dengan cara yang sama seperti aslinya.

3.16 Memotong Fragmen

Setelah melakukan fragmentasi, router meneruskan setiap fragmen ke tujuannya. Apa yang terjadi jika sebuah fragmen akhirnya mencapai jaringan yang memiliki MTU lebih kecil? Skema fragmentasi telah direncanakan dengan hati-hati untuk memungkinkan fragmentasi fragmen. Router di sepanjang

jalur membagi fragmen menjadi fragmen yang lebih kecil. Jika jaringan diatur dalam urutan penurunan MTU, setiap router di sepanjang jalur harus memecah lebih lanjut setiap fragmen. Tentu saja, desainer bekerja dengan hati-hati untuk memastikan bahwa situasi seperti itu tidak terjadi di Internet.

Bagaimanapun, IP tidak membedakan antara fragmen asli dan subfragmen. Secara khusus, penerima tidak dapat mengetahui apakah sebuah fragmen yang masuk adalah hasil dari satu router yang memecah datagram atau beberapa router yang memecah fragmen. Keuntungan membuat semua fragmen sama adalah penerima dapat melakukan perakitan kembali datagram asli tanpa terlebih dahulu merakit kembali subfragmen. Melakukannya menghemat waktu CPU, dan mengurangi jumlah informasi yang dibutuhkan di header setiap fragmen.

3.17 Ringkasan

Protokol Internet mendefinisikan datagram IP sebagai unit dasar transfer melalui internet TCP/IP. Setiap datagram menyerupai bingkai perangkat keras karena datagram berisi header diikuti oleh area muatan. Seperti bingkai perangkat keras, header datagram berisi informasi yang digunakan untuk mentransfer datagram ke tujuan tertentu. Tidak seperti bingkai perangkat keras, header datagram berisi alamat IP daripada alamat MAC.

Perangkat lunak IP di router menggunakan tabel rute untuk menentukan hop berikutnya ke mana datagram harus dikirim. Setiap entri dalam tabel penerusan sesuai dengan satu jaringan tujuan, membuat ukuran tabel penerusan sebanding dengan jumlah jaringan di Internet. Saat memilih rute, IP membandingkan awalan jaringan dari alamat tujuan dengan setiap entri dalam tabel. Untuk menghindari ambiguitas, IP menetapkan bahwa jika tabel penerusan berisi dua entri yang cocok dengan tujuan tertentu, penerusan harus cocok dengan awalan terpanjang.

Meskipun IP memilih hop berikutnya ke mana datagram harus dikirim, alamat hop berikutnya tidak muncul di header datagram. Sebaliknya, header selalu menentukan alamat tujuan akhir.

Datagram IP dienkapsulasi dalam bingkai untuk transmisi. Setiap teknologi jaringan menentukan MTU (Maximum Transmission Unit), ukuran muatan maksimum; ketika datagram melebihi jaringan MTU, IP memecah datagram. Sebuah fragmen dapat lebih terfragmentasi, jika perlu. Tujuan akhir menyusun kembali fragmen, menggunakan pengatur waktu untuk membuang datagram jika satu atau lebih fragmen hilang.

Latihan

1. Apa dua paradigma komunikasi dasar yang dipertimbangkan desainer saat mendesain internet?
2. Bagaimana desain Internet mengakomodasi jaringan heterogen yang masing-masing memiliki format paketnya sendiri?
3. Tulis program komputer untuk mengekstrak alamat sumber dan tujuan dari datagram IP, dan mencetaknya dalam notasi desimal bertitik.
4. Tulis program untuk mengekstrak semua bidang dari header datagram IP. Cetak nilai dalam heksadesimal atau desimal bertitik yang sesuai.
5. Berapa panjang maksimum datagram IP?

6. Tulis program komputer yang memasukkan tabel penerusan IP sebagai input seperti pada Gambar 3.3b dan urutan alamat tujuan. Untuk setiap alamat tujuan, cari tabel secara berurutan untuk menemukan hop berikutnya yang benar, dan keluarkan hasilnya.
7. Jika datagram berisi satu nilai data 8-bit dan tidak ada opsi header, nilai apa yang akan ditemukan di bidang header H. LEN dan TOTAL LENGTH?
8. Jika dua prefiks dalam tabel penerusan keduanya cocok dengan alamat tujuan yang diberikan, algoritma penerusan mana yang akan digunakan?
9. Apakah alamat tujuan dalam datagram IP pernah merujuk ke router perantara? Jelaskan.
10. Asumsikan dua router salah konfigurasi untuk membentuk loop perutean untuk beberapa tujuan, D. Jelaskan mengapa datagram yang ditujukan untuk D tidak akan terus berputar selamanya.
11. Bangun gateway emulasi Internet yang secara acak menjatuhkan, menggandakan, dan menunda paket.
12. Masalah apa yang dapat terjadi saat datagram IP melewati Internet?
13. Di mana dalam sebuah bingkai datagram IP berjalan?
14. Jika seseorang menangkap datagram IP yang melewati jaringan di tengah Internet, berapa banyak frame header yang akan muncul sebelum datagram?
15. Apa yang dimaksud dengan MTU jaringan?
16. Jika suatu datagram memiliki muatan 1480 byte dan harus dikirim melalui jaringan dengan MTU 500 byte, berapa banyak fragmen yang akan dikirim? Jelaskan.
17. Di Internet, di mana fragmen dipasang kembali?
18. datagram yang sama?
19. Jika sebuah fragmen hilang, apakah penerima meminta salinan baru? Jelaskan.
20. Baca RFC 1149 dan 1217. Apakah itu standar jaringan yang serius? (Petunjuk: pertimbangkan tanggalnya.)

Bab 4 Protokol dan Teknologi Pendukung

Bab ini akan membahas tentang:

- Empat teknologi pendukung utama: pengikatan alamat, pelaporan kesalahan, bootstrap, dan terjemahan alamat.

4.1 Address Resolution

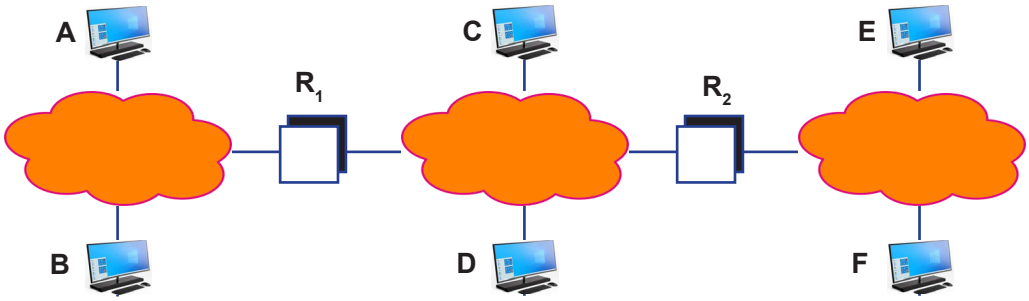
Ingat bahwa ketika datagram bergerak melintasi Internet, pengirim awal dan setiap router di sepanjang jalur menggunakan alamat IP tujuan dalam datagram untuk memilih alamat hop berikutnya, merangkum datagram dalam bingkai perangkat keras, dan mentransmisikan bingkai melintasi satu jaringan. Langkah penting dari proses penerusan memerlukan terjemahan: penerusan menggunakan alamat IP, dan bingkai yang ditransmisikan melalui jaringan fisik harus berisi alamat MAC dari hop berikutnya. Dengan demikian, perangkat lunak IP harus menerjemahkan alamat IP next-hop ke alamat MAC yang setara.

Ketika sebuah aplikasi yang mendukung teknologi protokol jaringan TCP/IP mencoba untuk mengakses sebuah host TCP/IP dengan menggunakan alamat IP, maka alamat IP yang dimiliki oleh host yang dituju harus diterjemahkan terlebih dahulu ke dalam MAC Address agar frame-frame data dapat diteruskan ke tujuan dan diletakkan di atas media transmisi (kabel, radio, atau cahaya),

Poin Penting

Alamat IP adalah abstraksi yang disediakan oleh perangkat lunak protokol. Karena perangkat keras jaringan fisik tidak tahu bagaimana menemukan komputer dari alamat IP-nya, alamat hop berikutnya harus diterjemahkan ke alamat MAC yang setara sebelum bingkai dapat dikirim.

Terjemahan dari alamat IP komputer ke alamat perangkat keras yang setara dikenal sebagai Address resolution (resolusi alamat), dan alamat IP dikatakan diselesaikan ke alamat MAC yang benar. Resolusi alamat bersifat lokal untuk jaringan. Satu komputer dapat menyelesaikan alamat komputer lain hanya jika kedua komputer terhubung ke jaringan fisik yang sama — komputer tidak pernah menyelesaikan alamat komputer di jaringan jarak jauh. Resolusi alamat selalu dibatasi untuk satu jaringan. Sebagai contoh, perhatikan internet sederhana pada Gambar 4.1.



Gambar 4.1 Contoh internet dari tiga jaringan dan komputer yang saling terhubung.

Pada gambar, jika router R1 meneruskan datagram ke router R2, router R1 akan menyelesaikan alamat IP R2 ke alamat MAC. Demikian pula, host A dan B terhubung ke jaringan fisik yang sama. Jika aplikasi pada host A mengirim data ke aplikasi pada host B, perangkat lunak protokol pada A harus menyelesaikan alamat IP B ke alamat MAC B, dan menggunakan alamat MAC untuk mengirim frame secara langsung.

Namun, jika aplikasi di host A mengirim pesan ke aplikasi di host F, yang terhubung ke jaringan jarak jauh, perangkat lunak protokol di A tidak akan mencoba menyelesaikan alamat F. Sebaliknya, perangkat lunak IP pada A menentukan bahwa paket harus berjalan melalui router R1, dan kemudian menyelesaikan alamat R1. Setelah menghitung R2 sebagai hop berikutnya, perangkat lunak IP pada R1 menyelesaikan alamat R2. Demikian pula, R2 menyelesaikan alamat F.

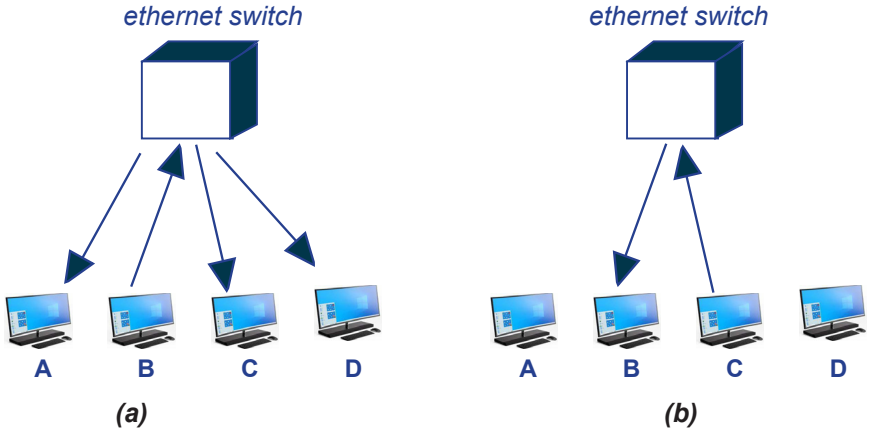
Poin Penting

Pemetaan antara alamat protokol dan alamat perangkat keras disebut resolusi alamat. Sebuah host atau router menggunakan resolusi alamat ketika perlu mengirim paket ke komputer lain di jaringan fisik yang sama. Komputer tidak pernah mencoba untuk menyelesaikan alamat komputer yang terhubung ke jaringan jarak jauh.

4.2 Address Resolution Protocol (ARP)

Algoritme apa yang digunakan perangkat lunak untuk menerjemahkan alamat protokol tingkat tinggi ke alamat yang dipahami perangkat keras? Jawabannya tergantung pada protokol dan skema pengalamatan perangkat keras. Di Internet, kami hanya peduli dengan resolusi alamat IP. Selanjutnya, karena sebagian besar perangkat keras telah mengadopsi skema pengalamatan Ethernet 48-bit, satu pendekatan untuk resolusi alamat mendominasi. Ini adalah teknik yang awalnya dirancang untuk digunakan dengan Ethernet: Address Resolution Protocol (ARP). ARP adalah sebuah protokol dalam TCP/IP Protocol Suite yang bertanggungjawab dalam melakukan resolusi alamat IP ke dalam alamat Media Access Control (MAC Address).

Ide ARP sangat mudah. Misalkan komputer B perlu menyelesaikan alamat IP komputer C. Komputer B mengirimkan permintaan yang mengatakan "Saya mencari alamat MAC komputer yang memiliki alamat IP C". Siaran hanya berjalan di satu jaringan. Ketika menerima salinan permintaan, komputer C mengirimkan balasan langsung ke B yang mengatakan, "Saya komputer dengan alamat IP C, dan alamat MAC saya adalah M". Gambar 4.2 mengilustrasikan pertukaran pesan.



Gambar 4.2 Ilustrasi pertukaran pesan ARP ketika komputer B menyelesaikan alamat komputer C.

Gambar tersebut menunjukkan bahwa meskipun pesan permintaan ARP mencapai semua komputer di jaringan, balasan tidak. Kita akan melihat bahwa pengirim memberikan informasi dalam permintaan siaran yang diterima semua komputer ketika mereka memproses permintaan tersebut.

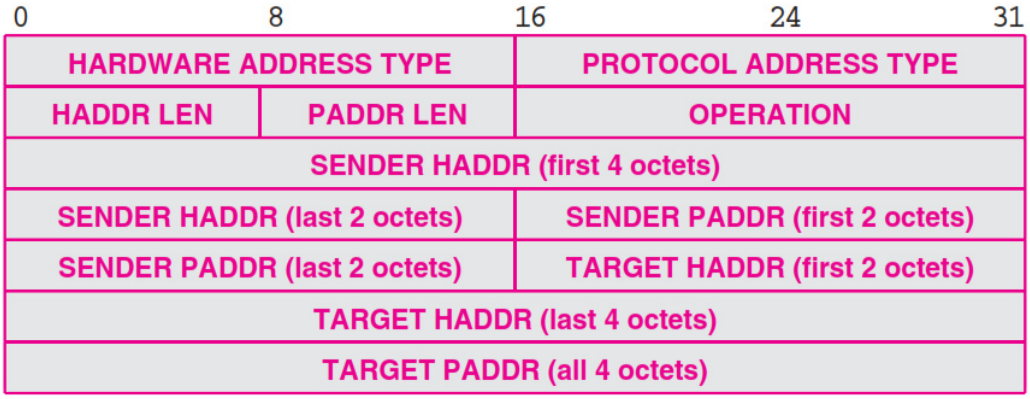
4.3 Format Pesan ARP

Daripada membatasi ARP ke IP dan Ethernet, para desainer membuat ARP menjadi umum. Jadi, alih-alih menentukan format pesan tetap, standar menggambarkan bentuk umum untuk pesan ARP, dan menentukan bagaimana format disesuaikan untuk setiap jenis alamat protokol dan setiap jenis perangkat keras jaringan. Motivasi untuk mengadaptasi pesan ARP ke perangkat keras muncul karena perancang menyadari bahwa mereka tidak dapat memilih ukuran tetap untuk alamat perangkat keras karena teknologi jaringan baru mungkin ditemukan yang memiliki alamat lebih besar dari ukuran yang dipilih. Akibatnya, para perancang menyertakan bidang ukuran tetap di awal pesan ARP untuk menentukan ukuran alamat perangkat keras yang digunakan. Misalnya, ketika ARP digunakan dengan Ethernet, panjang alamat perangkat keras diatur ke 6 oktet karena alamat Ethernet panjangnya 48 bit. Untuk meningkatkan keumuman ARP, perancang juga menyertakan bidang panjang alamat untuk alamat protokol serta untuk alamat perangkat keras. Intinya adalah bahwa ARP tidak terbatas pada alamat IP atau alamat perangkat keras tertentu — secara teori, protokol dapat digunakan untuk mengikat alamat tingkat tinggi yang sewenang-wenang ke alamat perangkat keras yang sewenang-wenang. Dalam praktiknya, ARP secara umum jarang digunakan: sebagian besar implementasi ARP digunakan untuk mengikat alamat IP ke alamat Ethernet.

Poin Penting

Meskipun format pesan ARP cukup umum untuk memungkinkan protokol sewenang-wenang dan alamat perangkat keras, ARP hampir selalu digunakan untuk mengikat alamat IP ke alamat Ethernet 48-bit.

Gambar 4.3 mengilustrasikan format pesan ARP ketika protokol digunakan dengan alamat IP versi 4 (4 oktet) dan alamat perangkat keras Ethernet (6 oktet). Setiap baris gambar sesuai dengan 32 bit pesan ARP. Paragraf berikutnya menjelaskan masing-masing bidang.

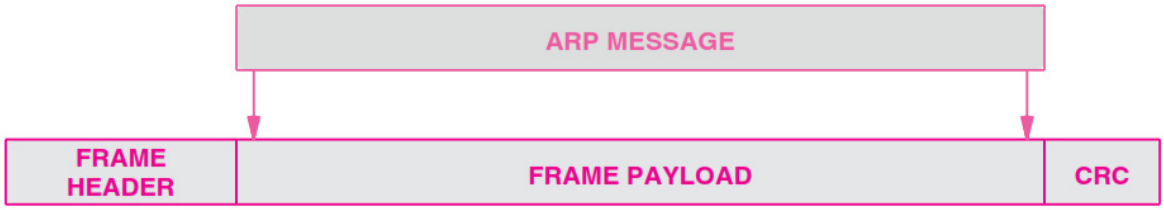


Gambar 4.3 Format pesan ARP saat mengikat alamat IPv4 ke alamat Ethernet.

- HARDWARE ADDRESS TYPE. Bidang 16-bit yang menentukan jenis alamat perangkat keras yang digunakan; nilainya adalah 1 untuk Ethernet.
- PROTOCOL ADDRESS TYPE. Bidang 16-bit yang menentukan jenis alamat protokol yang digunakan; nilainya 0x0800 untuk IPv4.
- HADDR LEN. Integer 8-bit yang menentukan ukuran alamat perangkat keras dalam byte.
- PADDR LEN. Integer 8-bit yang menentukan ukuran alamat protokol dalam byte.
- OPERATION. Bidang 16-bit yang menentukan apakah pesan adalah permintaan (bidang berisi 1) atau respons (bidang berisi 2).
- SENDER HADDR. Bidang yang diperluas untuk byte HADDR LEN dan berisi alamat perangkat keras pengirim.
- SENDER PADDR. Bidang yang diperluas untuk byte PADDR LEN dan berisi alamat protokol pengirim.
- TARGET HADDR. Bidang yang diperluas untuk byte HADDR LEN dan berisi alamat perangkat keras target.
- TARGET PADDR. Bidang yang diperluas untuk byte PADDR LEN dan berisi alamat protokol target.
- Seperti yang ditunjukkan gambar, pesan ARP berisi bidang untuk dua pengikatan alamat. Satu pengikatan sesuai dengan pengirim, dan yang lainnya sesuai dengan penerima yang dituju, yang disebut ARP sebagai target. Ketika permintaan dikirim, pengirim tidak mengetahui alamat perangkat keras target (yaitu informasi yang diminta). Oleh karena itu, field TARGET HADDR dalam permintaan ARP dapat diisi dengan nol karena isinya tidak digunakan. Sebagai tanggapan, pengikatan target mengacu pada komputer awal yang mengirim permintaan. Jadi, pasangan alamat target dalam respons tidak ada gunanya; dimasukkannya bidang target telah bertahan dari versi awal protokol.

4.4 Enkapsulasi ARP

Ketika melewati jaringan fisik, pesan ARP dienkapsulasi dalam bingkai perangkat keras. Seperti halnya IP, pesan ARP diperlakukan sebagai data yang diangkut — jaringan yang mendasarinya tidak mengurai pesan ARP atau menafsirkan bidang. Gambar 4.4 mengilustrasikan enkapsulasi ARP dalam bingkai Ethernet.



Gambar 4.4 Ilustrasi enkapsulasi ARP dalam bingkai Ethernet.

Bidang tipe di header bingkai menentukan bahwa bingkai berisi pesan ARP. Pengirim harus menetapkan nilai yang sesuai ke bidang tipe sebelum mengirimkan frame, dan penerima harus memeriksa bidang tipe di setiap frame yang masuk. Ethernet menggunakan bidang tipe 0x806 untuk menunjukkan pesan ARP. Nilai tipe yang sama digunakan untuk permintaan dan tanggapan ARP. Dengan demikian, jenis bingkai tidak membedakan antara jenis pesan ARP — penerima harus memeriksa bidang OPERASI dalam pesan untuk menentukan apakah pesan yang masuk merupakan permintaan atau tanggapan.

4.5 ARP Caching dan Pemrosesan Pesan

Meskipun ARP digunakan untuk mengikat alamat, mengirimkan permintaan ARP untuk setiap datagram tidak efisien — tiga frame melintasi jaringan untuk setiap datagram (permintaan ARP, respons ARP, dan datagram). Lebih penting lagi, karena sebagian besar komunikasi komputer melibatkan rangkaian paket, pengirim kemungkinan akan mengulangi pertukaran berkali-kali.

Untuk mengurangi lalu lintas jaringan, perangkat lunak ARP mengekstrak dan menyimpan informasi dari respons sehingga dapat digunakan untuk paket berikutnya. Perangkat lunak tidak menyimpan informasi tanpa batas. Sebagai gantinya, ARP menyimpan tabel kecil binding di memori. ARP mengelola tabel sebagai cache — entri diganti ketika respons tiba, dan entri terlama dihapus setiap kali tabel kehabisan ruang atau setelah entri tidak diperbarui untuk jangka waktu yang lama (misalnya, 20 menit) . Ketika perlu untuk mengikat alamat, ARP mulai dengan mencari cache. Jika pengikatan ada dalam cache, ARP menggunakan pengikatan tanpa mengirimkan permintaan. Jika pengikatan tidak ada dalam cache, ARP menyiarkan permintaan, menunggu respons, memperbarui cache, dan kemudian melanjutkan untuk menggunakan pengikatan.

Perhatikan bahwa tidak seperti kebanyakan skema caching, cache ARP tidak diperbarui ketika pencarian terjadi (yaitu, ketika entri direferensikan). Sebaliknya, cache hanya diperbarui ketika pesan ARP tiba melalui jaringan (baik permintaan atau tanggapan). Algoritma 4.1 menguraikan prosedur untuk menangani pesan ARP yang masuk.

Algoritma 4.1

Diberikan:
Pesan ARP masuk (baik permintaan atau tanggapan)
Lakukan:
Memproses pesan dan memperbarui cache ARP

Metode:

Ekstrak alamat IP pengirim, I, dan alamat MAC, M If (alamat I sudah ada di cache ARP) {
Ganti alamat MAC di cache dengan M
}
if (pesan adalah permintaan dan target adalah "saya") {
Tambahkan entri ke cache ARP untuk pengirim
asalkan tidak ada entri;
Menghasilkan dan mengirim tanggapan;
}

Algoritma 4.1 Langkah-langkah yang dilakukan ARP saat memproses pesan masuk.

Seperti yang ditentukan oleh algoritme, ARP melakukan dua langkah dasar untuk memproses pesan. Pertama, penerima mengekstrak pengikatan alamat pengirim dan memperbarui cache jika cache sudah berisi entri untuk pengirim. Memperbarui cache menangani kasus di mana alamat perangkat keras pengirim telah berubah. Pada langkah kedua, penerima memeriksa bidang OPERASI dari pesan untuk menentukan apakah pesan tersebut merupakan permintaan atau tanggapan. Jika pesan adalah sebuah respon, penerima harus telah mengeluarkan permintaan sebelumnya, dan menunggu pengikatan (yaitu, cache berisi entri untuk pengirim, yang diisi selama langkah pertama). Jika pesan adalah permintaan, penerima membandingkan bidang TARGET PADDR dengan alamat protokol lokal. Jika keduanya identik, komputer adalah target permintaan, dan harus mengirim respons ARP. Untuk membentuk respons, ARP memulai dengan pesan masuk, membalikkan ikatan pengirim dan target, memasukkan alamat perangkat kerasnya di bidang SENDER HADDR, dan mengubah bidang OPERASI menjadi 2, yang menunjukkan respons.

ARP berisi optimasi lebih lanjut: ketika menemukan permintaan yang harus dibalas, komputer mengekstrak pengikatan alamat pengirim dari permintaan dan menambahkan pengikatan ke cache untuk digunakan nanti. Untuk memahami optimasi, perlu diketahui dua fakta:

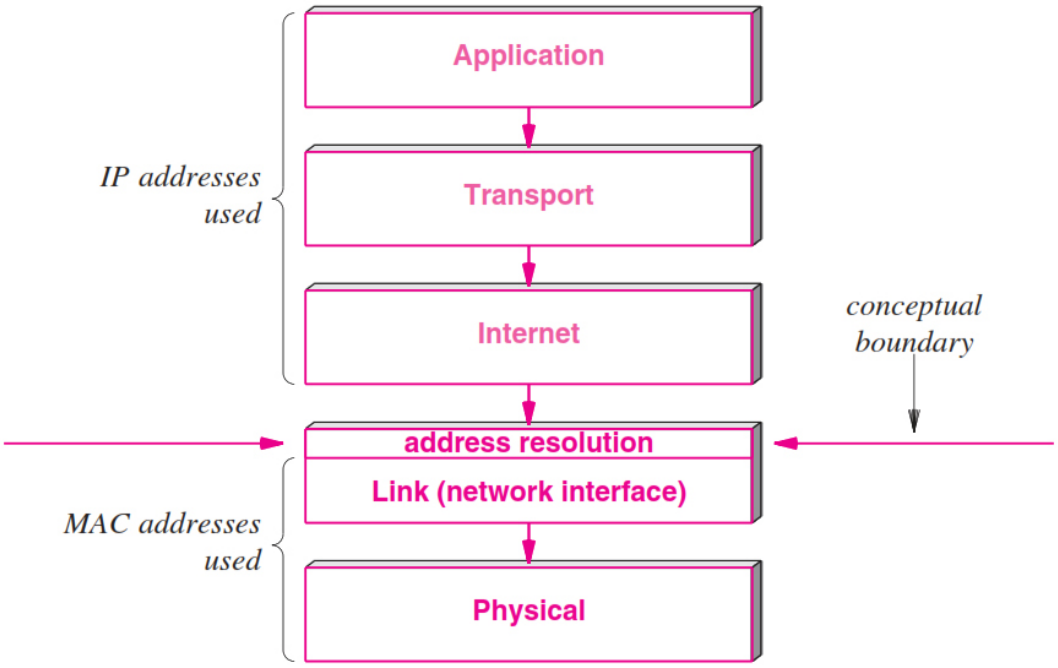
- Sebagian besar komunikasi komputer melibatkan lalu lintas dua arah — jika pesan berjalan dari A ke B, kemungkinan besar balasan akan dikirim dari B kembali ke A.
- Karena setiap pengikatan alamat memerlukan memori, komputer tidak dapat menyimpan sejumlah pengikatan alamat yang berubah-ubah.

Fakta pertama menjelaskan mengapa mengekstrak pengikatan alamat pengirim mengoptimalkan kinerja ARP. Komputer A hanya mengirim permintaan ARP untuk target B ketika A memiliki paket untuk dikirimkan ke B. Jadi, ketika B menemukan dirinya sebagai target permintaan dari A, kemungkinan besar setelah paket tiba, paket akan dikirim dari B ke A. Mengatur B untuk mengekstrak pengikatan A dari permintaan ARP yang masuk menghilangkan kebutuhan untuk permintaan ARP selanjutnya dari B ke A.

Fakta kedua menjelaskan mengapa entri cache baru hanya ditambahkan ke cache ARP oleh komputer yang menjadi target permintaan ARP dan bukan oleh komputer lain yang menerima permintaan: jika semua komputer memasukkan informasi, cache mereka akan cepat terisi, meskipun kebanyakan dari mereka tidak akan pernah berkomunikasi dengan banyak komputer di jaringan. Dengan demikian, ARP hanya mencatat binding alamat yang mungkin diperlukan.

4.6 Batas Alamat Konseptual

Ingat bahwa TCP/IP menggunakan model referensi lima lapis. Resolusi alamat adalah contoh fungsi yang terkait dengan lapisan antarmuka jaringan, (yaitu, lapisan 2). ARP memberikan batasan konseptual penting antara alamat MAC dan alamat IP: ARP menyembunyikan detail pengalamatan perangkat keras, dan memungkinkan lapisan perangkat lunak yang lebih tinggi untuk menggunakan alamat IP. Jadi, ada batasan konseptual penting yang dikenakan antara lapisan antarmuka jaringan dan semua lapisan yang lebih tinggi: aplikasi serta perangkat lunak protokol lapisan yang lebih tinggi dibangun untuk menggunakan alamat protokol. Gambar 4.5 mengilustrasikan batas pengalamatan.



Gambar 4.5 Ilustrasi batas antara penggunaan alamat IP dan alamat MAC.

Poin Penting

ARP membentuk batas konseptual dalam tumpukan protokol — lapisan di atas ARP menggunakan alamat IP, dan lapisan di bawah ARP menggunakan alamat MAC.

4.7 Internet Control Message Protocol (ICMP)

Kami mengatakan bahwa IP mendefinisikan layanan komunikasi upaya terbaik di mana datagram dapat hilang, digandakan, tertunda, atau dikirim rusak. Tampaknya layanan upaya terbaik tidak memerlukan deteksi kesalahan. Penting untuk disadari, bagaimanapun, bahwa layanan upaya terbaik bukannya ceroboh — IP berupaya menghindari kesalahan dan melaporkan masalah saat terjadi. Faktanya, kita telah melihat satu contoh deteksi kesalahan dalam IP: header checksum yang digunakan untuk mendeteksi kesalahan transmisi. Saat host membuat datagram IP, host menyertakan checksum yang mencakup seluruh header. Setiap kali datagram diterima, checksum diverifikasi untuk memastikan bahwa header tiba dengan utuh. Demikian pula, header IP berisi bidang TIME TO LIVE yang digunakan untuk mencegah datagram beredar selamanya jika tabel penerusan di router salah memperkenalkan jalur melingkar.

Tindakan yang diambil dalam menanggapi kesalahan checksum sangat mudah: datagram harus segera dibuang tanpa pemrosesan lebih lanjut. Penerima tidak dapat mempercayai bidang apa pun di header datagram karena penerima tidak dapat mengetahui bit mana yang diubah. Secara khusus, penerima tidak dapat mengirim pesan kesalahan kembali ke komputer yang mengirim datagram karena penerima tidak dapat mempercayai alamat sumber di header. Dengan demikian, penerima tidak memiliki pilihan selain membuang datagram yang rusak.

Untuk masalah yang lebih ringan daripada kesalahan checksum, IP menyertakan protokol pendamping, Internet Control Message Protocol (ICMP), yang digunakan untuk melaporkan kesalahan kembali ke sumber aslinya (yaitu, komputer yang mengirim datagram). Menariknya, IP dan ICMP saling bergantung — IP bergantung pada ICMP untuk melaporkan kesalahan, dan ICMP menggunakan IP untuk membawa pesan kesalahan. Meskipun lebih dari dua puluh pesan ICMP telah didefinisikan, hanya sedikit yang digunakan. Gambar 4.6 daftar pesan ICMP kunci dan tujuan masing-masing.

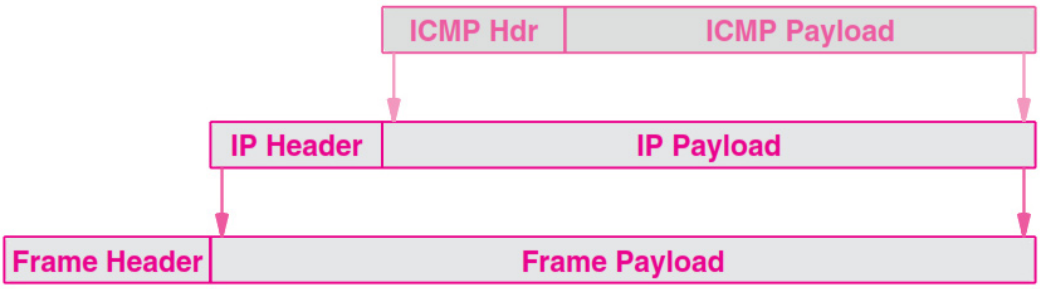
Nomor	Jenis	Tujuan
0	Echo Reply	Digunakan oleh program ping
3	Dest. Unreachable	Datagram yangu tidak dapat dikirim
5	Redirect	Host harus mengubah rute
8	Echo	Digunakan oleh program ping
11	Time Exceeded	TTL kedaluwarsa atau fragmen habis waktu
12	Parameter Problem	Masalah Header IP salah
30	Traceroute	Digunakan oleh program traceroute

Gambar 4.6 Contoh pesan ICMP dengan nomor dan tujuan pesan.

Seperti yang diilustrasikan pada gambar, ICMP berisi dua jenis pesan: pesan yang digunakan untuk melaporkan kesalahan dan pesan yang digunakan untuk memperoleh informasi. Misalnya, pesan Time Exceeded dan Destination Unreachable masing-masing melaporkan kesalahan saat datagram tidak berhasil dikirim. Alamat tujuan tidak dapat dijangkau jika tidak ada rute ke alamat tersebut; waktu datagram habis jika jumlah TTL di header kedaluwarsa atau fragmen datagram tidak tiba sebelum pengatur waktu reassembly berakhir. Sebaliknya, pesan Echo Request dan Echo Reply tidak sesuai dengan kesalahan. Sebaliknya, mereka digunakan oleh aplikasi ping untuk menguji konektivitas — ketika menerima pesan permintaan gema, perangkat lunak ICMP pada host atau router mengirimkan balasan gema yang membawa data yang sama dengan permintaan. Jadi, aplikasi ping mengirimkan permintaan ke host jarak jauh, menunggu balasan, dan menyatakan bahwa host dapat dijangkau, atau setelah batas waktu yang sesuai, menyatakan bahwa host tidak dapat dijangkau.

4.8 Format Pesan dan Enkapsulasi ICMP

ICMP menggunakan IP untuk mengangkut setiap pesan kesalahan: ketika router memiliki pesan ICMP untuk dikirim, ia membuat datagram IP dan merangkum pesan ICMP dalam datagram. Artinya, pesan ICMP ditempatkan di area muatan datagram IP. Datagram kemudian diteruskan seperti biasa, dengan datagram lengkap yang dienkapsulasi dalam bingkai untuk transmisi. Gambar 4.7 mengilustrasikan dua tingkat enkapsulasi.



Gambar 4.7 Dua tingkat enkapsulasi yang digunakan dengan pesan ICMP.

Datagram yang membawa pesan ICMP tidak memiliki prioritas khusus — mereka diteruskan seperti datagram lainnya, dengan satu pengecualian kecil. Jika datagram yang membawa pesan kesalahan ICMP menyebabkan kesalahan, tidak ada pesan kesalahan yang dikirim. Alasannya harus jelas: perancang ingin menghindari Internet menjadi padat membawa pesan kesalahan tentang pesan kesalahan.

Poin Penting

Protokol Pesan Kontrol Internet mencakup pesan tentang kesalahan dan pesan informasi. ICMP merangkum pesan dalam IP untuk transmisi, dan IP menggunakan ICMP untuk melaporkan masalah.

4.9 Perangkat Lunak Protokol, Parameter, dan Konfigurasi

Diskusi kami tentang protokol Internet telah menjelaskan operasinya setelah host atau router dihidupkan, sistem operasi telah dimulai, dan perangkat lunak protokol telah diinisialisasi. Muncul pertanyaan: bagaimana perangkat lunak protokol di host atau router mulai beroperasi? Untuk router, jawabannya biasa saja: manajer harus menentukan nilai awal untuk item seperti alamat IP untuk setiap koneksi jaringan, perangkat lunak protokol yang akan dijalankan, dan nilai awal untuk tabel penerusan. Konfigurasi disimpan di disk, dan router memuat nilai selama startup.

Konfigurasi host lebih kompleks, dan biasanya menggunakan proses dua langkah yang dikenal sebagai bootstrap†. Langkah pertama terjadi saat komputer melakukan booting. Sistem operasi mengisi satu set dasar parameter konfigurasi yang memungkinkan perangkat lunak protokol untuk berkomunikasi melalui jaringan lokal. Pada langkah kedua, perangkat lunak protokol mengisi informasi tambahan seperti alamat IP komputer, topeng alamat, dan alamat server DNS lokal. Intinya, perangkat lunak protokol terdiri dari gambar biner yang diparameterisasi, dan inisialisasi mengisi serangkaian parameter. Dengan demikian, citra biner yang sama dapat digunakan pada banyak komputer, dan citra tidak perlu diubah jika koneksi jaringan komputer berubah. Kami mengatakan bahwa perangkat lunak protokol dapat dikonfigurasi untuk situasi tertentu.

Poin Penting

Perangkat lunak protokol diparameterisasi untuk memungkinkan gambar biner yang dikompilasi berjalan di banyak komputer di berbagai lingkungan jaringan tanpa perubahan. Ketika salinan perangkat lunak dimulai pada komputer tertentu, itu harus dikonfigurasi dengan mengatur satu set parameter yang memasok informasi tentang komputer dan jaringan yang terhubung.

4.10 Dynamic Host Configuration Protocol (DHCP)

Berbagai mekanisme telah dibuat untuk memungkinkan komputer host mendapatkan parameter. Mekanisme awal yang dikenal sebagai Reverse Address Resolution Protocol (RARP) memungkinkan komputer untuk mendapatkan alamat IP dari server. ICMP, dijelaskan di atas, termasuk pesan Address Mask Request dan Router Discovery yang dapat memperoleh address mask yang digunakan pada jaringan tertentu dan alamat router. Masing-masing mekanisme awal digunakan secara independen, permintaan disiarkan dan host biasanya mengonfigurasi lapisan dari terendah ke tertinggi.

Dalam evolusi protokol Internet, protokol tunggal diciptakan untuk memungkinkan host memperoleh beberapa parameter dengan satu permintaan. Dikenal sebagai Bootstrap Protocol (BOOTP), mekanisme menyediakan alamat IP komputer, topeng alamat yang akan digunakan, dan alamat router default. Jadi, dalam satu langkah, sebuah host dapat memperoleh sebagian besar informasi yang diperlukan untuk mengonfigurasi tumpukan IP yang berfungsi.

Seperti protokol konfigurasi lainnya, BOOTP mengatur host untuk menyiarkan permintaan. Namun, tidak seperti protokol konfigurasi lainnya, BOOTP menggunakan IP untuk berkomunikasi dengan server — permintaan dikirim ke Alamat Tujuan all-1, dan menggunakan semua-0 sebagai Alamat Sumber. Server BOOTP menggunakan alamat MAC pada frame masuk untuk mengirim respons melalui unicast. Dengan demikian, sebuah host yang tidak mengetahui alamat IP-nya dapat berkomunikasi dengan server BOOTP.

Versi awal BOOTP menggunakan penetapan alamat tetap di mana server memiliki database alamat IP yang ditetapkan untuk setiap host. Permintaan dari host menyertakan ID unik (biasanya alamat MAC host), dan server menggunakan ID tersebut untuk menemukan alamat IP host. Intinya adalah bahwa BOOTP memerlukan administrasi manual — sebelum komputer dapat menggunakan BOOTP untuk mendapatkan alamat, administrator jaringan harus mengkonfigurasi server BOOTP untuk mengetahui alamat IP komputer.

Meskipun bekerja ketika satu set komputer tetap, spesifikasi manual tidak cukup jika satu set komputer berubah dengan cepat. Misalnya, pertimbangkan titik akses Wi-FI di kedai kopi yang menyediakan akses ke pelanggan yang sewenang-wenang. Untuk menangani kasus seperti itu, IETF memperluas BOOTP dan mengubah nama menjadi Dynamic Host Configuration Protocol (DHCP). DHCP menyediakan mekanisme yang memungkinkan komputer sewenang-wenang untuk bergabung dengan jaringan baru dan mendapatkan alamat IP secara otomatis. Konsep ini disebut jaringan plug-and-play.

Poin Penting

DHCP memungkinkan komputer untuk pindah ke jaringan baru dan memperoleh informasi konfigurasi tanpa memerlukan administrator untuk membuat perubahan manual ke database.

Faktanya, DHCP mengikuti pendekatan yang sama dengan BOOTP. Saat komputer melakukan booting, komputer mengirimkan Permintaan DHCP ke server yang mengirimkan Balasan DHCP†. Seorang administrator dapat mengkonfigurasi server DHCP untuk menyediakan dua jenis alamat: alamat yang ditetapkan secara permanen seperti yang disediakan oleh BOOTP atau kumpulan alamat dinamis yang akan dialokasikan sesuai permintaan. Biasanya, alamat permanen diberikan ke server, dan alamat dinamis diberikan ke host arbitrer. Faktanya, alamat yang diberikan berdasarkan permintaan tidak diberikan untuk jangka waktu yang sewenang-wenang. Sebaliknya, DHCP mengeluarkan sewa alamat untuk periode yang terbatas‡. Penggunaan sewa memungkinkan server DHCP untuk mendapatkan kembali alamat, jika perlu. Ketika masa sewa berakhir, server mengembalikan alamat ke kumpulan alamat yang tersedia, yang memungkinkan alamat untuk diberikan ke komputer lain. Leasing sangat penting untuk operasi server yang berkelanjutan karena memungkinkan server untuk mengontrol sumber daya dan mendapatkan kembali alamat bahkan jika host yang menyimpan alamat mengalami crash.

Ketika sewa berakhir, tuan rumah dapat memilih untuk melepaskan alamat atau bernegosiasi ulang dengan DHCP untuk memperpanjang sewa. Negosiasi terjadi bersamaan dengan aktivitas lain. Biasanya, DHCP menyetujui setiap perpanjangan sewa, dan komputer terus beroperasi tanpa gangguan untuk menjalankan program aplikasi atau komunikasi jaringan yang sedang berlangsung. Namun, server dapat dikonfigurasi untuk menolak perpanjangan sewa karena alasan administratif atau teknis. Misalnya, pertimbangkan jaringan di ruang kelas universitas. Dalam kasus seperti itu, server dapat dikonfigurasi sehingga semua sewa berakhir pada akhir periode kelas (untuk mengizinkan kumpulan alamat dipindahkan ke kelas berikutnya). DHCP memberikan kendali mutlak atas penyewaan ke server — jika server menolak permintaan perpanjangan, host harus berhenti menggunakan alamat tersebut.

4.11 Operasi dan Optimalisasi Protokol DHCP

Meskipun protokolnya sederhana, DHCP menyertakan beberapa detail penting yang mengoptimalkan kinerja. Tiga yang paling signifikan adalah:

- Pemulihan dari kehilangan atau duplikasi
- Caching alamat server
- Menghindari banjir yang disinkronkan

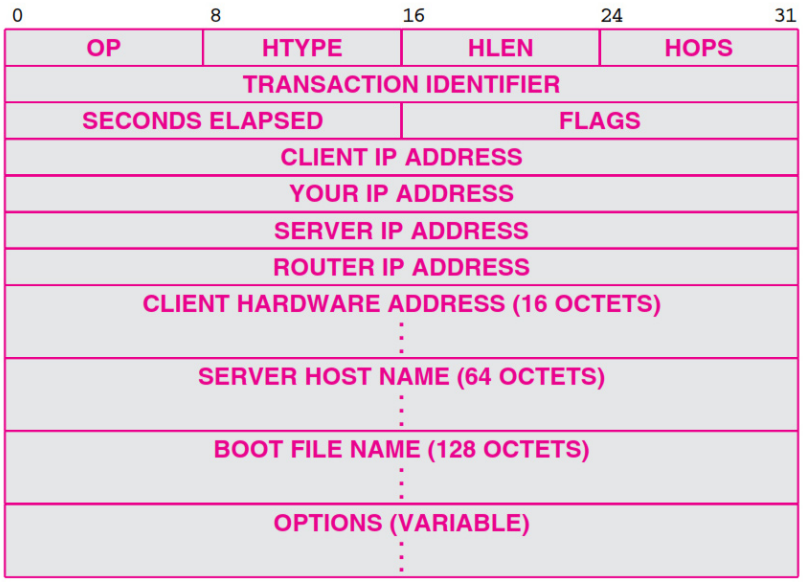
Item pertama berarti DHCP dirancang untuk memastikan bahwa paket yang hilang atau terduplikasi tidak mengakibatkan kesalahan konfigurasi — jika tidak ada respons yang diterima, host mengirimkan ulang permintaannya, dan jika respons duplikat tiba, host mengabaikan salinan tambahan. Item kedua berarti bahwa setelah sebuah host menggunakan pesan DHCP Discover untuk menemukan server DHCP, host tersebut menyimpan alamat server tersebut. Dengan demikian, perpanjangan sewa efisien.

Item ketiga berarti bahwa DCHP mengambil langkah-langkah untuk mencegah permintaan yang disinkronkan. Misalnya, permintaan yang disinkronkan mungkin terjadi jika semua komputer di jaringan melakukan boot ulang secara bersamaan setelah listrik mati. Untuk menghindari semua host di jaringan membanjiri server DHCP dengan permintaan simultan, DHCP mengharuskan setiap host untuk menunda waktu acak sebelum mengirimkan (atau mentransmisikan ulang) permintaan.

4.12 Format Pesan DHCP

Karena dirancang sebagai perpanjangan dari BOOTP, DHCP mengadopsi versi format pesan BOOTP yang sedikit dimodifikasi. Gambar 4.8 mengilustrasikan format pesan DHCP. Kecuali untuk OPTIONS, setiap field dalam pesan DHCP memiliki ukuran yang tetap. Tujuh bidang pertama berisi informasi yang digunakan untuk memproses pesan. Bidang OP menentukan apakah pesan adalah Permintaan atau Respons. Untuk membedakan di antara berbagai pesan yang digunakan klien untuk menemukan server atau meminta alamat atau yang digunakan server untuk mengakui atau menolak permintaan, DHCP menyertakan OPSI untuk jenis pesan tertentu. Artinya, bidang OP memberi tahu apakah pesan tersebut berjalan dari klien ke server atau server ke klien, dan salah satu OPSI memberikan jenis pesan yang tepat.

Bidang HTYPE dan HLEN menentukan jenis perangkat keras jaringan dan panjang alamat perangkat keras. Klien menggunakan bidang BENDERA untuk menentukan apakah dapat menerima siaran atau balasan terarah. Bidang HOPS menentukan berapa banyak server yang meneruskan permintaan, dan bidang TRANSACTION IDENTIFIER memberikan nilai yang dapat digunakan klien untuk menentukan apakah respons yang masuk cocok dengan permintaannya. Bidang SECONDS ELAPSED menentukan berapa detik yang telah berlalu sejak host mulai melakukan booting. Terakhir, jika ia mengetahui alamat IP-nya (misalnya, alamat diperoleh melalui mekanisme lain daripada melalui DHCP), sebuah host mengisi bidang CLIENT IP ADDRESS dalam sebuah permintaan.



Gambar 4.8 Format pesan DHCP.

Kolom selanjutnya dalam pesan digunakan sebagai respons untuk membawa informasi kembali ke host yang mengirim permintaan. Jika sebuah host tidak mengetahui alamat IP-nya, server menggunakan bidang ALAMAT IP ANDA untuk memberikan nilainya. Selain itu, server menggunakan bidang SERVER IP ADDRESS dan SERVER HOST NAME untuk memberikan informasi host tentang lokasi server. Field ROUTER IP ADDRESS berisi alamat IP dari router default.

Selain konfigurasi protokol, DHCP memungkinkan komputer untuk bernegosiasi untuk menemukan gambar boot. Untuk melakukannya, tuan rumah mengisi bidang NAMA FILE BOOT dengan permintaan (misalnya, tuan rumah dapat meminta sistem operasi LINUX). Server DHCP tidak mengirim gambar. Sebagai gantinya, server menentukan file mana yang berisi gambar yang diminta, dan menggunakan

bidang BOOT FILE NAME untuk mengembalikan nama file. Setelah respons DHCP tiba, host harus menggunakan protokol terpisah (mis., TFTP) untuk mengunduh gambar.

4.13 Akses Server DHCP Tidak Langsung Melalui Relay

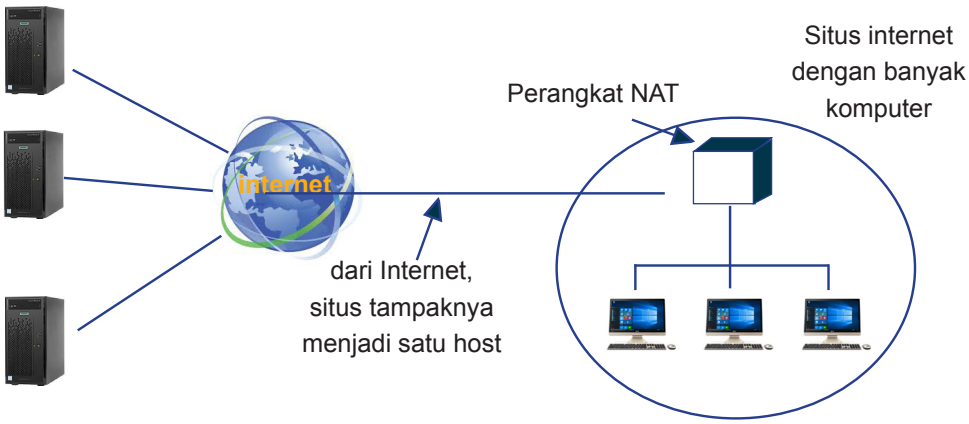
Meskipun disiarkan di jaringan lokal untuk menemukan server, DHCP tidak mengharuskan setiap jaringan individu untuk memiliki server. Sebaliknya, agen relai DHCP meneruskan permintaan dan tanggapan antara klien dan server. Setidaknya satu agen relai harus ada di setiap jaringan, dan agen relai harus dikonfigurasi dengan alamat server DHCP yang sesuai. Saat server merespons, agen relai meneruskan respons ke klien.

Tampaknya menggunakan beberapa agen relai tidak lebih baik daripada menggunakan beberapa server DHCP. Namun, manajer jaringan lebih memilih untuk mengelola beberapa agen relai karena dua alasan. Pertama, dalam jaringan dengan satu server DHCP dan beberapa agen relai, administrasi alamat dipusatkan ke dalam satu perangkat. Dengan demikian, manajer jaringan tidak perlu berinteraksi dengan banyak perangkat untuk mengubah kebijakan sewa atau menentukan status saat ini. Kedua, banyak router komersial berisi mekanisme yang menyediakan layanan relai DHCP di semua jaringan yang terhubung dengan router. Selain itu, fasilitas agen relai di router biasanya mudah dikonfigurasi (konfigurasi terdiri dari mengaktifkan penerusan dan menentukan alamat server DHCP), dan konfigurasi tidak mungkin berubah.

4.14 Network Address Translation (NAT)

Ketika Internet tumbuh dan alamat menjadi langka, pengalamatan subnet dan tanpa kelas (CIDR) diperkenalkan untuk membantu menghemat alamat†. Mekanisme ketiga ditemukan yang memungkinkan beberapa komputer di sebuah situs untuk berbagi satu alamat IP yang valid secara global. Dikenal sebagai Network Address Translation (NAT), teknologi menyediakan komunikasi transparan dalam arti bahwa sebuah host di situs tersebut tampaknya memiliki koneksi Internet normal, dan sebuah host di Internet selalu muncul untuk menerima komunikasi dari satu komputer daripada dari satu komputer. dari banyak komputer di situs. Artinya, host di situs menjalankan perangkat lunak dan aplikasi TCP/IP konvensional, dan berkomunikasi melalui Internet seperti biasa.

NAT berjalan sebagai layanan in-line, yang berarti bahwa NAT harus ditempatkan pada koneksi antara Internet dan sebuah situs. Meskipun NAT secara konseptual terpisah dari fasilitas dan layanan lain, sebagian besar implementasi menanamkan NAT di perangkat lain seperti titik akses nirkabel Wi-Fi atau router Internet. Gambar 4.9 mengilustrasikan pengaturan tipikal situs yang menggunakan NAT.



Gambar 4.9 Arsitektur konseptual yang digunakan dengan NAT.

4.15 Operasi NAT dan Alamat Pribadi

Tujuan NAT adalah untuk memberikan ilusi. Jika dilihat dari Internet, situs tampaknya terdiri dari satu komputer host yang telah diberi alamat IP yang valid — semua datagram yang dikirim dari situs tampaknya berasal dari satu host, dan semua datagram yang dikirim ke situs tampaknya dikirim ke satu host. Jika dilihat dari host di situs, Internet tampaknya menerima dan merutekan alamat pribadi. Tentu saja, satu alamat IP tidak dapat ditetapkan ke banyak komputer — jika dua atau lebih komputer menggunakan alamat yang sama, konflik akan muncul karena banyak komputer akan merespons permintaan ARP. Jadi, untuk memastikan kebenarannya, setiap komputer di jaringan tertentu harus diberi alamat IP yang unik. NAT memecahkan masalah dengan menggunakan dua jenis alamat. Perangkat NAT itu sendiri diberi satu alamat IP yang valid secara global seolah-olah perangkat NAT adalah host di Internet. Setiap komputer di situs diberi alamat pribadi yang unik, juga dikenal sebagai alamat yang tidak dapat dirutekan. Gambar 4.10 mencantumkan blok alamat yang ditetapkan IETF sebagai private.

Deskripsi	Blok
10.0.0.0/8	Blok alamat pribadi Kelas A
169.254.0.0/16	Blok alamat pribadi Kelas B
172.16.0.0/12	16 blok Kelas B yang berdekatan
192.168.0.0/16	256 blok Kelas C yang berdekatan

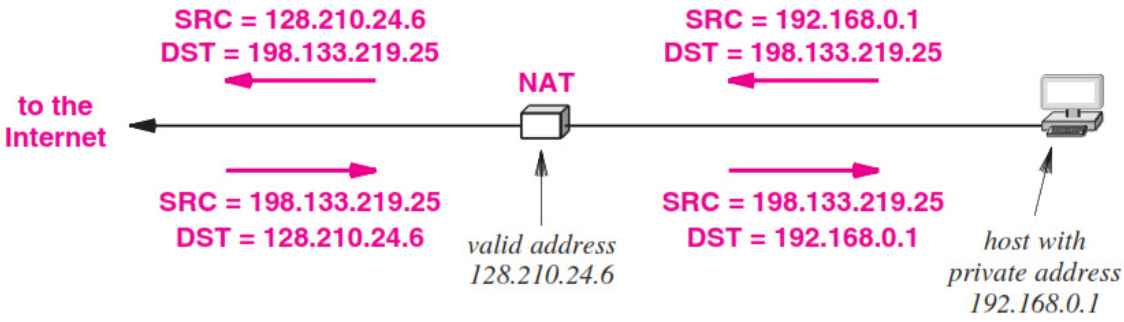
Gambar 4.10 Blok alamat pribadi (tidak dapat dirutekan) yang digunakan oleh NAT.

Sebagai contoh, asumsikan perangkat NAT tertentu menggunakan blok alamat 192.168.0.0 untuk menetapkan alamat pribadi ke host di dalam situs. Untuk memastikan bahwa setiap alamat dalam situs adalah unik (yaitu, untuk mencegah konflik), host mungkin diberi alamat

192.168.0.1, 192.168.0.2, dan seterusnya.

Sayangnya, alamat pribadi tidak valid di Internet global, dan router di Internet dikonfigurasikan untuk menolak datagram yang menentukan alamat yang tidak dapat dirutekan. Jadi, pengalamatan pribadi hanya digunakan di dalam situs — sebelum datagram dari situs dapat diizinkan ke Internet, NAT harus menerjemahkan alamat IP pribadi menjadi alamat IP yang valid secara global. Demikian pula, NAT harus menerjemahkan alamat IP yang valid secara global dalam paket masuk ke alamat pribadi sebelum mentransfer datagram ke host di situs.

Bentuk paling dasar dari NAT menerjemahkan alamat sumber sebagai datagram lewat dari situs ke Internet dan alamat tujuan sebagai datagram lewat dari Internet ke situs. Misalnya, asumsikan bahwa perangkat NAT telah diberi alamat IP yang valid secara global 128.210.24.6, dan pertimbangkan terjemahan yang terjadi jika host dengan alamat pribadi 192.168.0.1 mengirimkan datagram ke host di Internet dengan alamat 198.133.219.25 dan menerima balasan. Gambar 4.11 mengilustrasikan translasi yang terjadi di setiap arah.



Gambar 4.11 Ilustrasi terjemahan NAT dasar yang mengubah alamat sumber datagram keluar dan alamat tujuan datagram masuk.

Poin Penting

Bentuk paling dasar dari NAT menggantikan alamat sumber IP dalam datagram yang lewat dari situs ke Internet, dan menggantikan alamat tujuan IP dalam datagram yang lewat dari Internet ke situs.

Sebagian besar implementasi NAT menggunakan tabel terjemahan untuk menyimpan informasi yang diperlukan untuk menulis ulang alamat. Misalnya, Gambar 4.12 menunjukkan tabel terjemahan yang sesuai dengan pemetaan alamat pada Gambar 4.11.

Direction	Bidang	Lama	Baru
Out	Sumber IP	192.168.0.1	128.210.24.6
	IP Tujuan	198.133.219.25	-- tidak ada perubahan --
In	Sumber IP	198.133.219.25	-- tidak ada perubahan --
	IP Tujuan	128.210.24.6	192.168.0.1

Gambar 4.12 Contoh tabel terjemahan NAT untuk pemetaan pada Gambar 4.11.

Bagaimana nilai ditempatkan dalam tabel terjemahan? Meskipun nilai dapat dikonfigurasi secara manual oleh administrator sistem, sebagian besar sistem NAT beroperasi secara otomatis. Artinya, NAT menempatkan entri dalam tabel terjemahan setiap kali host di situs mengirimkan paket ke Internet. Misalnya, ketika komputer 192.168.0.1 pertama kali mengirim datagram ke tujuan 198.133.219.25, NAT menambahkan entri ke tabelnya. Kemudian, ketika menerima balasan dari 198.133.219.25, NAT menemukan entri dalam tabel, dan menerjemahkan alamat tujuan ke 192.168.0.1.

4.16 Transport-Layer NAT (NAPT)

Versi dasar NAT yang dijelaskan di atas hanya menangani situasi di mana setiap host di situs berkomunikasi dengan server unik di Internet. Jika dua host di situs mencoba untuk berkomunikasi dengan server jauh, X, tabel terjemahan akan berisi beberapa entri untuk X, dan NAT tidak akan dapat merutekan datagram yang masuk. Basic NAT juga gagal dalam situasi ketika dua atau lebih aplikasi yang berjalan pada host tertentu di situs mencoba komunikasi simultan dengan tujuan yang berbeda di Internet.

Variasi NAT yang paling banyak digunakan menangani kedua masalah: memungkinkan sebuah situs untuk memiliki sejumlah aplikasi yang berjalan pada host yang berubah-ubah, semuanya berkomunikasi secara simultan dengan tujuan yang berubah-ubah di seluruh Internet. Meskipun secara teknis dikenal sebagai Network Address and Port Translation (NAPT), mekanisme ini sangat populer sehingga sebagian besar profesional jaringan menganggap istilah NAT berarti NAPT.

Kunci untuk memahami NAPT adalah mengingat bahwa aplikasi menggunakan nomor port protokol untuk membedakan layanan. Secara khusus, Bab 25 dan 26 menjelaskan protokol transport UDP dan TCP yang masing-masing menggunakan nomor port. Selain menyimpan tabel alamat sumber dan tujuan, NAPT menggunakan nomor port untuk mengaitkan setiap datagram dengan aliran TCP atau UDP. Artinya, alih-alih berhenti di lapisan IP, NAPT beroperasi pada header lapisan transport. Akibatnya, entri dalam tabel terjemahan yang digunakan oleh NAPT berisi 4-tupel alamat IP sumber dan tujuan serta nomor port protokol.

Misalnya, pertimbangkan tabel terjemahan yang mungkin dihasilkan jika browser di komputer 192.168.0.1 dan browser di komputer 192.168.0.2 masing-masing menggunakan port lokal 30000, dan masing-masing membentuk koneksi TCP ke server web di port 80 melalui perangkat NAPT yang menggunakan alamat 128.10.24.6. Untuk menghindari konflik, NAPT harus memilih port sumber TCP alternatif untuk koneksi. Gambar 4.13 menunjukkan satu kemungkinan.

Direction	Bidang	Lama	Baru
Out	IP SRC: TCP SRC	192.168.0.1:30000	128.10.24.6:40001
Out	IP SRC:TCP SRC	192.168.0.2 :30000	128.10.24.6 :40002
In	IP DEST:TCP DEST	128.10.19.20 :40001	192.168.0.1 :30000
In	IP DEST:TCP DEST	128.10.19.20 :40002	192.168.0.2 :30000

Gambar 4.13 Contoh tabel terjemahan NAPT untuk dua koneksi TCP ke server web yang sama.

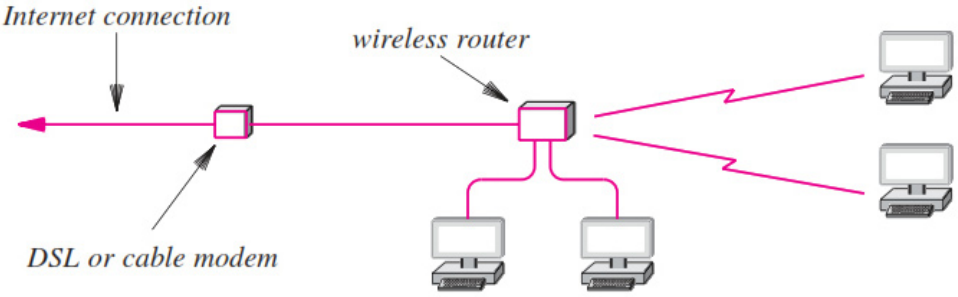
Pada gambar, aplikasi pada kedua komputer lokal menggunakan port lokal 3000. Karena sistem operasi berputar melalui nomor port, tidak mungkin memiliki dua nomor port yang identik. Namun, NAPT menangani kasus ekstrem seperti itu tanpa kebingungan. Dalam contoh, NAPT memilih port 40001 untuk satu koneksi dan 40002 untuk koneksi lainnya.

4.17 NAT dan Server

Kami mengatakan bahwa sistem NAT membangun tabel terjemahan secara otomatis dengan melihat lalu lintas keluar dan membuat pemetaan baru setiap kali aplikasi di situs memulai komunikasi. Sayangnya, konstruksi tabel otomatis tidak berfungsi dengan baik untuk komunikasi yang dimulai dari Internet ke situs. Misalnya, jika beberapa komputer di situs masing-masing menjalankan server web, perangkat NAT tidak dapat mengetahui komputer mana yang harus menerima koneksi web masuk. Varian NAT yang disebut Twice NAT telah dibuat untuk memungkinkan situs menjalankan beberapa server. Dua kali NAT mengatur sistem NAT untuk berinteraksi dengan server Sistem Nama Domain situs. Saat aplikasi di Internet mencari nama domain komputer di situs, server DNS di situs mengembalikan alamat IP valid yang telah ditetapkan ke perangkat NAT, dan juga membuat entri baru di tabel terjemahan NAT. Jadi, tabel terjemahan diinisialisasi sebelum paket pertama tiba. Meskipun tidak elegan, Twice NAT berfungsi untuk sebagian besar kasus. Namun, dua kali NAT gagal, jika aplikasi klien menggunakan alamat IP secara langsung tanpa melakukan pencarian nama domain atau jika klien menggunakan proxy DNS untuk menyelesaikan nama domain.

4.18 Perangkat Lunak dan Sistem NAT untuk Penggunaan Rumahan

NAT sangat berguna di tempat tinggal atau usaha kecil yang memiliki koneksi broadband karena memungkinkan satu set komputer untuk berbagi koneksi tanpa mengharuskan pelanggan untuk membeli alamat IP tambahan dari ISP. Selain perangkat lunak yang memungkinkan PC bertindak sebagai perangkat NAT untuk PC tambahan, sistem perangkat keras NAT khusus tersedia dengan biaya rendah. Sistem seperti ini biasanya disebut router nirkabel. Misalnya, Linksys menjual sistem khusus yang menyediakan NAT di antara empat kabel Ethernet dan koneksi nirkabel Wi-Fi. Gambar 4.14 mengilustrasikan bagaimana router tersebut terhubung.



Gambar 4.14 Ilustrasi koneksi untuk router nirkabel.

4.19 Ringkasan

IP menggunakan Address Resolution Protocol, ARP, untuk mengikat alamat IP next-hop ke alamat MAC yang setara. ARP mendefinisikan format pesan yang ditukar komputer untuk menyelesaikan alamat, enkapsulasi, dan aturan untuk menangani pesan ARP. Karena pengalamatan perangkat keras berbeda di antara jaringan, ARP hanya menentukan pola umum untuk format pesan dan memungkinkan detailnya ditentukan oleh skema pengalamatan MAC. ARP menetapkan bahwa komputer harus menyiarkan pesan permintaan, tetapi tanggapan harus diarahkan. Selanjutnya, ARP menggunakan caching untuk menghindari pengiriman permintaan untuk setiap paket.

Protokol Internet mencakup mekanisme pelaporan kesalahan pendamping yang dikenal sebagai Internet Control Message Protocol (ICMP). Router menggunakan ICMP ketika datagram tiba dengan nilai yang salah di bidang header atau ketika datagram tidak dapat dikirimkan. Pesan ICMP selalu dikirim kembali ke sumber asli datagram, tidak pernah ke router perantara. Selain pesan yang melaporkan kesalahan, ICMP menyertakan pesan informasi seperti pesan Echo Request dan Echo Reply yang digunakan oleh aplikasi ping. Setiap jenis pesan ICMP memiliki format yang unik; bidang tipe di header memungkinkan penerima untuk membagi pesan yang diberikan ke dalam bidang yang sesuai. Pesan ICMP dienkapsulasi dalam datagram IP untuk transmisi.

Awalnya, protokol terpisah digunakan untuk mendapatkan setiap parameter konfigurasi yang diperlukan saat startup. Dynamic Host Configuration Protocol (DHCP), yang memperluas Bootstrapping Protocol (BOOTP), memungkinkan host untuk mendapatkan semua informasi yang diperlukan dengan satu permintaan. Respons DHCP dapat memberikan alamat IP, alamat router default, dan alamat server nama. Ketika mengalokasikan alamat IP secara otomatis, DCHP menawarkan host sewa di mana alamat dapat digunakan. Setelah masa sewa berakhir, tuan rumah harus memperpanjang masa sewa, atau berhenti menggunakan alamat.

Mekanisme NAT memungkinkan sebuah situs untuk memiliki beberapa komputer menggunakan Internet melalui satu alamat IP. NAT menulis ulang bidang header di setiap datagram yang dikirimkan ke Internet atau ke situs. Untuk aplikasi klien, terjemahan NAT dapat dibuat secara otomatis ketika perangkat NAT menemukan paket keluar pertama dari komunikasi. Beberapa variasi NAT ada. Bentuk yang paling populer, NAPT, beroperasi pada header transport-layer, dan menerjemahkan nomor port protokol serta alamat IP. NAPT memungkinkan sejumlah aplikasi yang berjalan pada komputer yang berubah-ubah dalam sebuah situs untuk berkomunikasi dengan tujuan yang berubah-ubah di Internet secara bersamaan.

Latihan

1. Saat router menggunakan tabel penerusan untuk mencari alamat hop berikutnya, hasilnya adalah IP alamat. Apa yang harus terjadi sebelum datagram dapat dikirim?
2. Istilah apa yang digunakan untuk menggambarkan pemetaan antara alamat protokol dan alamat perangkat keras?
3. Apakah ARP dapat digunakan pada jaringan yang tidak menyediakan broadcast? Mengapa atau mengapa tidak?
4. Berapa oktet yang ditempati oleh pesan ARP saat digunakan dengan alamat IP dan Ethernet?
5. Bagaimana komputer mengetahui apakah frame yang datang berisi datagram IP atau Pesan ARP?
6. Misalkan komputer menerima dua balasan ARP untuk satu permintaan. Balasan pertama mengklaim bahwa alamat MAC adalah M1, dan balasan kedua mengklaim bahwa alamat MAC adalah M2. Bagaimana ARP menangani balasan?
7. Kapan Algoritma 4.1 membuat entri baru di cache ARP?
8. Jenis alamat apa yang digunakan pada lapisan di bawah ARP?
9. Jika datagram memiliki nilai yang salah di salah satu bidang header, pesan kesalahan ICMP mana yang akan diterima?
10. Apa perbedaan utama antara BOOTP dan DHCP?
11. Jika ada loop perutean, pesan kesalahan ICMP mana yang akan dikirim? Jelaskan prosesnya.
12. Misalkan pengguna menetapkan alamat broadcast terarah sebagai tujuan ping. Hasil apa yang mungkin? Menjelaskan.
13. Beberapa versi program traceroute mengirim pesan ICMP dan yang lain mengirim pesan UDP. Bereksperimenlah dengan versi di komputer Anda untuk menentukan versi mana yang dikirim.
15. Untuk mengoptimalkan reassembly, beberapa versi sistem operasi Linux mengirim fragmen terakhir dari datagram IP terlebih dahulu, kemudian mengirim fragmen yang tersisa secara berurutan. Jelaskan mengapa pengiriman fragmen terakhir terlebih dahulu tidak bekerja dengan baik dengan NAPT.
16. Saat menggunakan perute nirkabel, apa kemungkinan alamat IP yang dapat diberikan ke host?
17. Diberikan bingkai Ethernet, bidang apa yang perlu diperiksa oleh host untuk menentukan apakah bingkai berisi pesan ICMP?
18. Buat daftar informasi jaringan utama yang dapat dikonfigurasi saat komputer melakukan booting.
19. Beberapa aplikasi jaringan menunda konfigurasi hingga layanan diperlukan. Misalnya, komputer dapat menunggu hingga pengguna mencoba mencetak dokumen sebelum perangkat lunak mencari printer yang tersedia. Apa keuntungan utama dari konfigurasi yang ditangguhkan? Kerugian utama?

20. DHCP mengizinkan server untuk ditempatkan di jaringan jarak jauh. Bagaimana komputer bisa mengirim pesan DHCP ke server di jaringan lain?
21. Sebagai alternatif dari DHCP, buatlah algoritma terdistribusi yang mengimplementasikan skema penawaran. Asumsikan bahwa satu salinan algoritme akan berjalan di setiap komputer, dan minta algoritme menetapkan setiap komputer alamat host yang unik.
22. Apa tujuan utama dari NAT?
23. Banyak perangkat NAT memilih blok alamat 10.0.0.0 /8 dari Gambar 4.10 karena memberikan yang paling umum. Jelaskan mengapa.
24. Pada Gambar 4.11, ISP telah menetapkan satu alamat IP ke situs. Yang merupakan alamat yang ditetapkan?
25. Informasi penting apa yang digunakan oleh NAPT tidak tersedia di sebagian besar fragmen IP?

Bab 5 IP Masa Depan (IPv6)

Bab ini akan membahas tentang:

- Masa depan Protokol Internet
- Menilai kekuatan dan keterbatasan versi IP saat in
- Mempertimbangkan versi baru IP yang telah dikembangkan IETF
- Fitur-fitur versi baru, dan menunjukkan bagaimana fitur-fitur tersebut mengatasi beberapa keterbatasan versi saat ini.

5.1 Keberhasilan IP

Versi IP saat ini sangat berhasil. IP telah memungkinkan Internet untuk menangani jaringan yang heterogen, perubahan dramatis dalam teknologi perangkat keras, dan peningkatan skala yang ekstrem. Protokol Internet menyediakan satu set abstraksi yang memungkinkan aplikasi untuk berkomunikasi tanpa pengetahuan tentang arsitektur Internet atau perangkat keras yang mendasarinya. Untuk mengakomodasi perangkat keras yang heterogen, IP mendefinisikan skema pengalamatan jaringan-independen, format datagram, enkapsulasi, dan strategi fragmentasi.

Fleksibilitas dan skalabilitas IP terlihat dari aplikasi yang menggunakan IP dan dari ukuran Internet global. Lebih penting lagi, IP telah mengakomodasi perubahan dramatis dalam perangkat keras. Meskipun didefinisikan sebelum teknologi jaringan area lokal menjadi populer, desain protokol asli terus bekerja dengan baik melalui beberapa generasi teknologi. Selain kecepatan data yang lebih tinggi, IP telah mengakomodasi peningkatan ukuran frame.

Poin Penting

Keberhasilan versi IP saat ini luar biasa — protokolnya telah mengakomodasi perubahan dalam teknologi perangkat keras, jaringan yang heterogen, dan skala yang sangat besar.

5.2 Motivasi untuk Perubahan

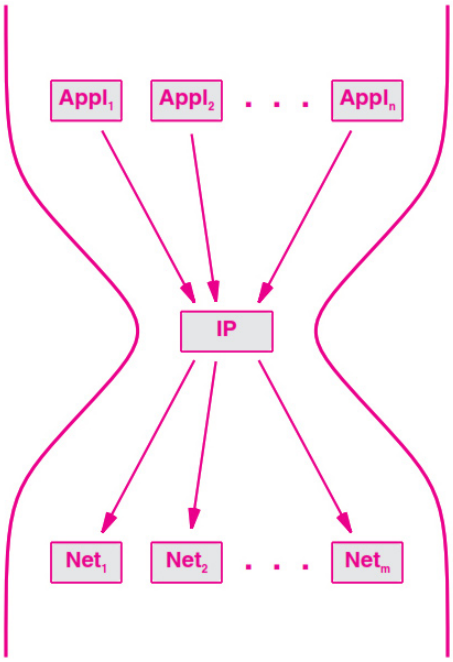
Jika IP bekerja dengan baik, mengapa berubah? Ketika IP didefinisikan, hanya beberapa jaringan komputer yang ada. Perancang memutuskan untuk menggunakan 32 bit untuk alamat IP karena hal itu memungkinkan Internet untuk memasukkan lebih dari satu juta jaringan. Namun, Internet global tumbuh secara eksponensial, dengan ukuran dua kali lipat dalam waktu kurang dari setahun. Pada tingkat pertumbuhan saat ini, setiap awalan jaringan yang mungkin pada akhirnya akan ditetapkan, dan tidak ada pertumbuhan lebih lanjut yang mungkin. Dengan demikian, motivasi utama untuk mendefinisikan versi baru IP muncul dari batasan ruang alamat — alamat yang lebih besar diperlukan untuk mengakomodasi pertumbuhan Internet yang berkelanjutan.

Motivasi sekunder untuk perubahan IP muncul dari persepsi bahwa fasilitas khusus diperlukan untuk beberapa aplikasi. Akibatnya, berbagai kelompok berpendapat bahwa ketika IP diganti, versi baru harus memiliki lebih banyak fitur. Misalnya, pertimbangkan aplikasi yang mengirim audio dan video real-time. Aplikasi tersebut mengirimkan data secara berkala, dan membutuhkan jaminan jitter yang rendah. Sayangnya, perubahan rute biasanya mengubah latensi ujung ke ujung, yang berarti peningkatan jitter. Meskipun header datagram IP saat ini menyertakan bidang yang dapat digunakan untuk meminta jenis layanan, protokol tidak mendefinisikan layanan waktu nyata. Dengan demikian, telah dikemukakan bahwa versi baru dari IP harus menyediakan mekanisme yang memungkinkan datagram membawa lalu lintas waktu nyata untuk menghindari perubahan rute.

Kelompok lain berpendapat bahwa versi baru IP harus mengakomodasi kemampuan pengalamatan dan perutean yang lebih kompleks. Secara khusus, seharusnya dimungkinkan untuk mengonfigurasi pengalamatan IP dan perutean untuk menangani layanan yang direplikasi. Misalnya, Google mengelola banyak pusat data di seluruh dunia. Ketika pengguna memasukkan google.com ke dalam browser, kelompok berpendapat, akan bermanfaat jika IP meneruskan datagram ke pusat data Google terdekat. Selain itu, banyak aplikasi saat ini memungkinkan sekumpulan pengguna untuk berkolaborasi. Untuk membuat kolaborasi menjadi efisien, Internet memerlukan mekanisme yang memungkinkan grup dibuat atau diubah dan cara untuk mengirim salinan paket ke setiap peserta dalam grup tertentu.

5.3 Model Jam Pasir dan Kendala Perubahan

Meskipun kelangkaan alamat yang tersisa dianggap penting ketika pekerjaan dimulai pada versi baru IP pada tahun 1993, tidak ada keadaan darurat yang terjadi, dan IP tidak diubah. Untuk memahami alasannya, pikirkan pentingnya IP dan biaya untuk mengubahnya. Dalam hal kepentingan, IP terletak di pusat komunikasi Internet — semua aplikasi menggunakan IP, dan IP berjalan di atas semua teknologi jaringan yang mendasarinya. Profesional jaringan mengatakan bahwa komunikasi Internet mengikuti model jam pasir, dan IP itu terletak pada posisi di mana jam pasir tipis. Gambar 5.1 mengilustrasikan konsep tersebut.



Gambar 5.1 Model jam pasir komunikasi Internet dengan IP di tengah.

Poin penting muncul dari ketergantungan pada IP dan IP inersia yang diakibatkannya memperkenalkan:

> Karena IP adalah pusat dari semua komunikasi Internet, mengubah IP memerlukan perubahan ke seluruh Internet.

5.4 Nama dan Nomor Versi

Ketika peneliti mulai mengerjakan versi baru IP, mereka membutuhkan nama untuk proyek tersebut. Meminjam dari acara televisi populer, mereka memilih IP — The Next Generation, dan laporan awal menyebut protokol baru sebagai IPng. Sayangnya, banyak proposal yang bersaing dibuat untuk IPng, dan namanya menjadi ambigu.

Ketika protokol tertentu didefinisikan, perancang perlu membedakan protokol dari semua proposal lainnya. Mereka memutuskan untuk menggunakan nomor versi resmi di header protokol standar akhir. Nomor versi yang dipilih adalah kejutan. Karena nomor versi IP saat ini adalah 4, komunitas jaringan mengharapkan versi resmi berikutnya adalah 5. Namun, versi 5 telah ditetapkan ke protokol eksperimental yang dikenal sebagai ST. Akibatnya, versi baru IP menerima 6 sebagai nomor versi resminya, dan protokol tersebut dikenal sebagai IPv6. Untuk membedakannya dari IPv6, versi IP saat ini dikenal sebagai IPv4.

5.5 Fitur IPv6

IPv6 mempertahankan banyak fitur desain yang membuat IPv4 begitu sukses. Seperti IPv4, IPv6 tidak memiliki koneksi — setiap datagram berisi alamat tujuan, dan setiap datagram dirutekan secara independen. Seperti IPv4, header dalam datagram berisi jumlah hop maksimum yang dapat diambil datagram sebelum dibuang. Lebih penting lagi, IPv6 mempertahankan sebagian besar fasilitas umum yang disediakan oleh opsi IPv4.

Meskipun mempertahankan konsep dasar dari versi saat ini, IPv6 mengubah semua detail. Misalnya, IPv6 menggunakan alamat yang lebih besar dan format header datagram yang sama sekali baru. Selanjutnya, IPv6 membagi informasi header menjadi serangkaian header dengan panjang tetap. Jadi, tidak seperti IPv4, yang menempatkan informasi kunci di bidang tetap dari header dan hanya menambahkan opsi panjang variabel untuk informasi yang kurang penting, header IPv6 selalu berukuran variabel.
Fitur-fitur baru di IPv6 dapat dikelompokkan ke dalam lima kategori besar:

- Ukuran Alamat. Alih-alih 32 bit, setiap alamat IPv6 berisi 128 bit. Ruang alamat yang dihasilkan cukup besar untuk mengakomodasi pertumbuhan berkelanjutan dari Internet di seluruh dunia selama beberapa dekade.
- Format Tajuk. Header datagram IPv6 benar-benar berbeda dari header IPv4. Hampir setiap bidang di header telah diubah; sebagian sudah diganti.
- Ekstensi Header. Tidak seperti IPv4, yang menggunakan format header tunggal untuk semua datagram, IPv6 mengkodekan informasi ke dalam header terpisah. Datagram terdiri dari header IPv6 dasar diikuti oleh nol atau lebih ekstensi header, diikuti oleh data.
- Dukungan Untuk Lalu Lintas Waktu Nyata. IPv6 mencakup mekanisme yang memungkinkan menurunkan pengirim dan penerima untuk membuat jalur berkualitas tinggi melalui jaringan yang mendasarinya dan untuk mengasosiasikan datagram dengan jalur tersebut. Meskipun mekanisme ini dimaksudkan untuk digunakan dengan aplikasi audio dan video yang memerlukan jaminan kinerja tinggi, mekanisme ini juga dapat digunakan untuk mengaitkan datagram dengan jalur berbiaya rendah.
- Protokol yang Dapat Diperluas. Tidak seperti IPv4, IPv6 tidak menentukan semua fitur protokol yang memungkinkan. Sebagai gantinya, perancang telah menyediakan skema yang memungkinkan pengirim menambahkan informasi tambahan ke datagram. Skema ekstensi membuat IPv6 lebih fleksibel daripada IPv4, dan berarti fitur baru dapat ditambahkan ke desain sesuai kebutuhan.

Bagian selanjutnya menjelaskan bagaimana fitur baru diimplementasikan dengan menunjukkan organisasi datagram IPv6 dan struktur pengalamatan.

5.6 Format Datagram IPv6

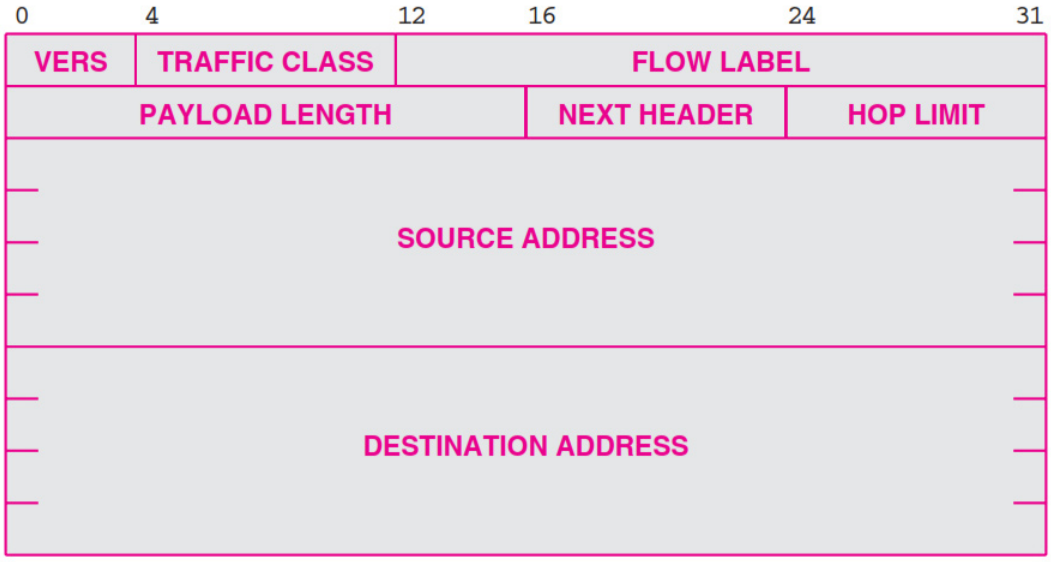
Datagram IPv6 berisi serangkaian header. Seperti yang diilustrasikan Gambar 5.2, setiap datagram dimulai dengan header dasar, yang diikuti oleh nol atau lebih ekstensi header diikuti oleh payload.

Gambar 5.2 Bentuk umum datagram IPv6.

Meskipun gambar tersebut mengilustrasikan struktur umum, bidang tidak digambar menurut skala. Secara khusus, beberapa tajuk ekstensi lebih besar dari tajuk dasar, dan yang lainnya lebih kecil. Dalam banyak datagram, ukuran payload jauh lebih besar daripada ukuran header.

5.7 Format Header Basis IPv6

Meskipun dua kali lebih besar dari header IPv4, header dasar IPv6 berisi lebih sedikit informasi. Gambar 5.3 mengilustrasikan formatnya.

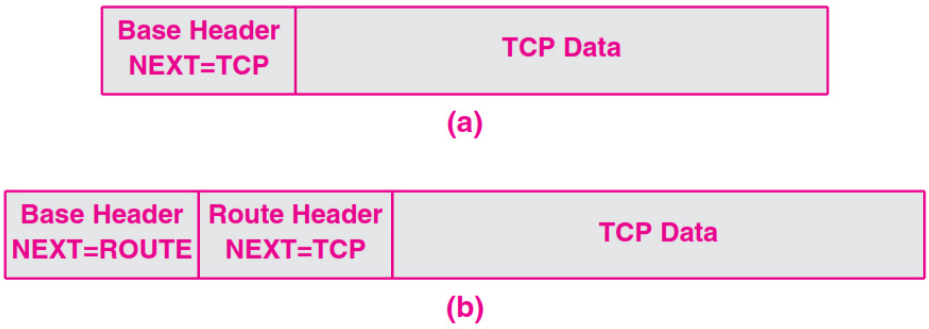


Gambar 5.3 Format header dasar dalam datagram IPv6.

Seperti yang ditunjukkan gambar, sebagian besar ruang di header dikhususkan untuk bidang ALAMAT SUMBER dan ALAMAT TUJUAN, yang masing-masing menempati enam belas oktet, empat kali lebih banyak dari alamat IPv4. Seperti di IPv4, alamat sumber mengidentifikasi sumber asli, dan alamat tujuan mengidentifikasi penerima akhir.

Selain alamat sumber dan tujuan, header dasar berisi enam bidang. Bidang VERS mengidentifikasi protokol sebagai versi 6. Bidang TRAFFIC CLASS menentukan kelas lalu lintas menggunakan definisi jenis lalu lintas yang dikenal sebagai layanan yang dibedakan untuk menentukan karakteristik umum yang dibutuhkan datagram. Misalnya, untuk mengirim lalu lintas interaktif (misalnya, penekanan tombol dan gerakan mouse), seseorang dapat menentukan kelas yang memiliki latensi rendah. Namun, untuk mengirim audio waktu-nyata melalui Internet, pengirim mungkin meminta jalur dengan jitter rendah. Bidang PANJANG PAYLOAD sesuai dengan bidang panjang datagram IPv4. Tidak seperti IPv4, PAYLOAD LENGTH hanya menentukan ukuran data yang dibawa (yaitu, payload); ukuran header dikecualikan. HOP LIMIT sesuai dengan bidang TIME-TO-LIVE IPv4. IPv6 menginterpretasikan HOP LIMIT secara ketat — datagram akan dibuang jika HOP LIMIT menghitung mundur hingga nol sebelum datagram tiba di tujuannya. Field FLOW LABEL awalnya dimaksudkan untuk mengasosiasikan datagram dengan jalur jaringan dasar tertentu. Sejak IPv6 didefinisikan, penggunaan label aliran ujung-ke-ujung tidak lagi disukai, dan LABEL FLOW menjadi kurang penting.

Bidang NEXT HEADER digunakan untuk menentukan jenis informasi yang mengikuti header saat ini. Misalnya, jika datagram menyertakan header ekstensi, bidang NEXT HEADER menentukan jenis header ekstensi. Jika tidak ada header ekstensi, bidang NEXT HEADER menentukan jenis data yang dibawa dalam payload. Gambar 5.4 mengilustrasikan bidang NEXT HEADER.

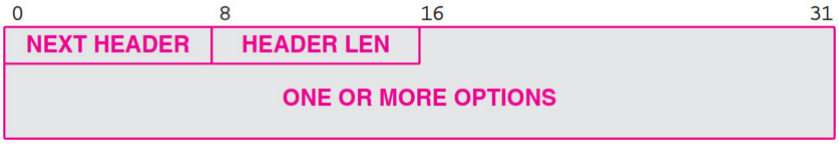


Gambar 5.4 Bidang NEXT HEADER dalam (a) datagram IPv6 yang memiliki header dasar dan muatan TCP, dan (b) datagram dengan header dasar, header rute, dan muatan TCP.

5.8 Ukuran Header Implisit dan Eksplisit

Karena standar menentukan nilai unik untuk setiap kemungkinan jenis header, tidak pernah ada ambiguitas tentang interpretasi bidang NEXT HEADER. Penerima memproses header secara berurutan, menggunakan bidang NEXT HEADER di setiap header untuk menentukan apa yang berikut.

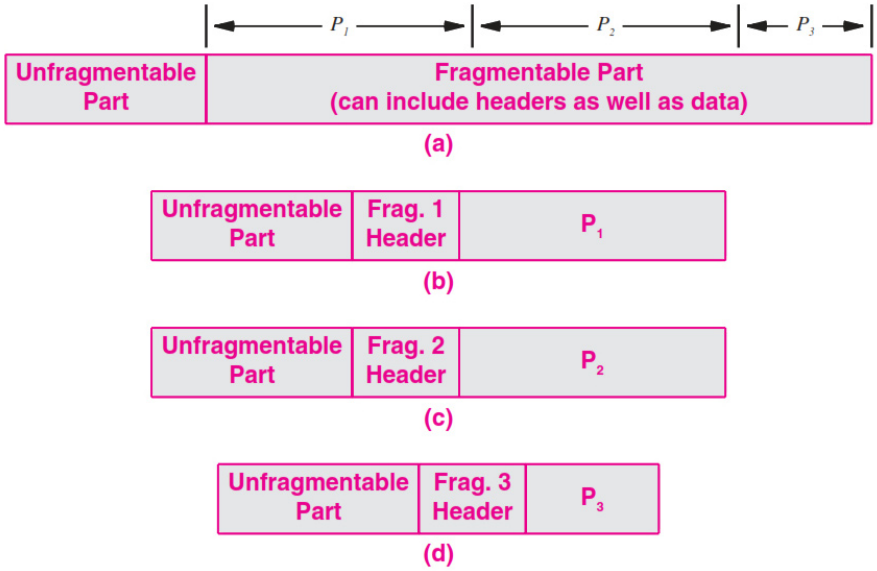
Beberapa jenis header memiliki ukuran tetap. Misalnya, header dasar memiliki ukuran tetap persis empat puluh oktet. Untuk berpindah ke item yang mengikuti header dasar, perangkat lunak IPv6 cukup menambahkan 40 ke alamat header dasar. Beberapa tajuk ekstensi tidak memiliki ukuran tetap. Dalam kasus seperti itu, header harus berisi informasi yang cukup untuk memungkinkan IPv6 menentukan di mana header berakhir. Misalnya, Gambar 5.5 mengilustrasikan bentuk umum dari header opsi IPv6 yang membawa informasi yang mirip dengan opsi dalam datagram IPv4.



Gambar 5.5 Ilustrasi header ekstensi opsi IPv6 dengan panjang eksplisit.

5.9 Fragmentasi, Perakitan Ulang, dan Jalur MTU

Meskipun fragmentasi IPv6 menyerupai fragmentasi IPv4, detailnya berbeda. Seperti IPv4, awalan dari datagram asli disalin ke setiap fragmen, dan panjang muatan dimodifikasi menjadi panjang fragmen. Tidak seperti IPv4, bagaimanapun, IPv6 tidak menyertakan bidang untuk informasi fragmentasi di header dasar. Sebaliknya, IPv6 menempatkan informasi fragmen di header ekstensi fragmen terpisah; keberadaan header mengidentifikasi datagram sebagai fragmen. Gambar 5.6 mengilustrasikan fragmentasi IPv6.



Gambar 5.6 Ilustrasi fragmentasi IPv6 dengan datagram (a) dibagi menjadi fragmen (b) sampai (d).

Pada gambar, Bagian yang Tidak Dapat Dipecahkan menunjukkan header dasar ditambah header yang mengontrol perutean. Untuk memastikan bahwa semua fragmen dirutekan secara identik, bagian yang tidak dapat difragmentasi direplikasi di setiap fragmen.

Seperti IPv4, ukuran fragmen dipilih untuk menjadi Unit Transmisi Maksimum (MTU) dari jaringan yang mendasari di mana fragmen harus dikirim. Jadi, fragmen terakhir mungkin lebih kecil dari yang lain karena mengandung sisa setelah potongan ukuran MTU diekstraksi dari datagram asli.

Fragmentasi di IPv6 berbeda secara dramatis dari fragmentasi di IPv4. Dalam IPv4, sebuah router melakukan fragmentasi ketika router menerima datagram yang terlalu besar untuk jaringan di mana datagram harus dikirim. Di IPv6, host pengirim bertanggung jawab atas fragmentasi. Artinya, host diharapkan untuk memilih ukuran datagram yang tidak memerlukan fragmentasi; router di sepanjang jalur yang menerima datagram yang lebih besar dari jaringan MTU akan mengirim pesan kesalahan dan membuang datagram.

Bagaimana sebuah host dapat memilih ukuran datagram yang tidak akan menghasilkan fragmentasi? Tuan rumah harus mempelajari MTU dari setiap jaringan di sepanjang jalur ke tujuan, dan harus memilih ukuran datagram agar sesuai dengan yang terkecil. MTU minimum sepanjang jalur dari sumber ke tujuan dikenal sebagai jalur MTU, dan proses mempelajari jalur MTU dikenal sebagai jalur penemuan MTU. Secara umum, penemuan jalur MTU adalah prosedur iteratif. Sebuah host mengirimkan urutan datagram berbagai ukuran ke tujuan untuk melihat apakah mereka tiba tanpa kesalahan. Jika fragmentasi diperlukan, host pengirim akan menerima pesan kesalahan ICMP. Setelah datagram cukup kecil untuk dilewati tanpa fragmentasi, host memilih ukuran datagram yang sama dengan jalur MTU.

Poin Penting

Di IPv6, fragmentasi dilakukan oleh host pengirim, dan bukan oleh router. Jika fragmentasi diperlukan, host pengirim menerima pesan kesalahan ICMP, dan mengurangi ukuran fragmen hingga fragmen dapat dikirim ke tujuan.

5.10 Tujuan Beberapa Header

Mengapa IPv6 menggunakan header ekstensi terpisah? Ada dua alasan:

- Ekonomi
- Kemungkinan diperpanjang

Ekonomis paling mudah dipahami: mempartisi fungsionalitas datagram ke dalam header terpisah adalah ekonomis karena menghemat ruang. Meskipun IPv6 mencakup banyak fitur, desainer mengharapkan datagram yang diberikan hanya menggunakan subset kecil. Memiliki header yang terpisah memungkinkan untuk menentukan sekumpulan besar fitur tanpa mengharuskan setiap header datagram memiliki setidaknya satu bidang untuk setiap fitur. Misalnya, meskipun banyak datagram IPv4 tidak terfragmentasi, header IPv4 memiliki bidang yang digunakan untuk menyimpan informasi fragmentasi. Sebaliknya, IPv6 tidak membuang ruang pada bidang untuk fragmentasi kecuali datagram terfragmentasi. Karena kebanyakan datagram hanya membutuhkan beberapa header, menghindari kolom header yang tidak perlu dapat menghemat banyak ruang. Datagram yang lebih kecil juga membutuhkan lebih sedikit waktu untuk mengirim. Dengan demikian, mengurangi ukuran datagram juga mengurangi bandwidth yang dikonsumsi.

Untuk memahami ekstensibilitas, pertimbangkan untuk menambahkan fitur baru ke protokol. Protokol seperti IPv4 yang menggunakan format header tetap memerlukan perubahan total — header harus didesain ulang untuk mengakomodasi bidang yang diperlukan untuk mendukung fitur baru. Namun, di IPv6, header protokol yang ada dapat tetap tidak berubah. Jenis NEXT HEADER baru didefinisikan serta format header baru.

Keuntungan lain menempatkan fungsionalitas baru di header baru terletak pada kemampuan untuk bereksperimen dengan fitur baru sebelum mengubah semua komputer di Internet. Misalnya, pemilik dua komputer ingin menguji teknik enkripsi datagram baru. Keduanya harus menyetujui rincian header enkripsi eksperimental. Pengirim menambahkan header baru ke datagram, dan penerima menafsirkan header dalam datagram yang masuk. Selama header baru muncul setelah header yang digunakan untuk perutean, router di Internet antara pengirim dan penerima dapat melewati datagram tanpa memahami header eksperimental†. Setelah fitur eksperimental terbukti berguna, fitur tersebut dapat dimasukkan ke dalam standar.

5.11 Pengalamatan IPv6

Seperti IPv4, IPv6 memberikan alamat unik untuk setiap koneksi antara komputer dan jaringan fisik. Jadi, jika komputer (misalnya, router) terhubung ke tiga jaringan fisik, komputer diberikan tiga alamat IPv6. Juga seperti IPv4, IPv6 memisahkan setiap alamat tersebut menjadi awalan yang mengidentifikasi jaringan dan akhiran yang mengidentifikasi komputer tertentu di jaringan.

Meskipun mengadopsi pendekatan yang sama untuk menetapkan alamat komputer, pengalamatan IPv6 berbeda dari pengalamatan IPv4 secara signifikan. Pertama, detail alamat sangat berbeda. Seperti alamat CIDR, pembagian antara awalan dan akhiran dapat terjadi pada batas yang berubah-ubah. Tidak seperti IPv4, IPv6 menyertakan alamat dengan hierarki multi-level. Meskipun penetapan alamat tidak tetap, dapat diasumsikan bahwa tingkat tertinggi sesuai dengan ISP, tingkat berikutnya sesuai dengan organisasi (misalnya, perusahaan), berikutnya ke situs, dan seterusnya. Kedua, IPv6 mendefinisikan satu set alamat khusus yang berbeda dari alamat khusus IPv4. Secara khusus, IPv6 tidak menyertakan alamat khusus untuk penyiaran pada jaringan jarak jauh yang diberikan. Sebaliknya, setiap alamat IPv6 adalah salah satu dari tiga tipe dasar yang tercantum pada Gambar 5.7.

Seperti yang ditunjukkan gambar, IPv6 mempertahankan pengalamatan unicast dan multicast. Siaran langsung dihilangkan karena menimbulkan masalah keamanan. Untuk menangani siaran terbatas (siaran di jaringan lokal), IPv6 mendefinisikan grup multicast khusus yang sesuai dengan semua host dan router di jaringan lokal.

Pengalamatan anycast awalnya dikenal sebagai pengalamatan cluster. Motivasi untuk pengalamatan tersebut muncul dari keinginan untuk memungkinkan replikasi layanan. Misalnya, sebuah perusahaan yang menawarkan layanan melalui jaringan memberikan alamat anycast ke beberapa komputer yang menyediakan layanan tersebut. Ketika pengguna mengirim datagram ke alamat anycast, IPv6 merutekan datagram ke salah satu komputer di set (yaitu, di cluster). Jika pengguna dari lokasi lain mengirim datagram ke alamat anycast, IPv6 dapat memilih untuk merutekan datagram ke anggota himpunan yang berbeda, memungkinkan kedua komputer memproses permintaan pada saat yang sama.

Jenis	Tujuan
unicast	Alamat sesuai dengan satu komputer. Datagram yang dikirim ke alamat dirutekan sepanjang jalur terpendek ke komputer.
multicast	Alamat sesuai dengan satu set komputer, dan keanggotaan dalam set dapat berubah setiap saat. IPv6 mengirimkan satu salinan datagram ke setiap anggota himpunan.
anycast	Alamat sesuai dengan sekumpulan komputer yang berbagi awalan yang sama. Datagram yang dikirim ke alamat dikirimkan ke salah satu komputer (misalnya, komputer yang paling dekat dengan pengirim).

Gambar 5.7 Tiga jenis alamat IPv6.

5.12 Notasi Heksadesimal Kolon IPv6

Karena alamat IPv6 menempati 128 bit, menulis angka seperti itu bisa jadi berat. Misalnya, pertimbangkan angka 128-bit yang ditulis dalam notasi desimal bertitik yang digunakan IPv4:

105.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255

Untuk membantu mengurangi jumlah karakter yang digunakan untuk menulis alamat, perancang IPv6 memilih bentuk sintaksis yang lebih ringkas yang dikenal sebagai notasi heksadesimal titik dua, biasanya disingkat hex titik dua, di mana setiap kelompok 16 bit ditulis dalam heksadesimal dengan kelompok yang memisahkan titik dua. . Misalnya, ketika angka di atas ditulis dalam hex titik dua, menjadi:

69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF

Seperti yang diilustrasikan pada contoh, notasi hex titik dua membutuhkan lebih sedikit karakter untuk mengekspresikan alamat. Pengoptimalan tambahan yang dikenal sebagai kompresi nol semakin mengurangi ukuran. Kompresi nol menggantikan urutan nol dengan dua titik dua. Misalnya, alamat:

FF0C:0:0:0:0:0:0:B1

dapat ditulis:

FF0C::B1

Ruang alamat IPv6 yang besar dan skema alokasi alamat yang diusulkan membuat kompresi nol menjadi sangat penting karena perancang mengharapkan banyak alamat IPv6 berisi string nol. Secara khusus, untuk membantu memudahkan transisi ke protokol baru, para perancang memetakan alamat IPv4 yang ada ke dalam ruang alamat IPv6. Setiap alamat IPv6 yang dimulai dengan 96 bit nol berisi alamat IPv4 dalam urutan rendah 32 bit.

5.13 Ringkasan

Meskipun versi IP saat ini telah bekerja dengan baik selama bertahun-tahun, pertumbuhan Internet yang eksponensial berarti bahwa ruang alamat 32-bit pada akhirnya akan habis. IETF telah merancang versi baru IP yang menggunakan 128 bit untuk mewakili setiap alamat. Untuk membedakan versi baru IP dari versi saat ini, kedua protokol diberi nama menggunakan nomor versinya. Versi IP saat ini adalah IPv4, dan versi baru adalah IPv6.

IPv6 mempertahankan banyak konsep dari IPv4, tetapi mengubah semua detailnya. Misalnya, seperti IPv4, IPv6 menyediakan layanan tanpa koneksi di mana dua komputer bertukar pesan singkat yang disebut datagram. Namun, tidak seperti datagram IPv4 di mana header berisi bidang untuk setiap fungsi, IPv6 mendefinisikan header terpisah untuk setiap fungsi. Setiap datagram IPv6 terdiri dari header dasar diikuti oleh nol atau lebih header ekstensi, diikuti oleh data.

Seperti IPv4, IPv6 mendefinisikan alamat untuk setiap koneksi jaringan. Jadi, seperti pada IPv4, komputer yang terhubung ke beberapa jaringan fisik (misalnya, router) memiliki banyak alamat. Namun, alamat khusus didefinisikan ulang di IPv6. Alih-alih gagasan IPv4 tentang siaran jaringan, IPv6 mendefinisikan alamat multicast dan anycast (cluster), keduanya sesuai dengan satu set komputer. Alamat multicast sesuai dengan satu set komputer di beberapa situs yang diperlakukan sebagai satu entitas — setiap komputer di set akan menerima salinan datagram apa pun yang dikirim ke set. Alamat anycast mengizinkan replikasi layanan — datagram yang dikirim ke alamat anycast akan dikirimkan ke tepat satu anggota grup (mis., anggota yang paling dekat dengan pengirim).

Untuk membuat alamat IPv6 lebih mudah digunakan orang, para perancang membuat notasi titik dua heksadesimal. Notasi hex titik dua menyatakan kelompok 16 bit dalam heksadesimal, dengan kelompok yang memisahkan titik dua. Kompresi nol menghilangkan nol jangka panjang. Notasi yang dihasilkan lebih kompak daripada bentuk desimal bertitik yang digunakan dalam IPv4.

Latihan

1. Apa motivasi utama perubahan dari IPv4 ke IPv6?
2. Apa model komunikasi Internet jam pasir?
3. Sebutkan fitur-fitur utama IPv6, dan berikan deskripsi singkat masing-masing.
4. Seberapa besar header datagram IPv6 terkecil?
5. Apa yang ditentukan oleh bidang NEXT HEADER dalam header datagram IPv6?
6. Apa bagian yang dapat terfragmentasi dari datagram IPv6?
7. Mengapa IPv6 menggunakan tajuk ekstensi terpisah alih-alih bidang dalam satu tajuk tetap?
8. Sebutkan tiga jenis alamat IPv6, dan berikan penjelasan singkat masing-masing.

9. Tulis program komputer yang membaca bilangan biner 128-bit dan mencetak bilangan tersebut dalam notasi hex titik dua.
10. Perluas program pada latihan sebelumnya untuk menerapkan kompresi nol.

Bab 6 UDP: Layanan Transportasi Datagram

Bab ini akan membahas tentang:

- UDP, salah satu dari dua protokol lapisan transport utama yang digunakan di Internet dan satu-satunya layanan transport tanpa koneksi
- Format paket UDP dan cara penggunaan UDP
- Konsep penting nomor port protokol

6.1 Protokol Transportasi dan Komunikasi End-To-End

Seperti yang ditunjukkan bab-bab sebelumnya, Internet Protocol menyediakan layanan pengiriman paket yang menjangkau Internet (yaitu, datagram dapat lewat dari host pengirim, melintasi satu atau lebih jaringan fisik, ke host penerima). Meskipun kemampuannya untuk melewatkan lalu lintas di Internet, IP tidak memiliki fitur penting: IP tidak dapat membedakan di antara beberapa program aplikasi yang berjalan pada host tertentu. Jika pengguna menjalankan aplikasi email dan browser web secara bersamaan atau menjalankan banyak salinan dari aplikasi tertentu, mereka harus dapat berkomunikasi secara independen.

IP tidak mampu mendukung banyak aplikasi karena bidang di header datagram hanya mengidentifikasi komputer. Artinya, dari sudut pandang IP, bidang sumber dan tujuan dalam datagram mengidentifikasi komputer host; alamat IP tidak mengandung bit tambahan untuk mengidentifikasi program aplikasi pada host. Kami mengatakan bahwa IP memperlakukan komputer sebagai titik akhir komunikasi. Sebaliknya, protokol lapisan transport dikenal sebagai protokol ujung ke ujung karena protokol transport memungkinkan program aplikasi individu menjadi titik akhir komunikasi. Alih-alih menambahkan fitur tambahan ke IP untuk mengidentifikasi aplikasi, perancang protokol TCP/IP menempatkan protokol ujung ke ujung di lapisan terpisah, Layer 4.

6.2 Protokol Datagram Pengguna

Seperti yang akan kita lihat, suite TCP/IP berisi dua protokol transport, User Datagram Protocol (UDP) dan Transmission Control Protocol (TCP), yang berbeda secara dramatis dalam layanan yang mereka tawarkan ke aplikasi. UDP kurang kompleks dan paling mudah dipahami. Kesederhanaan dan kemudahan pemahaman datang dengan biaya — UDP tidak menyediakan jenis layanan yang diharapkan oleh aplikasi biasa.

UDP dapat dicirikan sebagai:

- Ujung ke ujung. UDP adalah protokol transport yang dapat membedakan beberapa program aplikasi yang berjalan pada komputer tertentu.
- Tanpa koneksi. Antarmuka yang dipasok UDP ke aplikasi mengikuti paradigma tanpa koneksi.
- Berorientasi pesan. Aplikasi yang menggunakan UDP mengirim dan menerima pesan individual.
- Usaha terbaik. UDP menawarkan aplikasi semantik pengiriman upaya terbaik yang sama seperti IP.
- Interaksi Sewenang-wenang. UDP memungkinkan aplikasi untuk mengirim ke banyak aplikasi lain, menerima dari banyak aplikasi lain, atau berkomunikasi dengan tepat satu aplikasi lain.
- Sistem Operasi Independen. UDP menyediakan sarana untuk mengidentifikasi program aplikasi yang tidak bergantung pada pengenal yang digunakan oleh sistem operasi lokal.

Karakteristik paling penting dari UDP, semantik upaya terbaiknya, muncul karena UDP menggunakan IP untuk transmisi. Faktanya, UDP terkadang dicirikan sebagai lapisan protokol tipis yang menyediakan aplikasi dengan kemampuan untuk mengirim dan menerima datagram IP.

Poin Penting

UDP menyediakan layanan ujung ke ujung yang memungkinkan program aplikasi mengirim dan menerima pesan individual, yang masing-masing berjalan dalam datagram terpisah. Sebuah aplikasi dapat memilih untuk membatasi komunikasi ke satu program aplikasi lain atau berkomunikasi dengan beberapa aplikasi.

6.3 Paradigma Tanpa Koneksi

UDP menggunakan paradigma komunikasi tanpa koneksi, yang berarti bahwa aplikasi yang menggunakan UDP tidak perlu melakukan komunikasi sebelumnya sebelum mengirim data, aplikasi juga tidak perlu menginformasikan jaringan saat selesai. Sebaliknya, aplikasi dapat menghasilkan dan mengirim data kapan saja. Selain itu, UDP memungkinkan aplikasi untuk menunda waktu yang lama antara transmisi dua pesan. UDP tidak mempertahankan status, dan tidak menggunakan pesan kontrol; komunikasi hanya terdiri dari pesan data itu sendiri. Secara khusus, jika sepasang aplikasi berhenti mengirim data, tidak ada paket lain yang dipertukarkan. Akibatnya, UDP memiliki overhead yang sangat rendah.

Poin Penting

UDP bersifat connectionless, artinya aplikasi dapat mengirim data kapan saja dan UDP tidak mengirimkan paket selain paket yang membawa data pengguna.

6.4 Antarmuka Berorientasi Pesan

UDP menawarkan program aplikasi antarmuka berorientasi pesan. Setiap kali aplikasi meminta UDP mengirim blok data, UDP menempatkan data dalam satu pesan untuk transmisi. UDP tidak membagi pesan menjadi beberapa paket, dan tidak menggabungkan pesan untuk pengiriman — setiap pesan yang dikirim oleh aplikasi diangkut melalui Internet dan dikirimkan ke penerima.

Antarmuka berorientasi pesan memiliki beberapa konsekuensi penting bagi programmer. Sisi positifnya, aplikasi yang menggunakan UDP dapat bergantung pada protokol untuk menjaga batas data — setiap pesan yang dikirimkan UDP ke aplikasi penerima akan sama persis dengan yang dikirimkan oleh pengirim. Di sisi negatif, setiap pesan UDP harus masuk ke dalam satu datagram IP. Dengan demikian, ukuran datagram IP membentuk batas mutlak pada ukuran pesan UDP. Lebih penting lagi, ukuran pesan UDP dapat menyebabkan penggunaan jaringan yang mendasarinya menjadi tidak efisien. Jika sebuah aplikasi mengirimkan pesan yang sangat kecil, datagram yang dihasilkan akan memiliki rasio besar oktet header terhadap oktet data. Jika aplikasi mengirim pesan yang sangat besar, datagram yang dihasilkan mungkin lebih besar dari MTU jaringan, dan akan dipecah oleh IP.

Membiarkan pesan UDP menjadi besar menghasilkan anomali yang menarik. Biasanya, seorang programmer aplikasi dapat mencapai efisiensi yang lebih tinggi dengan menggunakan transfer yang besar. Misalnya, programmer didorong untuk mendeklarasikan buffer I/O yang besar, dan untuk menentukan transfer yang sesuai dengan ukuran buffer. Dengan UDP, bagaimanapun, mengirim pesan besar menyebabkan efisiensi yang lebih rendah karena pesan besar menyebabkan fragmentasi. Lebih mengejutkan lagi, fragmentasi dapat terjadi pada komputer pengirim — sebuah aplikasi mengirim pesan berukuran besar, UDP menempatkan seluruh pesan dalam datagram pengguna dan merangkum datagram pengguna dalam datagram Internet, dan IP harus melakukan fragmentasi sebelum datagram dapat dikirim.

Poin Penting

Meskipun intuisi programmer menyarankan bahwa menggunakan pesan yang lebih besar akan meningkatkan efisiensi, jika pesan UDP lebih besar dari jaringan MTU, IP akan memecah datagram yang dihasilkan, yang mengurangi efisiensi.

Akibatnya, banyak programmer yang menggunakan UDP memilih ukuran pesan yang menghasilkan datagram yang sesuai dengan MTU standar. Secara khusus, karena sebagian besar Internet sekarang mendukung MTU 1500 oktet, pemrogram sering memilih ukuran pesan 1400 atau 1450 untuk menyisakan banyak ruang untuk header IP dan UDP.

6.5 Semantik Komunikasi UDP

UDP menggunakan IP untuk semua pengiriman. Lebih lanjut, UDP menyediakan aplikasi dengan semantik pengiriman upaya terbaik yang sama persis seperti IP, yang berarti pesan dapat berupa:

- Hilang
- Digandakan
- Tertunda
- Dikirim tidak sesuai pesanan
- Rusak

Tentu saja, UDP tidak sengaja menimbulkan masalah pengiriman. Sebaliknya, UDP hanya menggunakan IP untuk mengirim pesan, dan tidak mendeteksi atau memperbaiki masalah pengiriman. Semantik pengiriman upaya terbaik UDP memiliki konsekuensi penting untuk aplikasi. Sebuah aplikasi harus kebal terhadap masalah atau programmer harus mengambil langkah tambahan untuk mendeteksi dan memperbaiki masalah. Sebagai contoh aplikasi yang dapat mentolerir kesalahan paket, pertimbangkan transmisi audio. Jika pengirim menempatkan sejumlah kecil audio di setiap pesan, hilangnya satu paket menghasilkan celah kecil dalam pemutaran, yang akan terdengar sebagai pop atau klik. Meskipun tidak diinginkan, kebisingan hanya mengganggu. Sebaliknya, pertimbangkan aplikasi belanja online. Aplikasi tersebut tidak ditulis untuk menggunakan UDP karena kesalahan paket dapat berakibat serius (misalnya, duplikasi pesan yang membawa pesanan katalog dapat mengakibatkan dua pesanan, dengan biaya ganda yang dibebankan ke kartu kredit pembeli).

Poin Penting

Karena UDP menawarkan semantik pengiriman upaya terbaik yang sama seperti IP, pesan UDP dapat hilang, diduplikasi, tertunda, dikirim tidak sesuai pesanan, atau bit dapat rusak saat transit. UDP hanya cukup untuk aplikasi seperti suara atau video yang dapat mentolerir kesalahan pengiriman.

6.6 Mode Interaksi dan Pengiriman Siaran

UDP memungkinkan empat gaya interaksi:

- 1-ke-1
- 1-ke-banyak
- Banyak-ke-1
- Banyak ke banyak

Artinya, aplikasi yang menggunakan UDP memiliki pilihan. Aplikasi dapat memilih interaksi 1-ke-1 di mana aplikasi bertukar pesan dengan tepat satu aplikasi lain, interaksi 1-ke-banyak di mana aplikasi mengirim pesan ke beberapa penerima, atau interaksi banyak-ke-1 di di mana aplikasi menerima pesan dari banyak pengirim. Akhirnya, satu set aplikasi dapat membangun interaksi banyak-ke-banyak di mana mereka bertukar pesan satu sama lain.

Meskipun interaksi 1-ke-banyak dapat dicapai dengan mengatur pengiriman salinan pesan individual ke setiap penerima yang dituju, UDP memungkinkan pertukaran menjadi efisien. Alih-alih mengharuskan aplikasi untuk berulang kali mengirim pesan ke beberapa penerima, UDP memungkinkan aplikasi untuk mengirimkan pesan melalui multicast IP atau siaran. Untuk melakukannya, pengirim menggunakan alamat IP broadcast sebagai alamat IP tujuan. Misalnya, siaran lokal dapat ditentukan dengan menggunakan alamat siaran terbatas IP, 255.255.255.255. Demikian pula, UDP memungkinkan aplikasi untuk mengirim pesan multicast. Pengiriman melalui siaran atau multicast sangat berguna untuk jaringan Ethernet karena perangkat keras yang mendasari mendukung kedua jenis secara efisien.

6.7 Identifikasi Titik Akhir dengan Nomor Port Protokol

Bagaimana tepatnya UDP mengidentifikasi program aplikasi sebagai titik akhir? Tampaknya UDP dapat menggunakan mekanisme yang sama dengan yang digunakan sistem operasi. Sayangnya, karena UDP harus menjangkau komputer yang heterogen, tidak ada mekanisme umum yang ada.

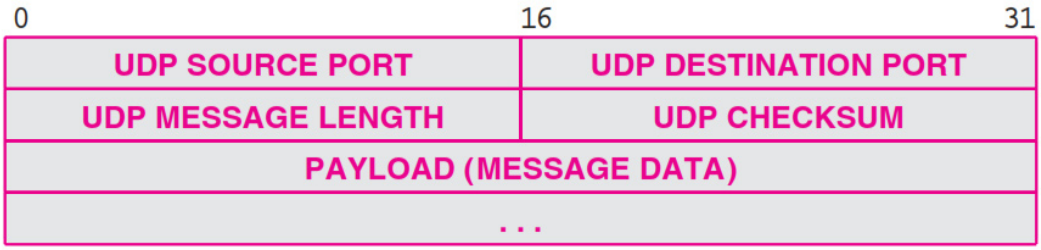
Misalnya, beberapa sistem operasi menggunakan pengidentifikasi proses, yang lain menggunakan nama pekerjaan, dan yang lain menggunakan pengidentifikasi tugas. Dengan demikian, pengidentifikasi yang berarti pada satu sistem mungkin tidak berarti pada yang lain.

Untuk menghindari ambiguitas, UDP mendefinisikan satu set abstrak pengidentifikasi yang disebut nomor port protokol yang independen dari sistem operasi yang mendasarinya. Setiap komputer yang mengimplementasikan UDP harus menyediakan pemetaan antara nomor port protokol dan pengidentifikasi program yang digunakan sistem operasi. Misalnya, standar UDP mendefinisikan nomor port protokol tujuh sebagai port untuk layanan gema dan nomor port tiga puluh tujuh sebagai port untuk layanan server waktu. Semua komputer yang menjalankan UDP mengenali nomor port protokol standar, terlepas dari sistem operasi yang mendasarinya. Jadi, ketika pesan UDP tiba untuk port tujuh, perangkat lunak protokol UDP harus mengetahui program mana di komputer lokal yang mengimplementasikan layanan gema dan harus meneruskan pesan masuk ke program.

Mode komunikasi ditentukan oleh cara aplikasi mengisi alamat dan nomor port protokol untuk soket. Untuk terlibat dalam komunikasi 1-ke-1, misalnya, aplikasi menentukan nomor port lokal, alamat IP jarak jauh, dan nomor port protokol jarak jauh; UDP hanya meneruskan pesan aplikasi yang datang dari pengirim yang ditentukan. Untuk terlibat dalam komunikasi banyak-ke-1, aplikasi menentukan nomor port lokal, tetapi memberi tahu UDP bahwa titik akhir jarak jauh dapat berupa sistem apa pun. UDP kemudian melewati aplikasi semua pesan yang datang untuk port yang ditentukan.

6.8 Format Datagram UDP

Setiap pesan UDP disebut user datagram dan terdiri dari dua bagian: header pendek yang menentukan program aplikasi pengirim dan penerima dan payload yang membawa data yang dikirim. Gambar 6.1 mengilustrasikan format datagram pengguna.



Gambar 6.1 Format datagram pengguna UDP dengan header 8 oktet.

Dua bidang pertama dari header UDP berisi nomor port protokol 16-bit. Field UDP SOURCE PORT berisi nomor port aplikasi pengirim, dan field UDP DESTINATION PORT berisi nomor port aplikasi tujuan pengiriman pesan. Bidang UDP MESSAGE LENGTH menentukan ukuran total pesan UDP, diukur dalam byte 8-bit.

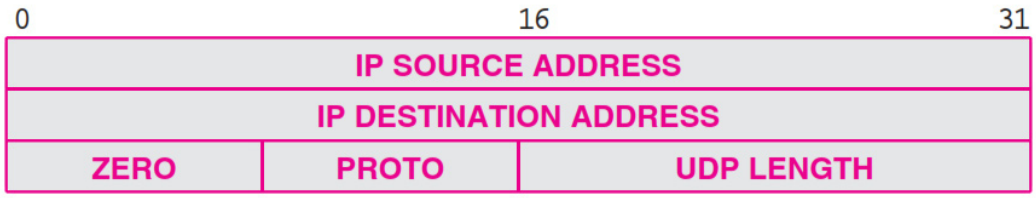
6.9 Checksum UDP dan Header Pseudo

Meskipun header UDP berisi bidang enam belas bit bernama UDP checksum, checksum bersifat opsional. Pengirim dapat memilih untuk menghitung checksum atau mengatur semua bit bidang checksum ke nol. Ketika sebuah pesan tiba di tujuan, perangkat lunak UDP memeriksa bidang checksum, dan hanya memverifikasi checksum jika nilainya bukan nol.

Perhatikan bahwa header UDP tidak berisi identifikasi pengirim atau penerima selain nomor port protokol. Secara khusus, UDP mengasumsikan bahwa sumber IP dan alamat tujuan terkandung dalam datagram IP yang membawa UDP. Dengan demikian, alamat IP tidak dibawa dalam header UDP.

Menghilangkan alamat IP sumber dan tujuan membuat UDP lebih kecil dan lebih efisien, tetapi menimbulkan kemungkinan kesalahan. Khususnya, jika IP mengalami malfungsi dan mengirimkan pesan UDP ke tujuan yang salah, UDP tidak dapat menggunakan bidang header untuk menentukan bahwa terjadi kesalahan.

Untuk mengizinkan UDP memverifikasi bahwa pesan mencapai tujuan yang benar tanpa menimbulkan overhead bidang header tambahan, UDP memperluas checksum. Saat menghitung checksum, perangkat lunak UDP menyertakan header semu yang berisi bidang sumber, tujuan, dan jenis (yaitu PROTO) dari datagram IP dan panjang datagram UDP. Artinya, pengirim menghitung checksum seolah-olah header UDP berisi bidang tambahan. Demikian pula, untuk memverifikasi checksum, penerima harus mendapatkan panjang UDP, dan bidang sumber, tujuan, dan jenis dari datagram IP; penerima menambahkannya ke pesan UDP sebelum memverifikasi checksum. Gambar 6.2 mengilustrasikan field dalam pseudo header.

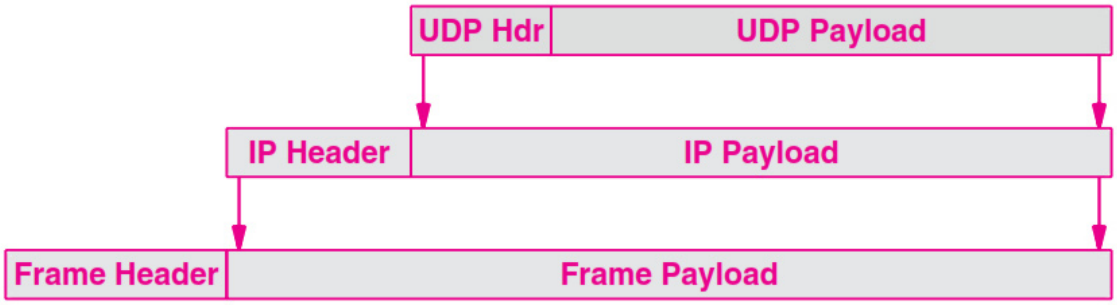


Gambar 6.2 Ilustrasi header semu yang digunakan untuk menghitung checksum UDP.

6.10 Enkapsulasi UDP

Seperti ICMP, setiap datagram UDP dienkapsulasi dalam datagram IP untuk transmisi di Internet. Gambar 6.3 mengilustrasikan enkapsulasi.

\



Gambar 6.3 Enkapsulasi pesan UDP dalam datagram IP.

6.11 Ringkasan

Protokol Datagram Pengguna menyediakan transportasi pesan ujung ke ujung dari aplikasi yang berjalan di satu komputer ke aplikasi yang berjalan di komputer lain. UDP menawarkan semantik pengiriman upaya terbaik yang sama seperti IP, yang berarti bahwa pesan dapat hilang, diduplikasi, atau dikirim tidak sesuai pesanan. Satu keuntungan dari pendekatan tanpa koneksi muncul dari kemampuan untuk memiliki interaksi 1-ke-1, 1-ke-banyak, dan banyak-ke-1 antar aplikasi.

Untuk tetap independen dari sistem operasi yang mendasarinya, UDP menggunakan nomor port protokol integer kecil untuk membedakan di antara program aplikasi. Perangkat lunak protokol pada komputer tertentu harus memetakan setiap nomor port protokol ke mekanisme yang sesuai (misalnya, ID proses) yang digunakan pada komputer.

Checksum UDP bersifat opsional — jika pengirim mengisi bidang checksum dengan nol, penerima tidak memverifikasi checksum. Untuk memverifikasi bahwa datagram UDP tiba di lokasi yang benar, checksum UDP dihitung melalui datagram ditambah header semu

UDP membutuhkan dua tingkat enkapsulasi. Setiap pesan UDP dienkapsulasi dalam datagram IP untuk transmisi di Internet. Datagram dienkapsulasi dalam bingkai untuk transmisi melalui jaringan individu.

Latihan

1. Apa perbedaan konseptual antara IP dan protokol ujung ke ujung?
2. Sebutkan fitur-fitur UDP.
3. Apakah aplikasi perlu bertukar pesan kontrol UDP sebelum bertukar data? Menjelaskan.
4. Hitung ukuran pesan UDP terbesar yang mungkin. (Petunjuk: seluruh pesan UDP harus sesuai dengan datagram IP.)
5. Apa yang terjadi jika pesan UDP yang berisi muatan 1500 byte data dikirim melalui Ethernet?
6. Jika aplikasi menggunakan UDP untuk mengirim pesan 8K byte melalui Ethernet, berapa banyak frame yang akan melintasi jaringan?
7. Jelaskan apa yang dimaskud dengan semantik dari UDP?
8. Nilai titik akhir apa yang harus ditentukan oleh aplikasi yang terlibat dalam komunikasi 1-ke-1? Dalam 1-ke-banyak? Dalam banyak-ke-1?
9. Jelaskan apa yang dimaskud dengan header semu, dan kapan digunakan?
10. Diberikan bingkai Ethernet, bidang apa yang harus diperiksa untuk menentukan apakah bingkai membawa pesan UDP?

Bab 7 TCP: Layanan Transportasi yang Andal

Bab ini akan membahas tentang:

- Protokol transport secara umum, dan membahas TCP, protokol transport utama yang digunakan di Internet
- Bagaimana protokol TCP menyediakan pengiriman yang andal.
- Teknik yang digunakan TCP untuk mencapai keandalan

7.1 Protokol Kontrol Transmisi

Pemrogram dilatih untuk berpikir bahwa keandalan adalah hal mendasar dalam sistem komputer. Misalnya, saat menulis aplikasi yang mengirimkan data ke perangkat I/O seperti printer, programmer mengasumsikan data akan tiba dengan benar atau sistem operasi akan menginformasikan aplikasi bahwa telah terjadi kesalahan. Artinya, seorang programmer mengasumsikan sistem yang mendasarinya menjamin bahwa data akan dikirimkan dengan andal.

Untuk memungkinkan pemrogram mengikuti teknik konvensional saat membuat aplikasi yang berkomunikasi melalui Internet, perangkat lunak protokol harus menyediakan semantik yang sama dengan sistem komputer konvensional: perangkat lunak harus menjamin komunikasi yang cepat dan andal. Data harus dikirimkan dalam urutan yang sama persis seperti saat dikirimkan, dan tidak boleh ada kehilangan atau duplikasi.

Dalam suite TCP/IP, Transmission Control Protocol (TCP) menyediakan layanan transportasi yang andal. TCP luar biasa karena memecahkan masalah yang sulit dengan baik — meskipun protokol lain telah dibuat, tidak ada protokol transport tujuan umum yang terbukti bekerja lebih baik. Akibatnya, sebagian besar aplikasi Internet dibangun untuk menggunakan TCP.

Poin Penting

Di Internet, Transmission Control Protocol (TCP) adalah protokol lapisan transport yang menyediakan keandalan.

7.2 Layanan yang Diberikan TCP ke Aplikasi

Layanan yang ditawarkan oleh TCP memiliki tujuh fitur utama:

- Orientasi Koneksi. TCP menyediakan layanan berorientasi koneksi di mana aplikasi harus terlebih dahulu meminta koneksi ke tujuan, dan kemudian menggunakan koneksi untuk mentransfer data.
- Komunikasi Titik ke Titik. Setiap koneksi TCP memiliki tepat dua titik akhir.
- Keandalan Lengkap. TCP menjamin bahwa data yang dikirim melalui koneksi akan dikirimkan persis seperti yang dikirim, lengkap, dan berurutan.
- Komunikasi Dupleks Penuh. Koneksi TCP memungkinkan data mengalir ke kedua arah, dan memungkinkan program aplikasi mana pun mengirim data kapan saja.
- Antarmuka Aliran. TCP menyediakan antarmuka aliran di mana aplikasi mengirimkan urutan oktet terus menerus di seluruh koneksi. TCP tidak mengelompokkan data ke dalam catatan atau pesan, dan tidak menjamin untuk mengirimkan data dalam potongan ukuran yang sama yang ditransfer oleh aplikasi pengirim.
- Startup Koneksi yang Andal. TCP memungkinkan dua aplikasi untuk memulai komunikasi dengan andal.
- Shutdown Koneksi Anggun. Sebelum menutup koneksi, TCP memastikan bahwa semua data telah dikirimkan dan kedua belah pihak telah sepakat untuk mematikan koneksi.

Poin Penting

TCP menyediakan layanan transportasi aliran dupleks penuh yang andal, berorientasi koneksi, yang memungkinkan dua program aplikasi membentuk koneksi, mengirim data ke kedua arah, dan kemudian mengakhiri koneksi. Setiap koneksi TCP dimulai dengan andal dan diakhiri dengan baik.

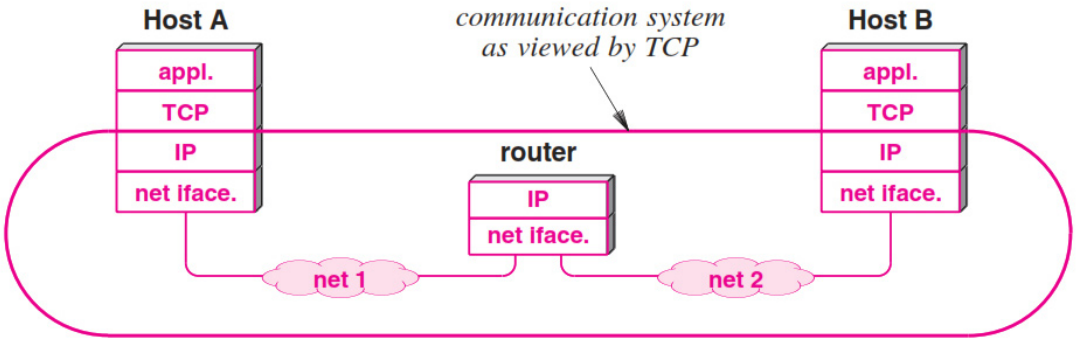
7.3 Layanan End-To-End dan Koneksi Virtual

Seperti UDP, TCP diklasifikasikan sebagai protokol end-to-end karena menyediakan komunikasi antara aplikasi di satu komputer ke aplikasi di komputer lain. Berorientasi koneksi karena aplikasi harus meminta TCP membentuk koneksi sebelum mereka dapat mentransfer data, dan harus menutup koneksi saat transfer selesai.

Koneksi yang disediakan oleh TCP disebut koneksi virtual karena dicapai dalam perangkat lunak. Memang, Internet yang mendasarinya tidak menyediakan dukungan perangkat keras atau perangkat lunak untuk koneksi. Sebagai gantinya, modul perangkat lunak TCP pada dua mesin bertukar pesan untuk mencapai ilusi koneksi.

Setiap pesan TCP dienkapsulasi dalam datagram IP dan dikirim melalui Internet. Ketika datagram tiba di host tujuan, IP meneruskan konten ke TCP. Perhatikan bahwa meskipun TCP menggunakan IP untuk membawa pesan, IP tidak membaca atau menafsirkan pesan. Faktanya, IP memperlakukan setiap pesan TCP sebagai data yang akan ditransfer. Sebaliknya, TCP memperlakukan IP sebagai

sistem komunikasi paket yang menyediakan komunikasi antara modul TCP di setiap ujung koneksi. Gambar 7.1 mengilustrasikan bagaimana TCP memandang Internet yang mendasarinya.



Gambar 7.1 Ilustrasi bagaimana TCP memandang Internet yang mendasarinya.

Seperti yang ditunjukkan gambar, perangkat lunak TCP diperlukan di setiap ujung koneksi virtual, tetapi tidak pada router perantara. Dari sudut pandang TCP, seluruh Internet adalah sistem komunikasi yang dapat menerima dan mengirimkan pesan tanpa mengubah atau menafsirkan isinya.

7.4 Teknik yang Digunakan Protokol Transportasi

Protokol transport ujung ke ujung harus dirancang dengan hati-hati untuk mencapai transfer yang efisien dan andal. Masalah utama adalah:

- Komunikasi yang Tidak Dapat Diandalkan. Pesan yang dikirim melalui Internet dapat hilang, digandakan, rusak, tertunda, atau dikirim dengan rusak.
- Akhiri Reboot Sistem. Setiap saat selama komunikasi, salah satu dari dua sistem akhir mungkin crash dan reboot. Tidak boleh ada kebingungan di antara sesi; beberapa sistem tertanam dapat melakukan boot ulang dalam waktu yang lebih singkat daripada yang dibutuhkan sebuah paket untuk melintasi Internet.
- Sistem Akhir Heterogen. Pengirim yang kuat dapat menghasilkan data dengan sangat cepat sehingga melampaui penerima yang lambat.
- Kemacetan Di Internet. Jika pengirim mengirimkan data secara agresif, sakelar perantara dan router dapat dibanjiri paket, analog dengan jalan raya yang padat.

Kita telah melihat contoh teknik dasar yang digunakan sistem komunikasi data untuk mengatasi beberapa masalah. Misalnya, untuk mengkompensasi bit yang diubah selama transmisi, protokol mungkin menyertakan bit paritas, checksum, atau cyclic redundancy check (CRC). Protokol transport melakukan lebih dari sekadar mendeteksi kesalahan — mereka menggunakan teknik yang dapat memperbaiki atau menghindari masalah. Secara khusus, protokol transport menggunakan berbagai alat untuk menangani beberapa masalah komunikasi yang paling rumit. Bagian selanjutnya membahas mekanisme dasar.

7.4.1 Urutan untuk Menangani Duplikat dan Pengiriman Tidak Sesuai Pesanan

Untuk menangani paket duplikat dan pengiriman yang tidak sesuai pesanan, protokol transport menggunakan pengurutan. Sisi pengirim melampirkan nomor urut ke setiap paket. Sisi penerima menyimpan nomor urut dari paket terakhir yang diterima secara berurutan serta daftar paket tambahan

yang tiba tidak sesuai pesanan. Ketika sebuah paket tiba, penerima memeriksa nomor urut untuk menentukan bagaimana paket harus ditangani. Jika paket adalah yang diharapkan berikutnya (yaitu, telah tiba secara berurutan), perangkat lunak protokol mengirimkan paket ke lapisan tertinggi berikutnya, dan memeriksa daftarnya untuk melihat apakah paket tambahan juga dapat dikirimkan. Jika paket tiba dalam keadaan rusak, perangkat lunak protokol menambahkan paket ke daftar. Sequencing juga memecahkan masalah duplikasi — penerima memeriksa duplikat ketika memeriksa nomor urut paket yang datang. Jika paket telah terkirim atau nomor urut cocok dengan salah satu paket yang menunggu dalam daftar, perangkat lunak akan membuang salinan baru.

7.4.2 Transmisi Ulang untuk Menangani Paket yang Hilang

Untuk menangani kehilangan paket, protokol transport menggunakan pengakuan positif dengan transmisi ulang. Setiap kali sebuah frame tiba dengan utuh, perangkat lunak protokol penerima mengirimkan pesan small acknowledgment (ACK) yang melaporkan penerimaan yang berhasil. Pengirim bertanggung jawab untuk memastikan bahwa setiap paket berhasil ditransfer. Setiap kali mengirim paket, perangkat lunak protokol sisi pengirim memulai pengatur waktu. Jika pengakuan tiba sebelum timer berakhir, perangkat lunak membatalkan timer; jika penghitung waktu berakhir sebelum pengakuan tiba, perangkat lunak mengirimkan salinan lain dari paket dan memulai penghitung waktu lagi. Tindakan mengirim salinan kedua dikenal sebagai transmisi ulang, dan salinannya biasa disebut transmisi ulang.

Tentu saja, transmisi ulang tidak dapat berhasil jika kegagalan perangkat keras telah memutuskan jaringan secara permanen atau jika komputer penerima mengalami gangguan. Oleh karena itu, protokol yang mengirim ulang pesan biasanya membatasi jumlah maksimum pengiriman ulang. Ketika batas telah tercapai, protokol berhenti mentransmisikan ulang dan menyatakan bahwa komunikasi tidak mungkin dilakukan.

Perhatikan bahwa jika paket tertunda, transmisi ulang dapat memperkenalkan paket duplikat. Jadi, protokol transport yang menggabungkan transmisi ulang biasanya dirancang untuk menangani masalah paket duplikat.

7.4.3 Teknik untuk Menghindari Pemutaran Ulang

Penundaan yang sangat lama dapat menyebabkan kesalahan pemutaran ulang di mana paket yang tertunda mempengaruhi komunikasi selanjutnya. Sebagai contoh, perhatikan urutan peristiwa berikut.

- Dua komputer setuju untuk berkomunikasi pada pukul 1 siang.
- Satu komputer mengirimkan urutan sepuluh paket ke komputer lainnya. Masalah perangkat keras menyebabkan paket 3 tertunda.
- Rute berubah untuk menghindari masalah perangkat keras.
- Perangkat lunak protokol pada komputer pengirim mentransmisi ulang paket 3, dan mengirimkan paket yang tersisa tanpa kesalahan.
- Pada pukul 13.05 kedua komputer setuju untuk berkomunikasi kembali.
- Setelah paket kedua tiba, salinan paket 3 yang tertunda datang dari percakapan sebelumnya.
- Paket 3 datang dari percakapan kedua.

Kecuali protokol transport dirancang dengan hati-hati untuk menghindari masalah seperti itu, paket dari percakapan sebelumnya mungkin diterima di percakapan selanjutnya dan paket yang benar dibuang sebagai duplikat.

Pemutaran ulang juga dapat terjadi dengan paket kontrol (yaitu, paket yang membangun atau mengakhiri komunikasi). Untuk memahami ruang lingkup masalah, pertimbangkan situasi di mana dua program aplikasi membentuk koneksi TCP, berkomunikasi, menutup koneksi, dan kemudian membentuk koneksi baru. Pesan yang menentukan penutupan koneksi mungkin diduplikasi dan satu salinan mungkin tertunda cukup lama untuk koneksi kedua dibuat. Protokol harus dirancang sedemikian rupa sehingga pesan duplikat tidak akan menyebabkan koneksi kedua ditutup.

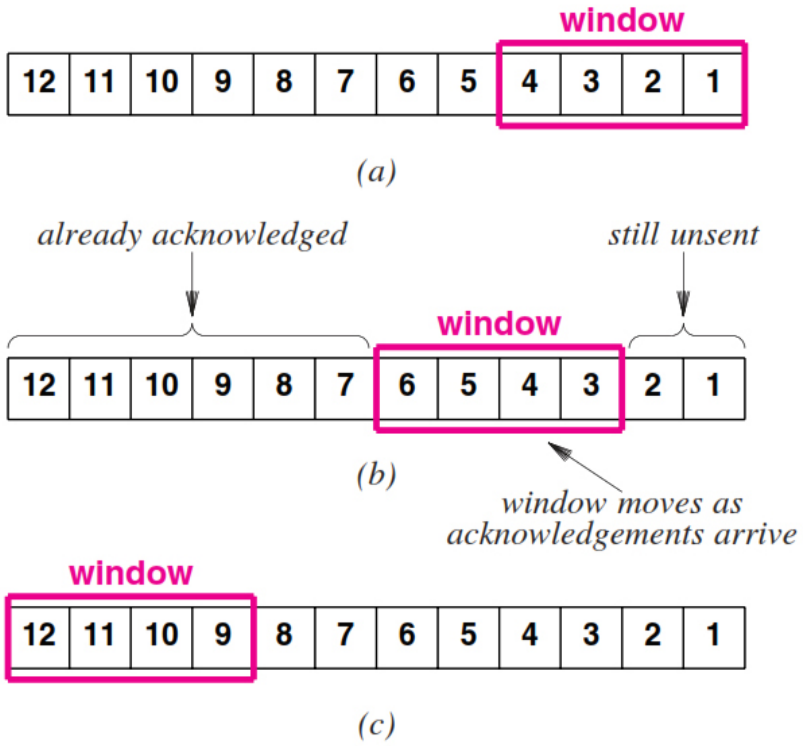
Untuk mencegah pemutaran ulang, protokol menandai setiap sesi dengan ID unik (mis., Waktu sesi dibuat), dan mengharuskan ID unik ada di setiap paket. Perangkat lunak protokol membuang semua paket yang tiba yang berisi ID yang salah. Untuk menghindari pemutaran ulang, ID tidak boleh digunakan kembali sampai waktu yang wajar telah berlalu (misalnya, jam).

7.4.4 Kontrol Aliran untuk Mencegah Data Overrun

Beberapa teknik tersedia untuk mencegah komputer yang cepat mengirimkan begitu banyak data sehingga melampaui penerima yang lambat. Kami menggunakan istilah kontrol aliran untuk merujuk pada teknik yang menangani masalah. Bentuk kontrol aliran yang paling sederhana adalah sistem stop-and-go di mana pengirim menunggu setelah mengirimkan setiap paket. Ketika penerima siap untuk paket lain, penerima mengirimkan pesan kontrol, biasanya bentuk pengakuan.

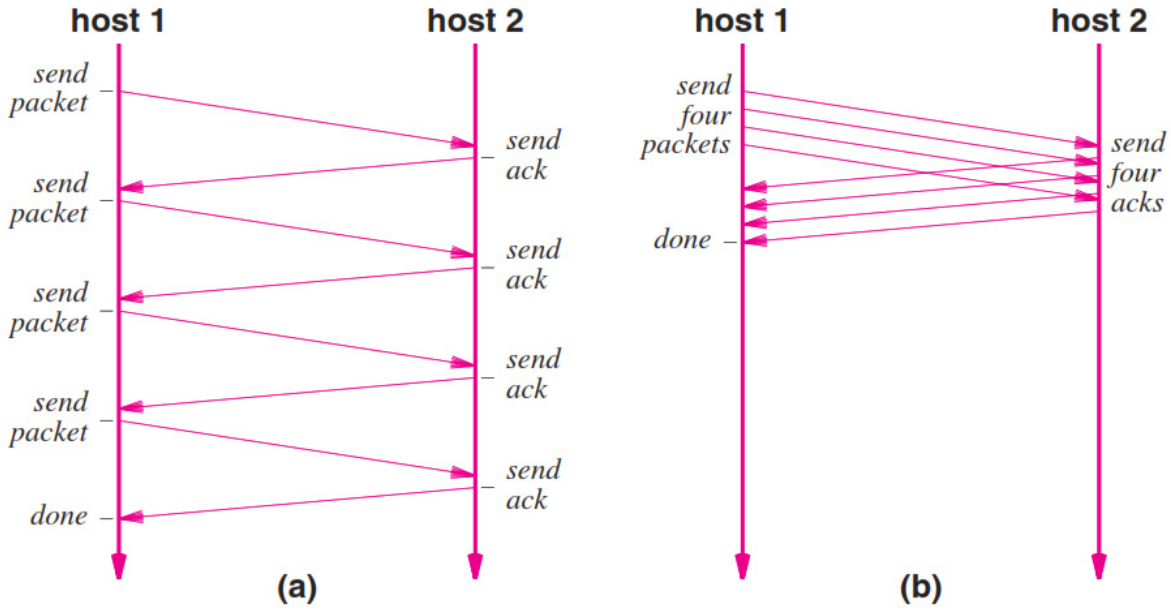
Meskipun protokol stop-and-go mencegah overrun, mereka menghasilkan throughput yang sangat rendah. Untuk memahami alasannya, pertimbangkan apa yang terjadi pada jaringan yang memiliki ukuran paket 1000 oktet, kapasitas throughput 2 Mbps, dan penundaan 50 milidetik. Perangkat keras jaringan dapat mengangkut 2 Mbps dari satu komputer ke komputer lain. Namun, setelah mentransmisikan sebuah paket, pengirim harus menunggu 100 msec sebelum mengirim paket lain (yaitu, 50 msec agar paket mencapai penerima dan 50 msec untuk acknowledgment untuk melakukan perjalanan kembali). Jadi, kecepatan maksimum di mana data dapat dikirim menggunakan stop-and-go adalah satu paket setiap 100 milidetik. Ketika dinyatakan sebagai bit rate, kecepatan maksimum yang dapat dicapai stop-and-go adalah 80.000 bps, yang hanya 4% dari kapasitas perangkat keras.

Untuk mendapatkan tingkat throughput yang tinggi, protokol transport menggunakan teknik kontrol aliran yang dikenal sebagai jendela geser. Pengirim dan penerima diprogram untuk menggunakan ukuran jendela tetap, yang merupakan jumlah maksimum data yang dapat dikirim sebelum pengakuan tiba. Misalnya, pengirim dan penerima mungkin menyetujui ukuran jendela empat paket. Pengirim mulai dengan data yang akan dikirim, mengekstrak data untuk mengisi empat paket (yaitu, jendela pertama), dan mengirimkan salinan dari setiap paket. Di sebagian besar protokol transport, pengirim menyimpan salinan jika transmisi ulang diperlukan. Penerima harus memiliki ruang buffer yang telah dialokasikan sebelumnya untuk seluruh jendela. Jika sebuah paket tiba secara berurutan, penerima meneruskan paket ke aplikasi penerima dan mengirimkan pengakuan ke pengirim. Ketika pengakuan tiba, pengirim membuang salinan paket yang diakui dan mengirimkan paket berikutnya. Gambar 7.2 mengilustrasikan mengapa mekanisme ini dikenal sebagai jendela geser.



Gambar 7.2 Ilustrasi jendela geser pada (a) posisi awal, (b) tengah, dan (c) akhir.

Jendela geser dapat meningkatkan throughput secara dramatis. Untuk memahami alasannya, bandingkan urutan transmisi dengan skema stop-and-go dan skema sliding window. Gambar 7.3 berisi perbandingan untuk transmisi 4-paket.



Gambar 7.3 Perbandingan transmisi menggunakan (a) stop-and-go, dan (b) sliding window.

Pada Gambar 7.3a, pengirim mentransmisikan empat paket, tetapi menunggu pengakuan sebelum mengirim setiap paket yang berurutan. Jika penundaan yang diperlukan untuk mengirim satu paket pada satu perjalanan melalui jaringan adalah N, total waktu yang diperlukan untuk mengirim empat paket adalah 8N. Pada Gambar 7.3b, pengirim mengirimkan semua paket di jendela sebelum menunggu. Gambar menunjukkan penundaan kecil antara transmisi paket berturut-turut karena transmisi tidak pernah seketika — waktu yang singkat (biasanya beberapa mikrodetik) diperlukan untuk perangkat keras untuk menyelesaikan transmisi paket dan mulai mengirimkan paket berikutnya. Jadi, total waktu yang diperlukan untuk mengirim empat paket adalah 2N + , di mana menunjukkan penundaan yang kecil.

Untuk memahami pentingnya jendela geser, bayangkan komunikasi yang diperluas yang melibatkan banyak paket. Dalam kasus seperti itu, total waktu yang dibutuhkan untuk transmisi sangat besar sehingga dapat diabaikan. Untuk jaringan seperti itu, protokol jendela geser dapat meningkatkan kinerja secara substansial. Potensi peningkatannya adalah:

$$Tw = Tg \times W \quad (7.1)$$

di mana Tw adalah throughput yang dapat dicapai dengan protokol sliding window, Tg adalah throughput yang dapat dicapai dengan protokol stop-and-go, dan W adalah ukuran jendela. Persamaan tersebut menjelaskan mengapa protokol jendela geser yang diilustrasikan pada Gambar 7.3b memiliki kira-kira empat kali throughput protokol stop-and-go pada Gambar 7.3a. Tentu saja, throughput tidak dapat ditingkatkan secara sembarangan hanya dengan memperbesar ukuran jendela. Bandwidth jaringan yang mendasari memaksakan batas atas - bit tidak dapat dikirim lebih cepat daripada yang dapat dibawa oleh perangkat keras. Dengan demikian, persamaan dapat ditulis ulang:

$$Tw = \min(B, Tg \times W) \quad (7.2)$$

di mana B adalah bandwidth perangkat keras yang mendasarinya.

7.5 Teknik Menghindari Kemacetan

Untuk memahami betapa mudahnya kongesti dapat terjadi, pertimbangkan empat host yang dihubungkan oleh dua sakelar seperti yang diilustrasikan Gambar 7.4

Gambar 7.4 Empat host yang dihubungkan oleh dua sakelar.

Asumsikan setiap koneksi pada gambar beroperasi pada 1 Gbps, dan pertimbangkan apa yang terjadi jika kedua komputer yang terhubung ke switch 1 mencoba mengirim data ke komputer yang terhubung ke switch 2. Switch 1 menerima data dengan kecepatan agregat 2 Gbps, tetapi dapat hanya meneruskan 1 Gbps untuk beralih 2. Situasi ini dikenal sebagai kemacetan. Bahkan jika switch

menyimpan paket sementara dalam memori, hasil kemacetan dalam penundaan meningkat. Jika kemacetan berlanjut, sakelar akan kehabisan memori dan mulai membuang paket. Meskipun transmisi ulang dapat digunakan untuk memulihkan paket yang hilang, transmisi ulang mengirimkan lebih banyak paket ke dalam jaringan. Jadi, jika situasinya terus berlanjut, seluruh jaringan dapat menjadi tidak dapat digunakan; kondisi ini dikenal sebagai kemacetan runtuh. Di Internet, kemacetan biasanya terjadi di router. Protokol transport berusaha untuk menghindari kemacetan kemacetan dengan memantau jaringan dan bereaksi cepat setelah kemacetan dimulai. Ada dua pendekatan dasar:

- Atur sistem perantara (yaitu, router) untuk memberi tahu pengirim ketika terjadi kemacetan
- Gunakan peningkatan penundaan atau kehilangan paket sebagai perkiraan kemacetan

Skema sebelumnya diimplementasikan baik dengan meminta router mengirim pesan khusus ke sumber paket ketika terjadi kemacetan atau dengan mengatur router sedikit di header setiap paket yang mengalami penundaan yang disebabkan oleh kemacetan. Ketika pendekatan kedua digunakan, komputer yang menerima paket menyertakan informasi dalam pengakuan untuk menginformasikan pengirim asli. Menggunakan delay dan loss untuk memperkirakan kemacetan masuk akal di Internet karena:

Perangkat keras jaringan modern bekerja dengan baik; sebagian besar penundaan dan kerugian disebabkan oleh kemacetan, bukan kegagalan perangkat keras.

Respon yang tepat untuk kemacetan terdiri dari pengurangan tingkat di mana paket-paket sedang ditransmisikan. Protokol jendela geser dapat mencapai efek pengurangan laju dengan mengurangi ukuran jendela untuk sementara.

7.6 Seni Desain Protokol

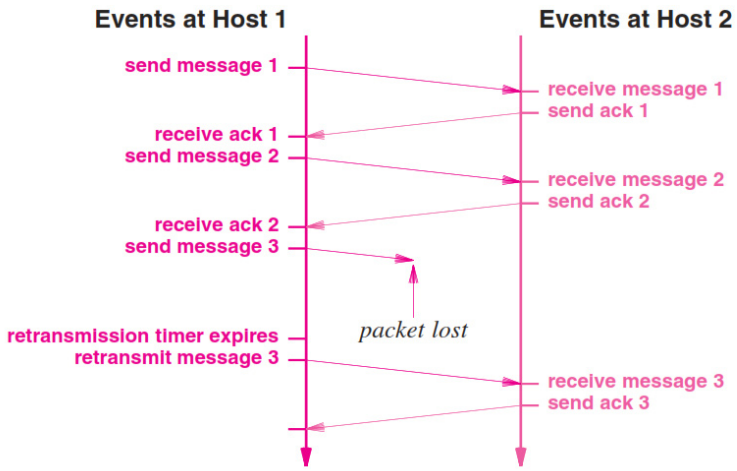
Meskipun teknik yang diperlukan untuk memecahkan masalah tertentu sudah dikenal luas, desain protokol tidak sepele karena dua alasan. Pertama, untuk membuat komunikasi menjadi efisien, detail harus dipilih dengan hati-hati — kesalahan desain kecil dapat mengakibatkan operasi yang salah, paket yang tidak diperlukan, atau penundaan. Misalnya, jika nomor urut digunakan, setiap paket harus berisi nomor urut di header paket. Bidang harus cukup besar sehingga nomor urut tidak sering digunakan kembali, tetapi cukup kecil untuk menghindari pemborosan bandwidth yang tidak perlu. Kedua, mekanisme protokol dapat berinteraksi dengan cara yang tidak terduga. Misalnya, pertimbangkan interaksi antara kontrol aliran dan mekanisme kontrol kemacetan. Skema jendela geser secara agresif menggunakan lebih banyak bandwidth jaringan yang mendasarinya untuk meningkatkan throughput. Mekanisme kontrol kemacetan melakukan sebaliknya dengan mengurangi jumlah paket yang dimasukkan untuk mencegah jaringan runtuh; keseimbangan antara jendela geser dan kontrol kemacetan bisa jadi rumit, dan desain yang melakukan keduanya dengan baik itu sulit. Artinya, kontrol aliran agresif dapat menyebabkan kemacetan dan kontrol kemacetan konservatif dapat menurunkan throughput lebih dari yang diperlukan. Desain yang mencoba untuk beralih dari perilaku agresif ke konservatif ketika terjadi kemacetan cenderung berosilasi — mereka perlahan-lahan meningkatkan penggunaan bandwidth hingga jaringan mulai mengalami kemacetan, mengurangi penggunaan hingga jaringan menjadi stabil, dan kemudian mulai meningkat lagi.

Reboot sistem komputer menimbulkan tantangan serius lainnya untuk desain protokol transport. Bayangkan situasi di mana dua program aplikasi membuat koneksi, mulai mengirim data, dan kemudian komputer yang menerima data melakukan boot ulang. Meskipun perangkat lunak protokol pada

komputer yang di-boot ulang tidak memiliki pengetahuan tentang koneksi, perangkat lunak protokol pada komputer pengirim menganggap koneksi tersebut valid. Jika protokol tidak dirancang dengan hati-hati, paket duplikat dapat menyebabkan komputer salah membuat sambungan dan mulai menerima data di tengah aliran.

7.7 Teknik Yang Digunakan Dalam TCP Untuk Menangani Packet Loss

Manakah dari teknik yang disebutkan di atas yang digunakan TCP untuk mencapai transfer yang andal? Jawabannya rumit karena TCP menggunakan berbagai skema yang digabungkan dengan cara baru. Seperti yang diharapkan TCP menggunakan transmisi ulang untuk mengkompensasi kehilangan paket. Karena TCP menyediakan aliran data di kedua arah, kedua sisi komunikasi berpartisipasi dalam transmisi ulang. Ketika TCP menerima data, ia mengirimkan pengakuan kembali ke pengirim. Setiap kali mengirim data, TCP memulai timer, dan mentransmisikan ulang data jika timer berakhir. Dengan demikian, transmisi ulang TCP dasar beroperasi seperti yang diilustrasikan Gambar 7.5.



Gambar 7.5 Ilustrasi transmisi ulang TCP setelah kehilangan paket.

Skema transmisi ulang TCP adalah kunci keberhasilannya karena menangani komunikasi melintasi jalur yang berubah-ubah melalui Internet. Misalnya, satu aplikasi mungkin mengirim data melalui saluran satelit ke komputer di negara lain, sementara aplikasi lain mengirim data melalui jaringan area lokal ke komputer di ruangan sebelah. TCP harus siap untuk mengirim ulang pesan apa pun yang hilang di kedua koneksi. Pertanyaannya adalah: berapa lama TCP harus menunggu sebelum mengirim ulang? Pengakuan dari komputer di jaringan area lokal diharapkan tiba dalam beberapa milidetik, tetapi koneksi satelit membutuhkan ratusan milidetik. Di satu sisi, menunggu terlalu lama untuk pengakuan seperti itu membuat jaringan menganggur dan tidak memaksimalkan throughput. Jadi, pada jaringan area lokal, TCP seharusnya tidak menunda waktu yang lama sebelum melakukan transmisi ulang. Di sisi lain, transmisi ulang dengan cepat tidak bekerja dengan baik pada koneksi satelit karena lalu lintas yang tidak perlu menghabiskan bandwidth jaringan dan menurunkan throughput.

TCP menghadapi tantangan yang lebih sulit daripada membedakan antara tujuan lokal dan jarak jauh: ledakan datagram dapat menyebabkan kemacetan, yang menyebabkan penundaan transmisi di sepanjang jalur tertentu untuk berubah dengan cepat. Faktanya, total waktu yang dibutuhkan untuk mengirim pesan dan menerima pengakuan dapat bertambah atau berkurang dengan urutan besarnya dalam beberapa milidetik.

Poin Penting

Penundaan yang diperlukan data untuk mencapai tujuan dan pengakuan untuk kembali tergantung pada lalu lintas di Internet serta jarak ke tujuan. Karena TCP memungkinkan beberapa program aplikasi untuk berkomunikasi dengan beberapa tujuan secara bersamaan dan kondisi lalu lintas mempengaruhi penundaan, TCP harus menangani berbagai penundaan yang dapat berubah dengan cepat.

7.8 Transmisi Ulang Adaptif

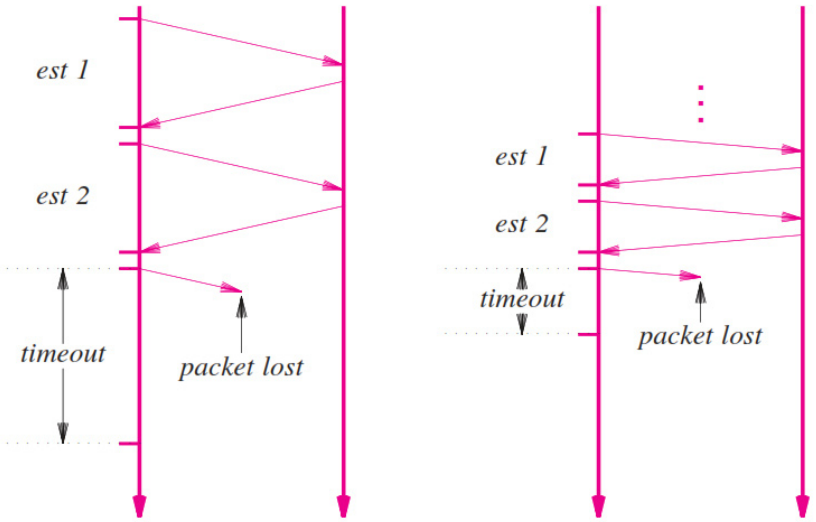
Sebelum TCP ditemukan, protokol transport menggunakan nilai tetap untuk penundaan transmisi ulang — perancang protokol atau manajer jaringan memilih nilai yang cukup besar untuk penundaan yang diharapkan. Desainer yang bekerja pada TCP menyadari bahwa batas waktu tetap tidak akan beroperasi dengan baik untuk Internet. Dengan demikian, mereka memilih untuk membuat transmisi ulang TCP adaptif. Artinya, TCP memantau penundaan saat ini pada setiap koneksi, dan mengadaptasi (yaitu, mengubah) pengatur waktu transmisi ulang untuk mengakomodasi perubahan kondisi.

Bagaimana TCP dapat memantau penundaan Internet? Faktanya, TCP tidak dapat mengetahui penundaan yang tepat untuk semua bagian Internet setiap saat. Sebaliknya, TCP memperkirakan penundaan bolak-balik untuk setiap koneksi aktif dengan mengukur waktu yang dibutuhkan untuk menerima respons. Setiap kali mengirim pesan yang mengharapkan tanggapan, TCP mencatat waktu di mana pesan itu dikirim. Ketika respons tiba, TCP mengurangi waktu pengiriman pesan dari waktu saat ini untuk menghasilkan perkiraan baru penundaan pulang-pergi untuk koneksi itu. Saat mengirimkan paket data dan menerima pengakuan, TCP menghasilkan urutan perkiraan bolak-balik dan menggunakan fungsi statistik untuk menghasilkan rata-rata tertimbang. Selain rata-rata tertimbang, TCP menyimpan perkiraan varians, dan menggunakan kombinasi linier dari estimasi mean dan varians saat menghitung waktu di mana transmisi ulang diperlukan.

Pengalaman menunjukkan bahwa transmisi ulang adaptif TCP bekerja dengan baik. Menggunakan varians membantu TCP bereaksi dengan cepat ketika penundaan meningkat mengikuti ledakan paket. Menggunakan rata-rata tertimbang membantu TCP mengatur ulang penghitung waktu transmisi ulang jika penundaan kembali ke nilai yang lebih rendah setelah ledakan sementara. Ketika penundaan tetap konstan, TCP menyesuaikan batas waktu pengiriman ulang ke nilai yang sedikit lebih lama dari penundaan pulang-pergi rata-rata. Ketika penundaan mulai bervariasi, TCP menyesuaikan batas waktu pengiriman ulang ke nilai yang lebih besar dari rata-rata untuk mengakomodasi puncak.

7.9 Perbandingan Waktu Transmisi Ulang

Untuk memahami bagaimana transmisi ulang adaptif membantu TCP memaksimalkan throughput pada setiap koneksi, pertimbangkan kasus kehilangan paket pada dua koneksi yang memiliki penundaan bolak-balik yang berbeda. Misalnya, Gambar 7.6 mengilustrasikan lalu lintas pada dua koneksi tersebut.



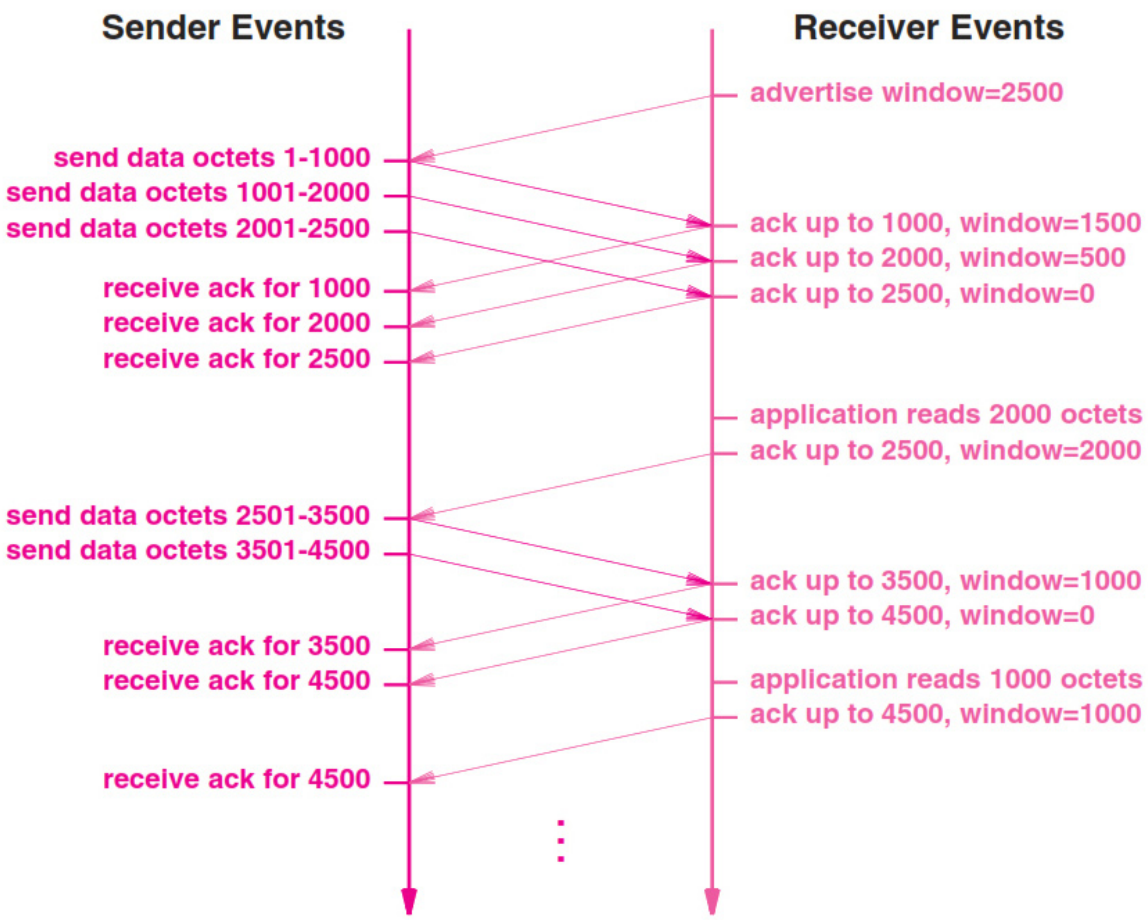
Gambar 7.6 Batas waktu dan transmisi ulang pada dua koneksi TCP yang memiliki penundaan pulang-pergi yang berbeda.

Seperti yang ditunjukkan gambar, TCP menetapkan batas waktu pengiriman ulang menjadi sedikit lebih lama daripada penundaan pulang-pergi rata-rata. Jika penundaannya besar, TCP menggunakan batas waktu pengiriman ulang yang besar; jika penundaannya kecil, TCP menggunakan batas waktu yang kecil. Tujuannya adalah untuk menunggu cukup lama untuk menentukan bahwa sebuah paket hilang, tanpa menunggu lebih lama dari yang diperlukan.

7.10 Buffer, Kontrol Aliran, dan Windows

TCP menggunakan mekanisme jendela untuk mengontrol aliran data. Tidak seperti skema jendela berbasis paket sederhana yang dijelaskan di atas, jendela TCP diukur dalam byte. Ketika koneksi dibuat, setiap ujung koneksi mengalokasikan buffer untuk menampung data yang masuk dan mengirimkan ukuran buffer ke ujung lainnya. Saat data tiba, TCP penerima mengirimkan pengakuan, yang menentukan ukuran buffer yang tersisa. TCP menggunakan istilah jendela untuk merujuk pada jumlah ruang buffer yang tersedia setiap saat; pemberitahuan yang menentukan ukuran jendela dikenal sebagai iklan jendela. Penerima mengirimkan iklan jendela dengan setiap pengakuan.

Jika aplikasi penerima dapat membaca data secepat tiba, penerima akan mengirimkan iklan jendela positif bersama dengan setiap pengakuan. Namun, jika sisi pengirim beroperasi lebih cepat daripada sisi penerima (misalnya, karena CPU lebih cepat), data yang masuk pada akhirnya akan mengisi buffer penerima, menyebabkan penerima mengiklankan jendela nol. Pengirim yang menerima iklan jendela nol harus berhenti mengirim sampai penerima kembali mengiklankan jendela positif. Gambar 7.7 mengilustrasikan iklan jendela.



Gambar 7.7 Urutan pesan yang menggambarkan aliran TCP untuk ukuran segmen maksimum 1000 byte.

Pada gambar, pengirim menggunakan ukuran segmen maksimum 1000 byte. Transfer dimulai ketika receiver mengumumkan ukuran jendela awal 2500 byte. Pengirim segera mentransmisikan tiga segmen, dua yang berisi 1000 byte data dan satu yang berisi 500 byte. Saat segmen tiba, penerima menghasilkan pengakuan dengan ukuran jendela dikurangi dengan jumlah data yang telah tiba.

Dalam contoh, tiga segmen pertama mengisi buffer penerima lebih cepat daripada yang dapat dikonsumsi oleh aplikasi penerima. Dengan demikian, ukuran jendela yang diiklankan mencapai nol, dan pengirim tidak dapat mengirimkan data tambahan. Setelah aplikasi penerima menggunakan 2000 byte data, TCP penerima mengirimkan pengakuan tambahan yang mengiklankan ukuran jendela 2000 byte. Ukuran jendela selalu diukur di luar data yang diakui, sehingga penerima mengiklankan bahwa ia dapat menerima 2000 byte di luar 2500 yang telah diterimanya. Pengirim merespon dengan mengirimkan dua segmen tambahan. Saat setiap segmen tiba, penerima mengirimkan pemberitahuan dengan ukuran jendela dikurangi 1000 byte (yaitu, jumlah data yang telah tiba).

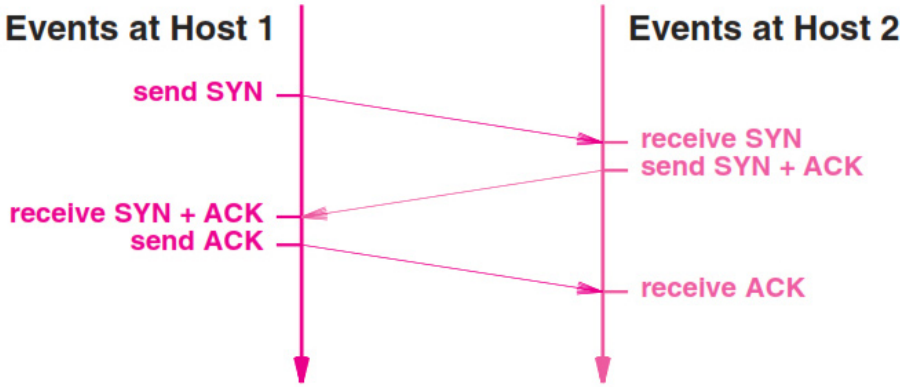
Sekali lagi, ukuran jendela mencapai nol, menyebabkan pengirim menghentikan transmisi. Akhirnya, aplikasi penerima menggunakan sebagian data, dan TCP penerima mengirimkan pengakuan dengan ukuran jendela positif. Jika pengirim memiliki lebih banyak data yang menunggu untuk dikirim, pengirim dapat melanjutkan untuk mengirimkan segmen lain.

7.11 Model TCP: Three-Way Handshake

Untuk menjamin bahwa koneksi dibuat atau diakhiri dengan andal, TCP menggunakan 3-way handshake di mana tiga pesan dipertukarkan. Selama 3-way handshake untuk memulai koneksi, masing-masing pihak mengirimkan pesan kontrol yang menentukan ukuran buffer awal (untuk kontrol aliran) dan nomor urut. Para ilmuwan telah membuktikan bahwa pertukaran 3-arah TCP diperlukan dan cukup untuk memastikan kesepakatan yang tidak ambigu meskipun terjadi kehilangan paket, duplikasi, penundaan, dan pemutaran ulang†. Selanjutnya, jabat tangan memastikan bahwa TCP tidak akan membuka atau menutup koneksi sampai kedua ujungnya setuju.

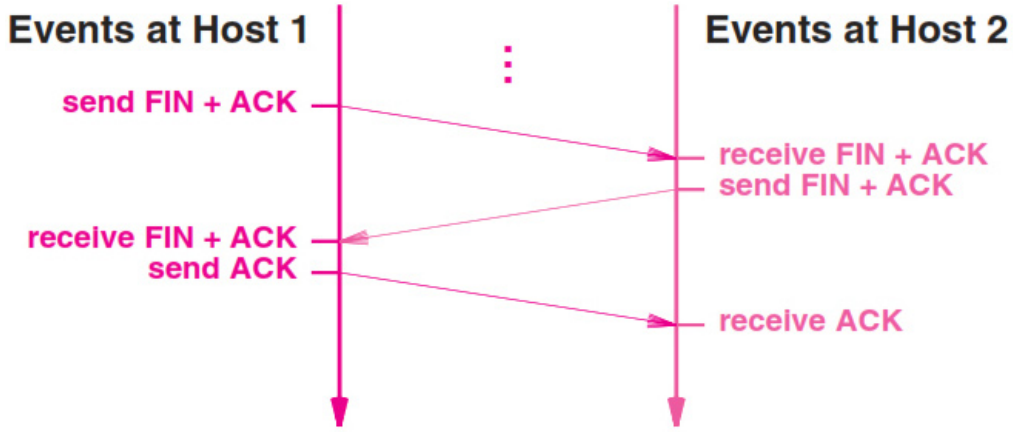
TCP menggunakan istilah segmen sinkronisasi (segmen SYN) untuk menggambarkan pesan kontrol yang digunakan dalam 3-way handshake untuk membuat koneksi, dan istilah segmen FIN (kependekan dari segmen akhir) untuk menggambarkan pesan kontrol yang digunakan dalam 3-way handshake untuk menutup koneksi. Gambar 7.8 mengilustrasikan 3-way handshake yang digunakan untuk membuat koneksi.

Aspek kunci dari 3-way handshake yang digunakan untuk membuat koneksi melibatkan pemilihan nomor urut. TCP mengharuskan setiap ujung untuk menghasilkan nomor urut 32-bit acak yang menjadi urutan awal untuk data yang dikirim. Jika aplikasi mencoba membuat koneksi TCP baru setelah komputer di-boot ulang, TCP memilih nomor acak baru. Karena kemungkinan memilih nilai acak yang cocok dengan urutan yang digunakan pada koneksi sebelumnya rendah, TCP menghindari masalah pemutaran ulang. Artinya, jika sepasang program aplikasi menggunakan TCP untuk berkomunikasi, menutup koneksi, dan kemudian membuat koneksi baru, nomor urut pada koneksi baru akan berbeda dari nomor urut yang digunakan pada koneksi lama, memungkinkan TCP untuk menolak penundaan. paket yang datang.



Gambar 7.8 3-way handshake yang digunakan untuk membuat koneksi TCP.

3-way handshake yang digunakan untuk menutup koneksi menggunakan segmen FIN. Pengakuan dikirim di setiap arah bersama dengan FIN untuk menjamin bahwa semua data telah tiba sebelum koneksi dihentikan. Gambar 7.9 mengilustrasikan pertukaran tersebut.



Gambar 7.9 3-way handshake yang digunakan untuk menutup sambungan.

7.12 Kontrol Kemacetan TCP

Salah satu aspek yang paling menarik dari TCP adalah mekanisme untuk kontrol kemacetan. Ingatlah bahwa di Internet, penundaan atau kehilangan paket lebih mungkin disebabkan oleh kemacetan daripada kegagalan perangkat keras, dan transmisi ulang itu dapat memperburuk masalah kemacetan dengan menyuntikkan salinan paket tambahan. Untuk menghindari kemacetan kemacetan, TCP menggunakan perubahan penundaan sebagai ukuran kemacetan, dan menanggapi kemacetan dengan mengurangi tingkat transmisi ulang data.

Meskipun kami berpikir untuk mengurangi kecepatan transmisi, TCP tidak menghitung kecepatan data. Sebaliknya, TCP mendasarkan transmisi pada ukuran buffer. Artinya, penerima mengiklankan ukuran jendela, dan pengirim dapat mengirimkan data untuk mengisi jendela penerima sebelum ACK diterima. Untuk mengontrol kecepatan data, TCP memberlakukan batasan pada ukuran jendela — dengan mengurangi sementara ukuran jendela, pengiriman TCP secara efektif mengurangi kecepatan data.

Poin Penting

Secara konseptual, protokol transport harus mengurangi laju transmisi ketika terjadi kemacetan. Karena menggunakan jendela ukuran variabel, TCP dapat mencapai pengurangan kecepatan data dengan mengurangi ukuran jendela sementara. Dalam kasus ekstrim di mana kerugian terjadi, TCP sementara mengurangi jendela menjadi setengah dari nilai saat ini.

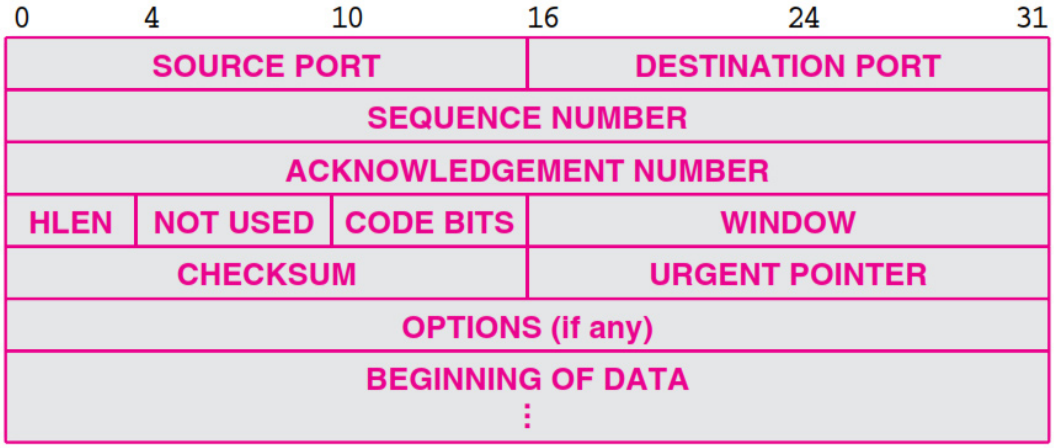
TCP menggunakan mekanisme kontrol kemacetan khusus saat memulai koneksi baru atau saat pesan hilang. Alih-alih mentransmisikan data yang cukup untuk mengisi buffer penerima (yaitu, ukuran jendela penerima), TCP memulai dengan mengirimkan satu pesan yang berisi data. Jika pengakuan datang tanpa kehilangan tambahan, TCP menggandakan jumlah data yang dikirim dan mengirim dua pesan tambahan. Jika kedua pengakuan tiba, TCP mengirim empat pesan, dan seterusnya. Peningkatan eksponensial berlanjut hingga TCP mengirim setengah dari jendela penerima yang diiklankan. Ketika setengah dari ukuran jendela asli tercapai, TCP memperlambat laju kenaikan, dan meningkatkan ukuran jendela secara linier selama kemacetan tidak terjadi. Pendekatan ini dikenal sebagai slow start.

Mekanisme kontrol kemacetan TCP merespon dengan baik terhadap peningkatan lalu lintas. Dengan mundur dengan cepat, TCP mampu mengurangi kemacetan. Intinya, TCP menghindari penambahan transmisi ulang ketika Internet menjadi padat. Lebih penting lagi, jika semua TCP mengikuti standar, skema kontrol kemacetan berarti bahwa semua pengirim mundur ketika kemacetan terjadi dan kemacetan kemacetan dihindari.

7.13 Format Segmen TCP

TCP menggunakan format tunggal untuk semua pesan, termasuk pesan yang membawa data, pesan yang membawa pengakuan, dan pesan yang merupakan bagian dari 3-way handshake yang digunakan untuk membuat atau mengakhiri koneksi (SYN dan FIN). TCP menggunakan istilah segmen untuk merujuk ke pesan. Gambar 7.10 mengilustrasikan format segmen TCP.

Untuk memahami format segmen, perlu diingat bahwa koneksi TCP berisi dua aliran data, satu mengalir di setiap arah. Jika aplikasi di setiap ujung mengirimkan data secara bersamaan, TCP dapat mengirim satu segmen yang membawa data keluar, pengakuan untuk data yang masuk, dan iklan jendela yang menentukan jumlah ruang buffer tambahan yang tersedia untuk data yang masuk. Dengan demikian, beberapa bidang dalam segmen mengacu pada aliran data yang bergerak dalam arah maju, sementara bidang lain merujuk pada aliran data yang berjalan dalam arah sebaliknya.



Gambar 7.10 Format segmen TCP yang digunakan untuk pesan data dan kontrol.

Saat komputer mengirim segmen, kolom ACKNOWLEDGMENT NUMBER dan WINDOW merujuk ke data yang masuk: ACKNOWLEDGMENT NUMBER menentukan nomor urut data yang diharapkan berikutnya, dan WINDOW menentukan berapa banyak ruang buffer tambahan yang tersedia di luar data yang diakui. Pengakuan selalu mengacu pada posisi pertama yang datanya hilang; jika segmen tiba rusak, TCP penerima menghasilkan pengakuan yang sama beberapa kali sampai data yang hilang tiba. Bidang NOMOR URUTAN mengacu pada data keluar. Ini memberikan nomor urut byte pertama data yang dibawa dalam segmen. Penerima menggunakan nomor urut untuk menyusun ulang segmen yang datang rusak dan untuk menghitung nomor pengakuan. Field DESTINATION PORT mengidentifikasi program aplikasi mana pada komputer penerima yang harus menerima data, sedangkan field SOURCE PORT mengidentifikasi program aplikasi yang mengirim data. Terakhir, bidang CHECKSUM berisi checksum yang mencakup header segmen TCP dan data.

Ide-ide kunci mengenai urutan dan penomoran pengakuan adalah:

Bidang SEQUENCE NUMBER dalam segmen TCP memberikan nomor urut untuk byte pertama data yang dibawa dalam segmen dalam arah maju; sebuah NOMOR PENGAKUAN memberikan nomor urut pertama yang datanya hilang dalam arah sebaliknya.

7.14 Ringkasan

Transmission Control Protocol (TCP) adalah protokol transport utama dalam rangkaian protokol TCP/IP. TCP menyediakan program aplikasi dengan layanan transportasi aliran yang andal, terkontrol aliran, dupleks penuh. Setelah meminta TCP untuk membuat koneksi, program aplikasi dapat menggunakan koneksi untuk mengirim atau menerima data; TCP menjamin pengiriman data secara berurutan tanpa duplikasi. Akhirnya, ketika kedua aplikasi selesai menggunakan koneksi, mereka meminta koneksi dihentikan.

TCP pada satu komputer berkomunikasi dengan TCP pada komputer lain dengan bertukar pesan. Semua pesan dari satu TCP ke TCP lainnya menggunakan format segmen TCP, termasuk pesan yang membawa data, pengakuan, dan iklan jendela, serta pesan yang digunakan untuk membuat dan mengakhiri koneksi. Setiap segmen TCP berjalan dalam datagram IP.

Secara umum, protokol transport menggunakan berbagai mekanisme untuk memastikan layanan yang andal. TCP memiliki kombinasi teknik yang sangat kompleks yang telah terbukti sangat sukses. Selain checksum di setiap segmen, TCP mengirim ulang pesan yang hilang. Agar berguna di Internet di mana penundaan bervariasi dari waktu ke waktu, batas waktu pengiriman ulang TCP bersifat adaptif — TCP mengukur penundaan perjalanan pulang pergi saat ini secara terpisah untuk setiap koneksi, dan menggunakan rata-rata tertimbang waktu perjalanan pulang pergi untuk memilih batas waktu pengiriman ulang.

Latihan

1. Asumsikan bahwa pesan yang dikirim antara dua program dapat hilang, diduplikasi, tertunda, atau dikirim secara tidak berurutan. Rancang protokol yang andal yang memungkinkan kedua program setuju untuk berkomunikasi. Berikan desain Anda kepada seseorang, dan lihat apakah mereka dapat menemukan urutan kehilangan, duplikasi, dan penundaan yang membuat protokol gagal.
2. Sebutkan fitur-fitur TCP.
3. Lapisan apa dari tumpukan protokol yang digunakan pada router? Tuan rumah?
4. Apa masalah utama yang harus dipecahkan oleh protokol transport untuk mencapai transfer yang andal?
5. Apa saja teknik yang digunakan protokol transport?
6. Saat menggunakan jendela geser ukuran N, berapa banyak paket yang dapat dikirim tanpa memerlukan satu ACK untuk diterima?
7. Mengapa protokol stop-and-go memiliki throughput yang sangat rendah melalui saluran satelit GEO yang beroperasi pada dua megabit per detik?
8. Perluas diagram pada Gambar 7.3 untuk menunjukkan transmisi enam belas paket yang berurutan.
9. Apa penyebab utama keterlambatan dan hilangnya paket di Internet?

10. Bagaimana TCP menangani kehilangan paket?
11. Apa yang terjadi pada throughput jika protokol menunggu terlalu lama untuk dikirim ulang? Jika protokol tidak menunggu cukup lama untuk mengirim ulang?
12. Bagaimana TCP menghitung batas waktu untuk transmisi ulang?
13. Apa yang dikontrol oleh ukuran jendela TCP?
14. Apa itu SYN? Sebuah FIN?
15. Misalkan dua program menggunakan TCP untuk membuat koneksi, berkomunikasi, mengakhiri koneksi, dan kemudian membuka koneksi baru. Selanjutnya misalkan pesan FIN yang dikirim untuk mematikan koneksi pertama diduplikasi dan ditunda hingga koneksi kedua dibuat. Jika salinan FIN lama dikirimkan, apakah TCP akan menghentikan koneksi baru? Mengapa atau mengapa tidak?
16. Masalah apa dalam jaringan yang menyebabkan TCP mengurangi ukuran jendela untuk sementara?
17. Tulis program komputer untuk mengekstrak dan mencetak bidang di header segmen TCP.
18. Apakah checksum TCP diperlukan, atau dapatkah TCP bergantung pada checksum IP untuk memastikan integritas? Menjelaskan.

Bab 8 Perutean Internet dan Protokol Perutean

Bab ini akan membahas tentang:

- Aspek penting dari teknologi internetworking: penyebaran informasi perutean yang digunakan untuk membuat dan memperbarui tabel penerusan
- Bagaimana tabel penerusan dibangun, dan menjelaskan bagaimana perangkat lunak perutean memperbarui tabel, sesuai kebutuhan
- Perbedaan antara protokol perutean interior dan eksterior.

8.1 Perutean Statis dan Dinamis

Routing merupakan hal yang sangat vital dalam dunia jaringan. Seperti yang sudah disebutkan di atas, routing adalah proses meneruskan paket-paket data dari satu jaringan ke yang lainnya. Proses ini dapat diartikan juga sebagai penggabungan beberapa jaringan untuk meneruskan paket data dari satu jaringan ke jaringan selanjutnya. Perutean IP dapat dipartisi menjadi dua kategori besar:

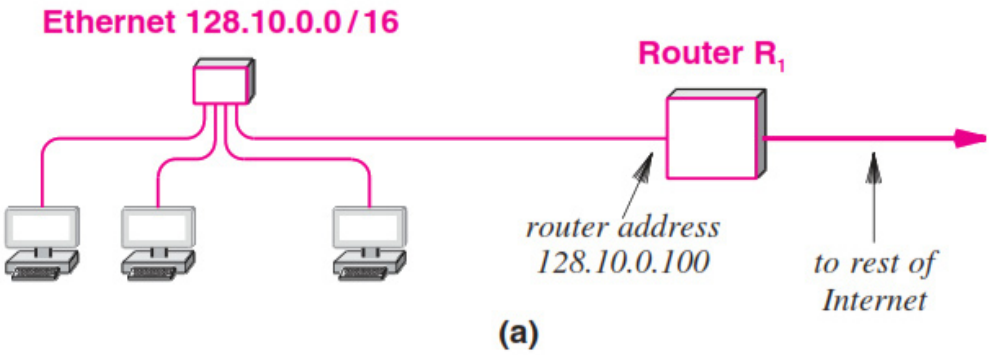
- Perutean statis
- Perutean dinamis

Istilah perutean statis mencirikan pendekatan yang membuat tabel penerusan saat sistem dimulai dan tidak mengubah entri kecuali jika administrator mengubahnya secara manual. Sebaliknya, istilah perutean dinamis mencirikan pendekatan di mana perangkat lunak propagasi rute berjalan pada sistem dan terus memperbarui tabel penerusan untuk memastikan bahwa setiap datagram mengikuti rute yang optimal. Artinya, perangkat lunak berkomunikasi dengan sistem lain untuk mempelajari rute optimal ke setiap tujuan, dan terus-menerus memeriksa kegagalan jaringan yang menyebabkan rute berubah. Ironisnya, perutean dinamis dimulai persis seperti perutean statis dengan memuat serangkaian rute awal ke dalam tabel penerusan saat sistem melakukan booting.

8.2 Perutean Statis dalam Host dan Rute Default

Perutean statis mudah, mudah ditentukan, dan tidak memerlukan perangkat lunak perutean tambahan. Itu tidak mengkonsumsi bandwidth, dan tidak ada siklus CPU yang diperlukan untuk menyebarkan informasi perutean. Namun, perutean statis relatif tidak fleksibel; itu tidak dapat mengakomodasi kegagalan jaringan atau perubahan topologi.

Di mana perutean statis digunakan? Sebagian besar host menggunakan perutean statis, terutama dalam kasus di mana host memiliki satu koneksi jaringan dan satu router menghubungkan jaringan ke seluruh Internet. Sebagai contoh, perhatikan arsitektur yang diilustrasikan Gambar 8.1. Empat host terhubung ke Ethernet, yang terhubung ke seluruh Internet melalui router R1.



(a)

Net	Mask	Next hop
128.10.0.0	255.255.0.0	direct
default	0.0.0.0	128.10.0.100

(b)

Gambar 8.1 (a) Koneksi tipikal ke Internet, dan (b) tabel penerusan statis yang digunakan di setiap host.

Seperti yang ditunjukkan gambar, tabel penerusan statis dengan dua entri cukup untuk host biasa. Satu entri menentukan alamat jaringan yang terhubung langsung, dan entri lainnya menentukan bahwa router R1 menyediakan rute default untuk semua tujuan lainnya. Saat aplikasi menghasilkan datagram untuk komputer di jaringan lokal (mis
printer), entri pertama dalam tabel penerusan mengarahkan IP untuk mengirimkan datagram langsung ke tujuannya. Ketika datagram ditujukan untuk tujuan lain di Internet, entri kedua dalam tabel mengarahkan IP untuk mengirim datagram ke router, R1.

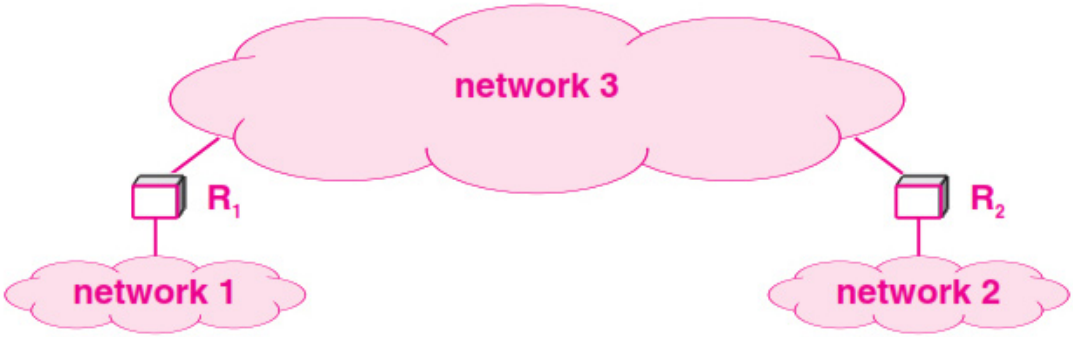
Poin Penting

Sebagian besar host Internet menggunakan perutean statis. Tabel penerusan host berisi dua entri: satu untuk jaringan yang dilampirkan host dan entri=default yang mengarahkan semua lalu lintas lain ke router tertentu.

8.3 Perutean dan Router Dinamis

Bisakah router di Internet menggunakan perutean statis dengan cara yang sama seperti yang dilakukan host? Meskipun ada kasus di mana router menggunakan perutean statis, sebagian besar perute menggunakan perutean dinamis. Untuk memahami kasus luar biasa di mana perutean statis cukup untuk router, lihat Gambar 8.1 lagi. Kita dapat membayangkan bahwa angka tersebut sesuai dengan sebuah organisasi kecil yang merupakan pelanggan dari ISP. Semua lalu lintas yang meninggalkan situs pelanggan melalui router R1 harus melakukan perjalanan ke ISP (misalnya, melalui koneksi DSL). Karena rute tidak pernah berubah, tabel penerusan di router R1 bisa statis. Selanjutnya, tabel penerusan di R1 dapat menggunakan rute default seperti halnya tabel penerusan di host.

Meskipun ada beberapa pengecualian, perutean statis dan perutean default tidak cukup untuk sebagian besar perute; penggunaannya terbatas pada konfigurasi khusus seperti di atas. Ketika dua ISP saling terhubung, keduanya perlu bertukar informasi perutean secara dinamis. Untuk mengetahui alasannya, pertimbangkan tiga jaringan yang saling terhubung oleh dua router seperti yang diilustrasikan pada Gambar 8.2.



Gambar 8.2 Ilustrasi arsitektur yang membutuhkan perutean dinamis.

Setiap router tahu tentang jaringan yang terhubung langsung. Jadi, router R1 tahu tentang jaringan 1 dan 3, dan R2 tahu tentang jaringan 2 dan 3. Namun, router R1 tidak tahu tentang jaringan 2, dan R2 tidak tahu tentang jaringan 1 karena tidak ada koneksi langsung. Untuk contoh sepele, sepertinya perutean statis akan sulit. Namun, pendekatan statis tidak berskala untuk menangani ribuan jaringan. Secara khusus, setiap kali ISP menambahkan jaringan pelanggan baru, informasi harus diteruskan ke seluruh Internet. Lebih penting lagi, proses manual terlalu lambat untuk mengakomodasi kegagalan jaringan dan kemacetan di Internet. Akibatnya, untuk memastikan bahwa semua router memperoleh informasi tentang bagaimana mencapai setiap tujuan yang mungkin, setiap router menjalankan perangkat lunak yang menggunakan protokol propagasi rute untuk bertukar informasi dengan router lain. Ketika mempelajari tentang perubahan rute, perangkat lunak perutean memperbarui tabel penerusan lokal. Selanjutnya, karena router bertukar informasi secara berkala, tabel penerusan lokal diperbarui terus menerus.

Pada Gambar 8.2, misalnya, router R1 dan R2 akan bertukar informasi perutean di seluruh jaringan 3. Akibatnya, perangkat lunak perutean di R2 akan menginstal rute ke jaringan 1 dan perangkat lunak yang berjalan di R1 akan menginstal rute ke jaringan 2. Jika router R2 crash, perangkat lunak propagasi rute di R1 akan mendeteksi bahwa jaringan 2 tidak lagi dapat dijangkau, dan akan menghapus rute dari tabel penerusannya. Kemudian, ketika R2 kembali terhubung, perangkat lunak perutean di

R1 akan menentukan bahwa jaringan 2 dapat dijangkau kembali, dan akan menginstal ulang rute tersebut.

Poin Penting

Setiap router menjalankan perangkat lunak perutean yang mempelajari tentang tujuan yang dapat dijangkau oleh perute lain, dan menginformasikan kepada perute lain tentang tujuan yang dapat dijangkaunya. Perangkat lunak perutean menggunakan informasi yang masuk untuk memperbarui tabel penerusan lokal secara terus menerus.

8.4 Perutean dalam Internet Global

Sejauh ini, kami telah menjelaskan perutean untuk konektivitas yang paling sepele (yaitu, situasi yang hanya melibatkan beberapa perute). Bagian ini membahas masalah yang lebih luas: perutean di Internet global. Bagian ini mempertimbangkan prinsip-prinsip umum; bagian selanjutnya menjelaskan protokol propagasi rute tertentu.

Kami mengatakan bahwa protokol propagasi rute memungkinkan satu router untuk bertukar informasi routing dengan yang lain. Namun, skema seperti itu tidak dapat menskalakan ke seluruh Internet — jika router di Internet mencoba bertukar informasi perutean dengan semua perute lain, lalu lintas yang dihasilkan akan membanjiri inti Internet. Untuk membatasi lalu lintas perutean, Internet menggunakan hierarki perutean. Router dan jaringan di Internet dibagi menjadi beberapa kelompok. Semua router dalam grup bertukar informasi perutean. Kemudian, setidaknya satu router (mungkin lebih) di setiap grup merangkum informasi sebelum meneruskannya ke grup lain.

Berapa besar kelompok? Protokol apa yang digunakan router dalam grup? Bagaimana informasi perutean direpresentasikan? Protokol apa yang digunakan router antar grup? Perancang sistem perutean Internet tidak menentukan ukuran yang tepat dan juga tidak menentukan representasi atau protokol data yang tepat. Sebaliknya, para desainer sengaja menjaga arsitektur cukup fleksibel untuk menangani berbagai macam organisasi. Misalnya, untuk mengakomodasi organisasi dengan berbagai ukuran, perancang menghindari menentukan ukuran minimum atau maksimum untuk sebuah grup. Untuk mengakomodasi protokol perutean yang berubah-ubah, perancang memutuskan untuk mengizinkan setiap organisasi memilih protokol perutean secara independen.

8.5 Konsep Sistem Otonom

Untuk menangkap konsep grup router, kami menggunakan istilah Autonomous System (AS). Secara intuitif, seseorang dapat memikirkan sistem otonom sebagai kumpulan jaringan dan router yang berdekatan, semuanya di bawah kendali satu otoritas administratif. Tidak ada arti pasti untuk otoritas administratif — istilah ini cukup fleksibel untuk mengakomodasi banyak kemungkinan. Misalnya, sistem otonom dapat sesuai dengan ISP, seluruh perusahaan, atau universitas. Sebagai alternatif, organisasi besar dengan banyak situs dapat memilih untuk menentukan satu sistem otonom untuk setiap situs. Secara khusus, setiap ISP biasanya merupakan sistem otonom tunggal, tetapi ada kemungkinan bagi ISP besar untuk membagi dirinya menjadi beberapa sistem otonom.

Pilihan ukuran sistem otonom dapat dibuat karena alasan ekonomi, teknis, atau administratif. Misalnya, pertimbangkan sebuah perusahaan multi-nasional. Mungkin lebih murah bagi perusahaan untuk membagi menjadi beberapa sistem otonom, yang masing-masing memiliki koneksi ke ISP di negara tertentu daripada bertindak sebagai sistem otonom tunggal dengan satu koneksi ke seluruh Internet. Alasan lain untuk ukuran tertentu muncul dari protokol perutean yang akan digunakan — sebuah

protokol dapat menghasilkan lalu lintas perutean yang berlebihan ketika digunakan pada banyak perute (yaitu, lalu lintas perutean dapat bertambah sebagai kuadrat dari jumlah perute).

Poin Penting

Internet dibagi menjadi satu set sistem otonom; router dalam sistem otonom bertukar informasi perutean, yang kemudian diringkas sebelum diteruskan ke grup lain.

8.6 Dua Jenis Protokol Perutean Internet

Sekarang setelah kita memahami konsep sistem otonom, perutean Internet dapat didefinisikan dengan lebih tepat. Semua protokol perutean Internet termasuk dalam salah satu dari dua kategori:

- Protokol Gateway Interior (IGP)
- Protokol Gateway Eksterior (EGP)

Setelah mendefinisikan dua kategori, kita akan memeriksa satu set contoh protokol routing yang menggambarkan setiap kategori.

8.6.1 Protokol Gateway Interior (IGP)

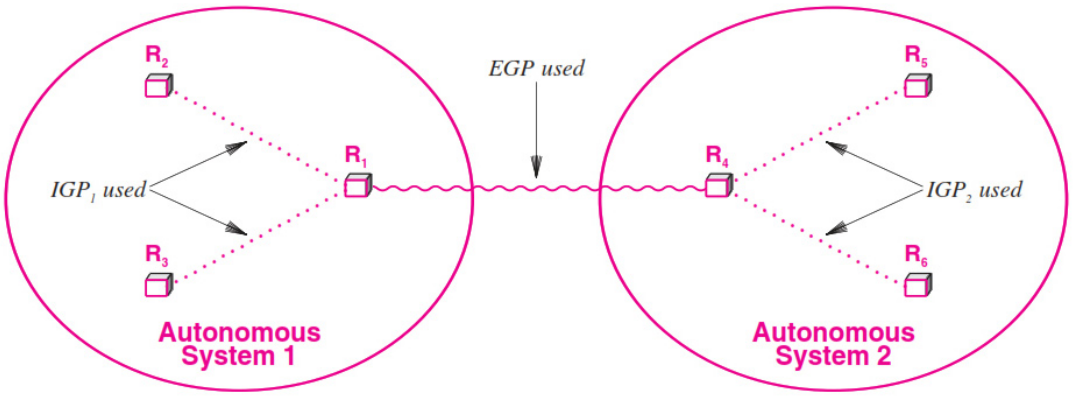
Router dalam sistem otonom menggunakan Interior Gateway Protocol (IGP) untuk bertukar informasi perutean. Beberapa IGP tersedia; setiap sistem otonom bebas memilih IGPnya sendiri. Biasanya, IGP mudah dipasang dan dioperasikan, tetapi IGP dapat membatasi ukuran atau kompleksitas perutean sistem otonom.

8.6.2 Protokol Gateway Eksterior (EGP)

Router dalam satu sistem otonom menggunakan Exterior Gateway Protocol (EGP) untuk bertukar informasi perutean dengan router di sistem otonom lain. EGP biasanya lebih kompleks untuk dipasang dan dioperasikan daripada IGP, tetapi EGP menawarkan lebih banyak fleksibilitas dan overhead yang lebih rendah (yaitu, lebih sedikit lalu lintas). Untuk menghemat lalu lintas, EGP merangkum informasi perutean dari sistem otonom sebelum meneruskannya ke sistem otonom lain. Lebih penting lagi, EGP mengimplementasikan batasan kebijakan yang memungkinkan manajer sistem untuk menentukan dengan tepat informasi apa yang dirilis di luar organisasi.

8.6.3 Ilustrasi Bagaimana IGP dan EGP Digunakan

Gambar 8.3 mengilustrasikan hierarki perutean dua tingkat yang digunakan di Internet dengan menunjukkan dua perute dalam dua sistem otonom.



Gambar 8.3 Ilustrasi perutean Internet dengan IGP yang digunakan di setiap sistem otonom dan EGP yang digunakan di antara sistem otonom.

Pada gambar, Autonomous System 1 (AS1) telah memilih IGP1 untuk digunakan secara internal, dan Autonomous System 2 (AS2) telah memilih IGP2. Semua router di AS1 berkomunikasi menggunakan IGP1, dan semua router di AS2 berkomunikasi menggunakan IGP2. Router R1 dan R4 menggunakan EGP untuk berkomunikasi antara dua sistem otonom. Artinya, R1 harus meringkas informasi dari sistem otonomnya dan mengirim ringkasan ke R4. Selain itu, R1 menerima ringkasan dari R4, dan menggunakan IGP1 untuk menyebarkan informasi ke router di AS1. R4 melakukan layanan yang sama untuk AS2.

8.6.4 Rute Optimal, Metrik Perutean, dan IGP

Tampaknya alih-alih hanya menemukan satu jalur ke setiap tujuan, perangkat lunak perutean harus menemukan semua jalur yang mungkin dan kemudian memilih satu yang optimal. Meskipun Internet biasanya memiliki banyak jalur antara sumber dan tujuan, tidak ada kesepakatan universal tentang jalur mana yang optimal. Untuk memahami alasannya, pertimbangkan persyaratan berbagai aplikasi. Untuk aplikasi desktop jarak jauh, jalur dengan penundaan paling sedikit adalah optimal. Untuk browser yang mengunduh file grafik besar, jalur dengan throughput maksimum adalah optimal. Untuk aplikasi webcast audio yang menerima audio real-time, jalur dengan jitter paling sedikit adalah optimal.

Kami menggunakan istilah metrik perutean untuk merujuk pada ukuran jalur yang digunakan perangkat lunak perutean saat memilih rute. Meskipun dimungkinkan untuk menggunakan throughput, delay, atau jitter sebagai metrik perutean, sebagian besar perangkat lunak perutean Internet tidak. Sebaliknya, perutean Internet biasa menggunakan kombinasi dua metrik: biaya administrasi dan jumlah hop. Dalam perutean Internet, hop sesuai dengan jaringan perantara (atau router). Jadi, jumlah hop untuk tujuan memberikan jumlah jaringan perantara di jalur ke tujuan. Biaya administrasi ditetapkan secara manual, seringkali untuk mengontrol jalur mana yang dapat digunakan lalu lintas. Misalnya, dalam sebuah perusahaan, dua jalur menghubungkan departemen akuntansi ke departemen penggajian: jalur 2-hop yang mencakup jaringan yang dirancang untuk digunakan untuk lalu lintas pelanggan dan jalur 3-hop yang mencakup jaringan untuk lalu lintas internal perusahaan. Artinya, jalur terpendek melanggar kebijakan perusahaan dengan melintasi jaringan yang ditunjuk untuk melayani pelanggan. Dalam kasus seperti itu, administrator jaringan dapat mengesampingkan biaya aktual dari jalur 2-hop dengan menetapkan jalur tersebut sebagai biaya administrasi empat hop (yaitu, manajer mengganti biaya aktual dengan nilai administratif untuk mencapai efek yang diinginkan). Perangkat lunak perutean akan

memilih jalur dengan biaya lebih rendah (yaitu jalur dengan metrik tiga lompatan). Dengan demikian, lalu lintas akan mengikuti kebijakan perusahaan.

Poin Penting

Meskipun sebagian besar protokol perutean Internet dirancang untuk menggunakan metrik hop-count, administrator jaringan dapat mengesampingkan metrik tersebut untuk menegakkan kebijakan.

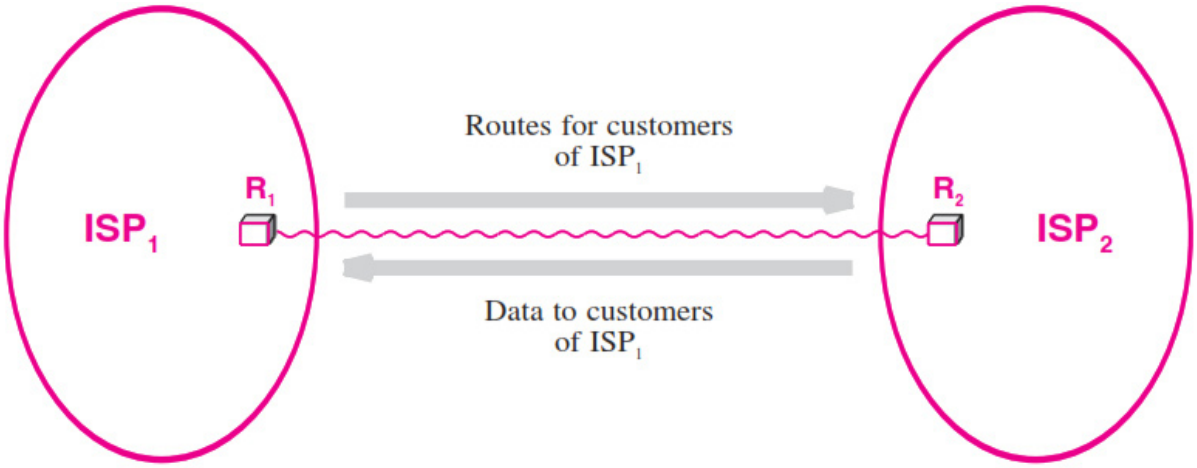
IGP dan EGP berbeda dalam hal penting sehubungan dengan metrik perutean: IGP menggunakan metrik perutean, tetapi EGP tidak. Artinya, setiap sistem otonom memilih metrik perutean dan mengatur perangkat lunak perutean internal untuk mengirim metrik dengan setiap rute sehingga perangkat lunak penerima dapat menggunakan metrik untuk memilih jalur yang optimal. Di luar sistem otonom, bagaimanapun, EGP tidak mencoba untuk memilih jalur yang optimal. Sebaliknya, EGP hanya menemukan jalan. Alasannya sederhana: karena setiap sistem otonom bebas memilih metrik perutean, EGP tidak dapat membuat perbandingan yang berarti. Misalnya, satu sistem otonom melaporkan jumlah hop di sepanjang jalur ke tujuan D dan sistem otonom lainnya melaporkan throughput di sepanjang jalur yang berbeda ke D. EGP yang menerima dua laporan tidak dapat memilih jalur mana yang memiliki biaya paling rendah karena tidak ada cara untuk mengkonversi dari hop ke throughput. Dengan demikian, EGP hanya dapat melaporkan keberadaan jalur dan bukan biayanya.

Poin Penting

Dalam sistem otonom, perangkat lunak IGP menggunakan metrik perutean untuk memilih jalur optimal ke setiap tujuan. Perangkat lunak EGP menemukan jalur ke setiap tujuan, tetapi tidak dapat menemukan jalur yang optimal karena tidak dapat membandingkan metrik perutean dari beberapa sistem otonom.

8.7 Rute dan Lalu Lintas Data

Sebuah pepatah dalam jaringan menunjukkan bahwa respons terhadap iklan perutean adalah data. Konsepnya sederhana: lalu lintas data untuk tujuan tertentu mengalir dalam arah yang berlawanan dengan lalu lintas perutean. Misalnya, sistem otonom yang dimiliki oleh ISP1 berisi jaringan N. Sebelum lalu lintas dapat tiba yang ditujukan untuk N, ISP1 harus mengiklankan rute ke N. Artinya, ketika iklan perutean mengalir keluar, data akan mulai mengalir masuk. Gambar 8.4 mengilustrasikan aliran data dalam menanggapi iklan perutean.



Gambar 8.4 Aliran data setelah router di ISP mengiklankan rute.

8.8 Border Gateway Protocol (BGP)

Satu protokol tertentu telah muncul sebagai Exterior Gateway Protocol yang paling banyak digunakan di Internet. Dikenal sebagai Border Gateway Protocol (BGP), protokol ini telah melewati tiga revisi besar. Versi 4 adalah standar saat ini, dan secara resmi disingkat BGP-4. Dalam praktiknya, nomor versi tetap tidak berubah begitu lama sehingga profesional jaringan menggunakan istilah BGP untuk merujuk ke versi 4.

BGP memiliki ciri-ciri sebagai berikut:

- Perutean Di Antara Sistem Otonom. Karena ditujukan untuk digunakan sebagai Exterior Gateway Protocol, BGP menyediakan informasi perutean pada tingkat sistem otonom. Artinya, semua rute diberikan sebagai jalur sistem otonom. Misalnya, jalur ke tujuan tertentu dapat terdiri dari sistem otonom 17, 2, 56, dan 12. Tidak ada penggunaan metrik perutean, dan tidak ada cara bagi BGP untuk memberikan detail tentang router dalam setiap sistem otonom di jalur tersebut.
- Ketentuan Kebijakan. BGP memungkinkan pengirim dan penerima untuk menegakkan kebijakan. Secara khusus, seorang manajer dapat mengonfigurasi BGP untuk membatasi rute mana yang diiklankan BGP kepada pihak luar.
- Fasilitas Untuk Transit Routing. BGP mengklasifikasikan setiap sistem otonom sebagai sistem transit jika setuju untuk melewatkan lalu lintas ke sistem otonom lain, atau sebagai sistem rintisan jika tidak. Demikian pula, lalu lintas yang melewati dalam perjalanannya ke AS lain diklasifikasikan sebagai lalu lintas transit. Klasifikasi memungkinkan BGP untuk membedakan antara ISP dan sistem otonom lainnya. Lebih penting lagi, BGP memungkinkan sebuah perusahaan untuk mengklasifikasikan dirinya sebagai sebuah rintisan bahkan jika multi-homed (yaitu, sebuah perusahaan dengan beberapa koneksi eksternal dapat menolak untuk menerima lalu lintas transit).
- Transportasi Terpercaya. BGP menggunakan TCP untuk semua komunikasi. Artinya, program BGP pada router dalam satu sistem otonom membentuk koneksi TCP ke program BGP pada

router di sistem otonom lain, dan kemudian mengirimkan data melalui koneksi. TCP memastikan bahwa data tiba dalam urutan yang benar dan tidak ada data yang hilang.

BGP menyediakan perekat yang menyatukan perutean Internet — di pusat Internet, ISP Tier-1 menggunakan BGP untuk bertukar informasi perutean dan belajar tentang pelanggan satu sama lain.

Poin Penting

Border Gateway Protocol (BGP) adalah Exterior Gateway Protocol yang digunakan ISP Tier-1 untuk bertukar informasi perutean di antara sistem otonom di pusat Internet; versi saat ini adalah BGP-4.

8.9 Routing Information Protocol (RIP)

Routing Information Protocol (RIP) adalah salah satu Protokol Gateway Interior pertama yang digunakan di Internet. RIP memiliki ciri-ciri sebagai berikut:

- Perutean Dalam Sistem Otonom. RIP dirancang sebagai Interior Gateway Protocol yang digunakan untuk melewatkan informasi antar router dalam sistem otonom.
- Metrik Hitungan Hop. RIP mengukur jarak dalam lompatan jaringan, di mana setiap jaringan antara sumber dan tujuan dihitung sebagai satu lompatan; RIP menghitung jaringan yang terhubung langsung sebagai satu hop.
- Transportasi yang Tidak Dapat Diandalkan. RIP menggunakan UDP untuk mentransfer pesan antar router.
- Pengiriman Siaran Atau Multicast. RIP dimaksudkan untuk digunakan melalui teknologi Jaringan Area Lokal yang mendukung siaran atau multicast (mis., Ethernet). Versi 1 dari RIP menyiarkan pesan; versi 2 memungkinkan pengiriman melalui multicast.
- Dukungan Untuk CIDR Dan Subnetting. RIP versi 2 menyertakan topeng alamat dengan setiap alamat tujuan.
- Dukungan Untuk Propagasi Rute Default. Selain menentukan tujuan eksplisit, RIP memungkinkan router untuk mengiklankan rute default.
- Algoritma Vektor Jarak. RIP menggunakan pendekatan vektor jarak untuk perutean yang didefinisikan dalam Algoritma 18.3†.
- Versi Pasif Untuk Host. Meskipun hanya router yang dapat menyebarkan informasi perutean, RIP memungkinkan host untuk mendengarkan secara pasif dan memperbarui tabel penerusannya. RIP pasif berguna pada jaringan di mana sebuah host memilih di antara beberapa router.

Untuk memahami bagaimana RIP menyebarkan rute, ingat bagaimana perutean vektor jarak bekerja. Setiap pesan keluar berisi iklan yang mencantumkan jaringan yang dapat dijangkau pengirim beserta jarak ke masing-masing. Ketika menerima iklan, perangkat lunak RIP menggunakan daftar tujuan untuk memperbarui tabel penerusan lokal. Setiap entri dalam iklan RIP terdiri dari sepasang:

(jaringan tujuan, jarak)

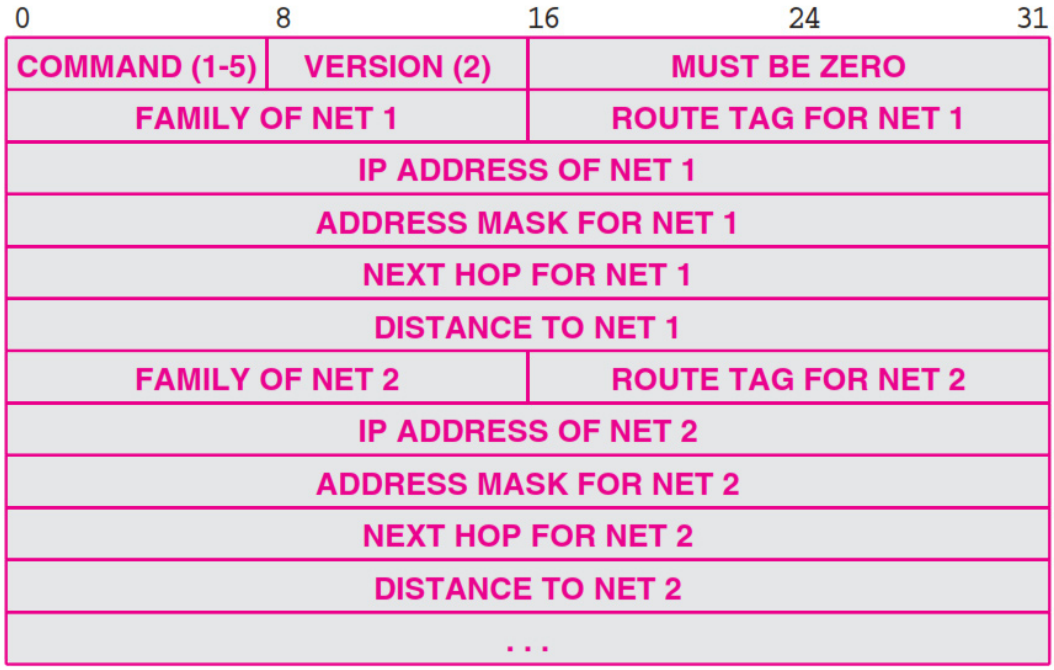
di mana jarak adalah jumlah hop ke tujuan. Ketika sebuah pesan tiba, jika penerima tidak memiliki rute ke tujuan yang diiklankan atau jika jarak yang diiklankan lebih pendek dari jarak rute saat ini, penerima mengganti rutenya dengan rute ke pengirim.

Keuntungan utama dari RIP adalah kesederhanaan. RIP memerlukan sedikit konfigurasi — seorang manajer hanya memulai RIP berjalan pada setiap router dalam organisasi dan memungkinkan router untuk menyiarkan pesan satu sama lain. Setelah waktu yang singkat, semua router dalam organisasi akan memiliki rute ke semua tujuan.

RIP juga menangani propagasi rute default. Organisasi hanya perlu mengonfigurasi salah satu routernya agar memiliki default (biasanya, organisasi memilih router yang terhubung ke ISP). RIP menyebarkan rute default ke semua router lain dalam organisasi, yang berarti bahwa setiap datagram yang dikirim ke tujuan di luar organisasi akan diteruskan ke ISP.

8.10 Format Paket RIP

Format pesan RIP membantu menjelaskan bagaimana protokol perutean vektor jarak beroperasi. Gambar 8.5 mengilustrasikan pesan pembaruan RIP.



Gambar 8.5 Format pesan pembaruan RIP versi 2.

Seperti yang ditunjukkan oleh gambar, setiap entri berisi alamat IP tujuan dan jarak ke tujuan itu. Selain itu, untuk mengizinkan RIP digunakan dengan CIDR atau pengalamatan subnet, sebuah entri berisi topeng alamat 32-bit. Setiap entri juga memiliki alamat hop berikutnya, dan dua bidang 16-bit yang mengidentifikasi entri sebagai alamat IP dan menyediakan tag yang digunakan untuk mengelompokkan entri bersama-sama. Secara keseluruhan, setiap entri berisi dua puluh oktet.

Poin Penting

RIP adalah Interior Gateway Protocol yang menggunakan algoritma distance vector untuk menyebarkan informasi routing.

8.11 Open Shortest Path First Protocol (OSPF)

Format pesan RIP menggambarkan kelemahan protokol vektor jarak: ukuran pesan sebanding dengan jumlah jaringan yang dapat dijangkau. Mengirim pesan RIP menyebabkan penundaan, dan memproses pesan RIP menghabiskan banyak siklus CPU. Penundaan berarti bahwa perubahan rute menyebar perlahan, satu router pada satu waktu. Jadi, meskipun RIP bekerja dengan baik di antara beberapa router, skalanya tidak baik.

Untuk memenuhi permintaan akan protokol perutean yang dapat berskala ke organisasi besar, IETF merancang IGP yang dikenal sebagai Open Shortest Path First Protocol (OSPF). Nama ini berasal dari penggunaan algoritma SPF Dijkstra yang menghitung jalur terpendek. OSPF memiliki karakteristik sebagai berikut:

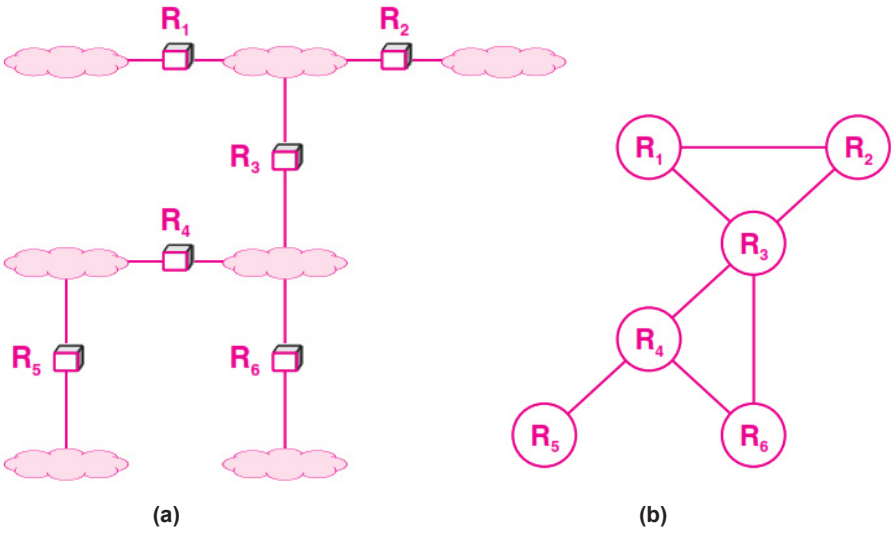
- Perutean Dalam Sistem Otonom. OSPF adalah Protokol Gerbang Interior yang digunakan dalam sistem otonom.
- Dukungan CIDR. Untuk mengakomodasi pengalamatan CIDR, OSPF menyertakan topeng alamat 32-bit dengan setiap alamat.
- Pertukaran Pesan yang Diautentikasi. Sepasang router menggunakan OSPF
- dapat mengotentikasi setiap pesan.
- Rute yang Diimpor. OSPF memungkinkan router untuk memperkenalkan rute yang dipelajari dari cara lain (misalnya, dari BGP).
- Algoritma Status Tautan. OSPF menggunakan perutean link-state seperti yang dijelaskan dalam Bab 18.
- Dukungan Untuk Metrik. OSPF memungkinkan administrator untuk menetapkan biaya untuk setiap rute.
- Dukungan Untuk Jaringan Multi-akses. Perutean status tautan tradisional tidak efisien di jaringan multi-akses, seperti Ethernet, karena semua router terhubung ke status tautan siaran jaringan. OSPF mengoptimalkan dengan menunjuk satu router untuk disiarkan di jaringan.

Poin Penting

OSPF adalah Interior Gateway Protocol yang menggunakan algoritma link-state untuk menyebarkan informasi routing. Router menggunakan algoritma SPF Dijkstra untuk menghitung jalur terpendek.

8.12 Contoh Grafik OSPF

Ingat dari Bab 18 bahwa perutean link-state menggunakan abstraksi teori-grafik. Meskipun OSPF memungkinkan hubungan yang kompleks antara jaringan dan grafik, contoh sederhana akan membantu menjelaskan konsep dasar†. Pertimbangkan jaringan dan grafik terkait yang diilustrasikan pada Gambar 8.6.



Gambar 8.6 (a) Contoh topologi, dan (b) grafik OSPF yang sesuai.

Gambar tersebut menunjukkan grafik OSPF khas di mana setiap node sesuai dengan router. Tepi dalam grafik sesuai dengan koneksi antara sepasang router (yaitu, jaringan). Untuk mengikuti algoritma link-state, setiap pasangan router yang terhubung oleh jaringan secara berkala menyelidiki satu sama lain dan kemudian menyiarkan pesan link-state ke router lain. Semua router menerima pesan broadcast; masing-masing menggunakan pesan untuk memperbarui salinan grafik lokalnya, dan menghitung ulang jalur terpendek saat status berubah.

8.13 Area OSPF

Salah satu fitur khusus yang membuat OSPF lebih kompleks daripada protokol perutean lainnya juga membuatnya lebih kuat: perutean hierarkis. Untuk mencapai hierarki, OSPF memungkinkan sistem otonom dipartisi untuk tujuan perutean. Artinya, seorang manajer dapat membagi router dan jaringan dalam sistem otonom menjadi subset yang disebut oleh OSPF area. Setiap router dikonfigurasi untuk mengetahui batas area (yaitu, router lain mana yang berada di areanya). Ketika OSPF berjalan, router dalam area tertentu bertukar pesan link-state secara berkala.

Selain bertukar informasi dalam suatu area, OSPF memungkinkan komunikasi antar area. Satu router di setiap area dikonfigurasi untuk berkomunikasi dengan router di satu atau lebih area lainnya. Kedua router meringkas informasi routing yang telah mereka pelajari dari router lain dalam area masing-masing, dan kemudian bertukar ringkasan. Jadi, alih-alih menyiarkan ke semua router dalam sistem otonom, OSPF membatasi siaran status tautan ke router dalam suatu area. Sebagai hasil dari hierarki, OSPF dapat menskala untuk menangani sistem otonom yang jauh lebih besar daripada protokol perutean lainnya.

Poin Penting

Karena memungkinkan manajer untuk mempartisi router dan jaringan dalam sistem otonom ke beberapa area, OSPF dapat menskala untuk menangani jumlah router yang lebih besar daripada IGP lainnya.

8.14 Intermediate System - Intermediate System (IS-IS)

Awalnya dirancang oleh Digital Equipment Corporation untuk menjadi bagian dari DECNET V, IS-IS (Sistem Menengah ke Sistem Menengah) adalah IGP. IS-IS dibuat sekitar waktu yang sama dengan OSPF, dan kedua protokol serupa dalam banyak hal. Keduanya menggunakan pendekatan link-state dan menggunakan algoritma Dijkstra untuk menghitung jalur terpendek. Selain itu, kedua protokol memerlukan dua router yang berdekatan untuk secara berkala menguji tautan di antara mereka dan menyiarkan pesan status.

Perbedaan utama antara OSPF dan IS-IS asli dapat diringkas sebagai:

- IS-IS adalah milik (dimiliki oleh Digital) dan OSPF dibuat sebagai standar terbuka, tersedia untuk semua vendor.
- OSPF dirancang untuk dijalankan melalui IP; IS-IS dirancang untuk dilindas
- CLNS (bagian dari tumpukan protokol OSI yang bernasib buruk).
- OSPF dirancang untuk menyebarkan rute IPv4 (alamat IPv4 dan masker alamat); IS-IS dirancang untuk menyebarkan rute untuk protokol OSI.
- Seiring waktu, OSPF memperoleh banyak fitur. Akibatnya, IS-IS sekarang memiliki lebih sedikit overhead.

Ketika protokol awalnya ditemukan, keterbukaan dan dedikasi OSPF terhadap IP membuatnya jauh lebih populer daripada IS-IS. Faktanya, IS-IS hampir sepenuhnya dilupakan. Seiring berjalannya waktu, popularitas OSPF mendorong IETF untuk menambahkan fitur tambahan. Ironisnya, di awal tahun 2000-an, sepuluh tahun setelah protokol dirancang, beberapa hal berubah untuk memberi IS-IS kesempatan kedua. Digital Equipment Corporation telah bubar, dan IS-IS tidak lagi dianggap sebagai properti kepemilikan yang berharga. Versi IS-IS yang lebih baru didefinisikan untuk mengintegrasikannya dengan IP dan Internet. Karena OSPF dibangun untuk IPv4, versi yang benar-benar baru harus dikembangkan untuk menangani alamat IPv6 yang lebih besar. ISP terbesar telah berkembang ke ukuran di mana overhead ekstra di OSPF membuat IS-IS lebih menarik. Akibatnya, IS-IS mulai bangkit kembali.

8.15 Perutean Multicast

8.15.1 Semantik Multicast IP

Sejauh ini, kita telah membahas unicast routing. Artinya, kami telah mempertimbangkan protokol perutean yang menyebarkan informasi tentang tujuan yang masing-masing memiliki alamat statis dan lokasi yang tidak berubah. Salah satu tujuan desain untuk propagasi rute unicast adalah stabilitas — perubahan rute yang terus-menerus tidak diinginkan karena menyebabkan jitter yang lebih tinggi dan datagram yang tiba-tiba rusak. Jadi, setelah protokol perutean unicast menemukan jalur terpendek, biasanya ia akan mempertahankan rute tersebut hingga kegagalan membuat jalur tersebut tidak dapat digunakan.

Menyebarkan informasi routing multicast berbeda secara dramatis dari propagasi rute unicast. Perbedaan muncul karena multicast Internet memungkinkan keanggotaan grup dinamis dan pengirim anonim. Keanggotaan grup dinamis berarti bahwa aplikasi dapat memilih untuk berpartisipasi dalam

grup kapan saja dan tetap menjadi peserta untuk durasi yang berubah-ubah. Artinya, abstraksi multicast IP memungkinkan aplikasi yang berjalan di komputer arbitrer untuk:

- Bergabunglah dengan grup multicast kapan saja dan mulai menerima salinan semua paket yang dikirim ke grup. Untuk bergabung dengan grup, host menginformasikan router terdekat. Jika beberapa aplikasi pada host yang sama memutuskan untuk bergabung dengan grup, host menerima satu salinan dari setiap datagram yang dikirim ke grup dan membuat salinan lokal untuk setiap aplikasi.
- Keluar dari grup multicast kapan saja. Sebuah host secara berkala mengirimkan pesan keanggotaan grup ke router lokal. Setelah aplikasi terakhir pada host meninggalkan grup, host menginformasikan router lokal bahwa ia tidak lagi berpartisipasi dalam grup.

Grup multicast IP bersifat anonim dalam dua cara. Pertama, baik pengirim maupun penerima tidak mengetahui (juga tidak dapat mengetahui) identitas atau jumlah anggota kelompok. Kedua, router dan host tidak mengetahui aplikasi mana yang akan mengirim datagram ke grup karena aplikasi arbitrer dapat mengirim datagram ke grup multicast kapan saja. Artinya, keanggotaan dalam grup multicast hanya menentukan satu set penerima — pengirim tidak perlu bergabung dengan grup multicast sebelum mengirim pesan ke grup.

Poin Penting

Keanggotaan dalam grup multicast IP bersifat dinamis: komputer dapat bergabung atau keluar dari grup kapan saja. Keanggotaan kelompok mendefinisikan satu set penerima; aplikasi sewenang-wenang dapat mengirim datagram ke grup, bahkan jika aplikasi tersebut bukan anggota grup.

8.15.2 IGMP

Bagaimana cara tuan rumah bergabung atau keluar dari grup multicast? Ada protokol standar yang memungkinkan host untuk menginformasikan router terdekat setiap kali host perlu bergabung atau meninggalkan grup multicast tertentu. Dikenal sebagai Internet Group Multicast Protocol (IGMP), protokol ini hanya digunakan pada jaringan antara host dan router. Selanjutnya, protokol mendefinisikan host, bukan aplikasi, untuk menjadi anggota grup, dan tidak menentukan apa pun tentang aplikasi. Jika beberapa aplikasi pada host tertentu bergabung dengan grup multicast, host harus membuat salinan dari setiap datagram yang diterimanya untuk aplikasi lokal. Saat aplikasi terakhir pada host keluar dari grup, host menggunakan IGMP untuk menginformasikan router lokal bahwa ia tidak lagi menjadi anggota grup.

8.15.3 Teknik Penerusan dan Penemuan

Ketika sebuah router mengetahui bahwa sebuah host di salah satu jaringannya telah bergabung dengan grup multicast, router harus membuat jalur ke grup tersebut dan menyebarkan datagram yang diterimanya untuk grup tersebut ke host. Jadi, router, bukan host, memiliki tanggung jawab untuk menyebarkan informasi routing multicast.

Keanggotaan grup yang dinamis dan dukungan untuk pengirim anonim membuat perutean multicast tujuan umum menjadi sangat sulit. Selain itu, ukuran dan topologi grup sangat bervariasi di antara aplikasi. Misalnya, telekonferensi sering menciptakan kelompok-kelompok kecil (misalnya, antara

dua dan lima anggota) yang mungkin secara geografis tersebar atau dalam organisasi yang sama. Aplikasi webcast berpotensi membuat grup dengan jutaan anggota yang tersebar di seluruh dunia.

Untuk mengakomodasi keanggotaan dinamis, protokol routing multicast harus dapat mengubah rute dengan cepat dan terus menerus. Misalnya, jika pengguna di Prancis bergabung dengan grup multicast yang memiliki anggota di AS dan Jepang, perangkat lunak perutean multicast harus terlebih dahulu menemukan anggota grup lainnya, lalu membuat struktur penerusan yang optimal. Lebih penting lagi, karena pengguna yang sewenang-wenang dapat mengirim datagram ke grup, informasi tentang rute harus melampaui anggota grup. Dalam praktiknya, protokol multicast telah mengikuti tiga pendekatan berbeda untuk penerusan datagram:

- Flood-And-Prune
- Configuration-And-Tunneling
- Core-Based Discovery

Flood-And-Prune

Flood-and-prune sangat ideal dalam situasi di mana grup kecil dan semua anggota terhubung ke Jaringan Area Lokal yang berdekatan (mis., Grup dalam perusahaan). Awalnya, router meneruskan setiap datagram ke semua jaringan. Artinya, ketika datagram multicast tiba, router mentransmisikan datagram pada semua LAN yang terhubung langsung melalui multicast perangkat keras. Untuk menghindari loop perutean, protokol flood-and-prune menggunakan teknik yang dikenal sebagai Reverse Path Broadcasting (RPB) yang memutus siklus. Sementara tahap flooding berlangsung, router bertukar informasi tentang keanggotaan grup. Jika router mengetahui bahwa tidak ada host di jaringan tertentu yang menjadi anggota grup, router berhenti meneruskan multicast ke jaringan (yaitu, "memangkas" jaringan dari set).

Configuration-And-Tunneling

Configuration-And-Tunneling sangat ideal dalam situasi di mana kelompok secara geografis tersebar (yaitu, memiliki beberapa anggota di setiap situs, dengan situs dipisahkan oleh jarak yang jauh). Sebuah router di setiap situs dikonfigurasi untuk mengetahui tentang situs lain. Ketika datagram multicast tiba, router di situs mentransmisikan datagram pada semua LAN yang terhubung langsung melalui multicast perangkat keras. Router kemudian berkonsultasi dengan tabel konfigurasinya untuk menentukan situs jarak jauh mana yang harus menerima salinan, dan menggunakan tunneling IP-in-IP untuk mentransfer salinan datagram multicast ke masing-masing situs jarak jauh.

Core-Based Discovery

Meskipun flood-and-prune dan configuration-and-tunneling masing-masing menangani kasus ekstrim dengan baik, diperlukan teknik yang memungkinkan multicast untuk menskalakan dengan anggun dari grup kecil di satu area ke grup besar dengan anggota di lokasi yang berubah-ubah. Untuk memberikan pertumbuhan yang lancar, beberapa protokol perutean multicast menetapkan alamat unicast inti untuk setiap grup multicast. Setiap kali router R1 menerima datagram multicast yang harus ditransmisikan ke grup, R1 merangkum datagram multicast dalam datagram unicast dan meneruskan datagram unicast ke alamat unicast inti grup. Saat datagram unicast berjalan melalui Internet, setiap router memeriksa isinya. Ketika datagram mencapai router R2 yang berpartisipasi dalam grup, R2 menghapus dan memproses pesan multicast. R2 menggunakan perutean multicast untuk meneruskan datagram ke anggota grup. Permintaan untuk bergabung dengan grup mengikuti pola yang sama — jika menerima permintaan untuk bergabung dengan grup, R2 menambahkan

rute baru ke tabel penerusan multicast dan mulai meneruskan salinan setiap datagram multicast ke R1. Dengan demikian, set router yang menerima grup multicast tertentu tumbuh dari inti ke luar. Dalam istilah teori graf, router membentuk pohon.

8.15.4 Protokol Multicast

Meskipun banyak protokol routing multicast telah diusulkan; tidak ada perutean multicast seluruh Internet saat ini. Beberapa protokol yang diusulkan adalah:

Protokol Perutean Multicast Vektor Jarak (DVMRP). Sebuah protokol yang digunakan oleh program UNIX mrouted dan Internet Multicast backBONE (MBONE), DVMRP melakukan multicast lokal, dan menggunakan enkapsulasi IP-in-IP untuk mengirim datagram multicast dari satu situs di Internet ke situs lainnya. Informasi lebih lanjut tentang MBONE dapat ditemukan di:

http://www.lbl.gov/web/Computers-and-Networks.html#MBONE

- Pohon Berbasis Inti (CBT). Protokol tertentu di mana router membangun pohon pengiriman dari titik pusat untuk setiap grup. CBT bergantung pada perutean unicast untuk mencapai titik pusat.
- Protokol Independen Multicast – Mode Jarang (PIM-SM). Sebuah protokol yang menggunakan pendekatan yang sama seperti CBT untuk membentuk pohon routing multicast. Perancang memilih istilah protokol independen untuk menekankan bahwa meskipun datagram unicast digunakan untuk menghubungi tujuan jarak jauh saat membuat penerusan multicast, PIM-SM tidak bergantung pada protokol perutean unicast tertentu.
- Protokol Independen Multicast – Mode Padat (PIM-DM). Sebuah protokol yang dirancang untuk digunakan dalam suatu organisasi. Router yang menggunakan paket multicast siaran PIM-DM (yaitu banjir) ke semua lokasi dalam organisasi. Setiap router yang tidak memiliki anggota grup tertentu mengirimkan kembali pesan untuk memangkas pohon perutean multicast (yaitu, permintaan untuk menghentikan aliran paket). Skema ini bekerja dengan baik untuk sesi multicast berumur pendek (misalnya, beberapa menit) karena tidak memerlukan pengaturan sebelum transmisi dimulai.
- Ekstensi Multicast Ke Open Shortest Path First Protocol (MOSPF). Daripada protokol routing multicast tujuan umum, MOSPF dirancang untuk melewati rute multicast antara router dalam suatu organisasi. Jadi, alih-alih pendekatan multicast untuk tujuan umum, MOSPF dibangun di atas OSPF dan menggunakan fasilitas LSR.

Gambar 8.7 merangkum protokol routing multicast yang dijelaskan di atas.

Protokol	Jenis
DVMRP	Configuration-and-Tunneling
CBT	Core-Based-Discovery
PIM-SM	Core-Based-Discovery
PIM-DM	Flood-And-Prune
MOSPF	Link-State (within an organization)

Gambar 8.7 Protokol perutean multicast dan pendekatan yang digunakan masing-masing.

Terlepas dari dua puluh tahun penelitian dan banyak percobaan, multicast Internet tujuan umum belum berhasil. Bahkan aplikasi kolaboratif belum memberikan insentif yang memadai. Hasilnya dapat kita rangkum sebagai berikut:

> *Karakteristik dinamis dari multicast Internet membuat masalah propagasi rute multicast menjadi sulit. Meskipun banyak protokol telah diusulkan, Internet saat ini tidak memiliki fasilitas perutean multicast di seluruh Internet.*

8.16 Ringkasan

Sebagian besar host menggunakan perutean statis di mana tabel penerusan diinisialisasi saat startup sistem; router menggunakan perutean dinamis di mana perangkat lunak propagasi rute memperbarui tabel penerusan secara terus menerus. Dalam hal perutean, Internet dibagi menjadi satu set sistem otonom. Protokol yang digunakan untuk melewati rute antara sistem otonom dikenal sebagai Exterior Gateway Protocols (EGPs); protokol yang digunakan untuk melewatkan informasi perutean di dalam sistem otonom dikenal sebagai Interior Gateway Protocols (IGPs).

Border Gateway Protocol (BGP) adalah EGP utama di Internet; ISP Tier-1 menggunakan BGP untuk saling menginformasikan tentang pelanggan mereka. IGP termasuk RIP, OSPF, dan IS-IS.

Karena multicast Internet memungkinkan keanggotaan grup dinamis dan sumber arbitrer dapat mengirim ke grup multicast tanpa menjadi anggota, masalah propagasi rute multicast menjadi sulit. Meskipun beberapa protokol perutean multicast telah diusulkan, tidak ada teknologi multicast di seluruh Internet.

Latihan

1. Sebutkan dua kategori besar perutean Internet, dan jelaskan masing-masing.
2. Apa dua entri yang diperlukan dalam tabel penerusan dari host biasa?
3. Misalkan semua router di Internet berisi rute default; menunjukkan bahwa loop perutean harus ada.
4. Apa yang dimaksud dengan sistem otonom?
5. Sebutkan dan jelaskan dua jenis protokol perutean Internet.
6. Misalkan sebuah router dalam suatu organisasi menggunakan protokol routing untuk menyatakan bahwa tujuan yang diberikan berjarak sepuluh hop ketika tujuan hanya berjarak tiga hop. Apakah deklarasi tersebut selalu merupakan kesalahan? Menjelaskan.
7. Apa konsekuensi yang diharapkan ketika router mengiklankan rute ke tujuan tertentu?
8. Sebutkan dan jelaskan ciri-ciri BGP.
9. Di mana BGP digunakan?
10. Jenis algoritma perutean apa yang digunakan RIP, dan di mana RIP digunakan?
11. Sebutkan ciri-ciri RIP.
12. Ketika router menerima pesan RIP, bagaimana router membagi setiap alamat IP menjadi awalan dan akhiran?
13. Tulis program komputer yang membaca pesan pembaruan RIP dan mencetak konten setiap kolom.

14. RIP membatasi nilai jarak hingga maksimum 16 hop. Rancang contoh intranet perusahaan yang memiliki lebih dari 16 router dan lebih dari 16 jaringan tetapi masih dapat menggunakan RIP.
15. Sebutkan ciri-ciri OSPF.
16. Apa yang dimaksud dengan “Buka” di OSPF?
17. Mengapa OSPF memiliki banyak area?
18. Protokol mana yang memiliki overhead lebih rendah, OSPF atau IS-IS? Yang memiliki lebih banyak fitur?
19. Apa tujuan utama IGMP, dan di mana digunakan?
20. Apa tiga pendekatan utama yang digunakan untuk meneruskan datagram multicast?
21. Misalkan Anda dan dua teman di perguruan tinggi yang jauh ingin berpartisipasi dalam telekonferensi 3 arah menggunakan IP multicast. Protokol perutean multicast mana yang bekerja paling baik? Mengapa?
22. Meskipun setiap grup multicast IP membutuhkan alamat IP multicast yang unik, menggunakan server pusat untuk mengalokasikan alamat unik menciptakan hambatan pusat. Rancang skema yang memungkinkan satu set komputer untuk memilih alamat multicast secara acak dan menyelesaikan konflik, jika terjadi.
23. Lalu lintas yang dihasilkan oleh flood-and-prune membatasi ukuran wilayah jaringan yang dapat digunakan. Perkirakan total lalu lintas pada satu jaringan jika G grup multicast masing-masing menghasilkan lalu lintas dengan kecepatan P paket per detik, setiap paket berisi B bit, N jaringan merupakan intranet, dan setiap jaringan berisi setidaknya satu pendengar untuk setiap grup.
24. Apakah multicast digunakan secara luas di Internet? Menjelaskan.
25. Protokol multicast mana yang memungkinkan pesan multicast dikirim sebelum protokol menetapkan rute?

BAGIAN V
Aspek Lain Jaringan Komputer Kinerja Jaringan, QoS, Keamanan, Manajemen, dan Teknologi Baru

Bab 9 Kinerja Jaringan (QoS dan DiffServ)

Bab ini akan membahas tentang:

- Ukuran kuantitatif jaringan
- Bagaimana protokol dan teknologi penerusan paket dapat menerapkan mekanisme yang memberikan prioritas untuk beberapa lalu lintas.

9.1 Ukuran Kinerja

Secara informal, kami menggunakan istilah kecepatan untuk menggambarkan kinerja jaringan, dan mengacu pada jaringan berkecepatan rendah atau berkecepatan tinggi. Namun, definisi tersebut tidak memadai karena teknologi jaringan berubah begitu cepat sehingga jaringan yang diklasifikasikan sebagai "kecepatan tinggi" dapat menjadi kecepatan sedang atau rendah dalam waktu tiga atau empat tahun. Jadi, sebagai pengganti deskripsi kualitatif, ilmuwan dan insinyur menggunakan ukuran kuantitatif formal untuk menentukan kinerja jaringan secara tepat. Setelah meninjau langkah-langkah dasar, kami akan menjelaskan bagaimana mereka digunakan untuk menerapkan layanan berjenjang. Meskipun pemula sering lebih menyukai deskripsi informal, pengukuran kuantitatif penting karena memungkinkan untuk membandingkan fitur yang tepat dari dua jaringan dan untuk membangun mekanisme yang memberikan prioritas lebih tinggi untuk beberapa lalu lintas. Gambar 9.1 berisi daftar ukuran utama kinerja jaringan, dan bagian berturut-turut menjelaskan masing-masing.

Ukuran	Deskripsi
Latensi (penundaan)	Waktu yang diperlukan untuk mentransfer data melalui jaringan
Throughput (kapasitas)	Jumlah data yang dapat ditransfer per satuan waktu
Jitter (variabilitas)	Perubahan delay yang terjadi dan durasi perubahan

Gambar 9.1 Ukuran utama kinerja jaringan data.

9.2 Latensi atau Penundaan

Properti pertama jaringan yang dapat diukur secara kuantitatif adalah latensi atau penundaan. Latensi menentukan berapa lama waktu yang dibutuhkan data untuk melakukan perjalanan melintasi jaringan dari satu komputer ke komputer lain; itu diukur dalam sepersekian detik. Penundaan di Internet bergantung pada infrastruktur yang mendasarinya serta lokasi pasangan komputer tertentu yang berkomunikasi. Meskipun pengguna peduli dengan penundaan total jaringan, para insinyur membutuhkan pengukuran yang lebih tepat. Dengan demikian, para insinyur biasanya melaporkan penundaan maksimum dan rata-rata, dan membagi penundaan menjadi beberapa bagian konstituen. Gambar 9.2 mencantumkan berbagai jenis penundaan.

Jenis	Penjelasan
Propagation Delay	Waktu yang diperlukan sinyal untuk melakukan perjalanan melintasi media transmisi
Access Delay	Waktu yang dibutuhkan untuk mendapatkan akses ke media transmisi (misalnya, kabel)
Switching Delay	Waktu yang dibutuhkan untuk meneruskan sebuah paket
Queuing Delay	Waktu yang dihabiskan sebuah paket dalam memori switch atau router menunggu untuk dipilih untuk transmisi
Server Delay	Waktu yang dibutuhkan server untuk menanggapi permintaan dan mengirim tanggapan

Gambar 9.2 Macam-Macam Jenis Delay dan Penjelasannya Masing-masing.

Propagation Delay / Penundaan Perambatan

Beberapa penundaan dalam jaringan muncul karena sinyal membutuhkan sedikit waktu untuk melakukan perjalanan melintasi media transmisi. Secara umum, tundaan propagasi sebanding dengan jarak yang terbentang. Bahkan dengan kabel yang panjang, LAN tipikal yang digunakan dalam satu gedung memiliki penundaan propagasi di bawah satu milidetik. Meskipun penundaan seperti itu tampaknya tidak relevan bagi manusia, komputer modern dapat mengeksekusi lebih dari seratus ribu instruksi dalam satu milidetik. Dengan demikian, penundaan milidetik adalah signifikan ketika satu set komputer perlu berkoordinasi (misalnya, dalam industri keuangan, di mana waktu yang tepat dari pesanan stok tiba menentukan apakah pesanan diterima). Jaringan yang menggunakan satelit GEO memiliki penundaan yang jauh lebih tinggi — bahkan pada kecepatan cahaya, diperlukan waktu ratusan milidetik untuk melakukan perjalanan ke satelit dan kembali ke bumi.

Access Delay / Penundaan Akses

Banyak jaringan menggunakan media bersama. Himpunan komputer yang berbagi media harus bersaing untuk akses. Misalnya, jaringan nirkabel Wi-Fi menggunakan pendekatan CSMA/CA untuk akses menengah. Penundaan tersebut dikenal sebagai penundaan akses. Penundaan akses tergantung pada jumlah stasiun yang bersaing untuk akses dan jumlah lalu lintas yang dikirim setiap stasiun. Penundaan akses tetap kecil dan tetap kecuali media kelebihan beban.

Switching Delay

Perangkat elektronik dalam jaringan (misalnya, sakelar atau router Layer 2) harus menghitung hop berikutnya untuk setiap paket sebelum mentransmisikan paket melalui antarmuka keluaran. Perhitungan sering melibatkan pencarian tabel, yang berarti akses memori. Di beberapa perangkat, waktu tambahan diperlukan untuk mengirim paket melalui mekanisme komunikasi internal seperti bus atau fabric. Waktu yang diperlukan untuk menghitung hop berikutnya dan memulai transmisi dikenal sebagai penundaan switching. CPU cepat dan perangkat keras tujuan khusus telah membuat penundaan peralihan di antara penundaan yang paling tidak signifikan dalam jaringan komputer.

Queuing Delay / Penundaan Antrian

Paradigma store-and-forward yang digunakan dalam packet switching berarti bahwa perangkat seperti router mengumpulkan bit dari sebuah paket, menempatkannya dalam memori, memilih next-hop, dan kemudian menunggu sampai paket dapat dikirim sebelum memulai transmisi. Penundaan semacam itu dikenal sebagai penundaan antrian. Dalam kasus yang paling sederhana, sebuah paket ditempatkan dalam antrian keluaran FIFO, dan paket tersebut hanya perlu menunggu sampai paket yang datang lebih awal dikirim; sistem yang lebih kompleks menerapkan algoritma pemilihan yang memberikan prioritas pada beberapa paket. Penundaan antrian bervariasi — ukuran antrian sepenuhnya bergantung pada jumlah lalu lintas yang baru saja tiba. Penundaan antrian merupakan penyebab sebagian besar penundaan di Internet. Ketika penundaan antrian menjadi besar, kami mengatakan bahwa jaringan macet.

Server Delay / Penundaan Server

Meskipun bukan bagian dari jaringan itu sendiri, server sangat penting untuk sebagian besar komunikasi. Waktu yang dibutuhkan server untuk memeriksa permintaan dan menghitung serta mengirim respons merupakan bagian penting dari keseluruhan penundaan. Server mengantri permintaan masuk, yang berarti penundaan server bervariasi dan bergantung pada beban saat ini. Dalam banyak kasus, persepsi pengguna tentang penundaan Internet muncul dari penundaan server daripada penundaan jaringan.

9.3 Throughput, Kapasitas, dan Goodput

Properti fundamental kedua dari jaringan yang dapat diukur secara kuantitatif adalah kapasitas jaringan, yang sering dinyatakan sebagai throughput maksimum yang dapat dipertahankan jaringan. Throughput adalah ukuran kecepatan di mana data dapat dikirim melalui jaringan, ditentukan dalam bit per detik (bps). Sebagian besar jaringan komunikasi data menawarkan tingkat throughput lebih dari 1 Mbps, dan jaringan berkecepatan tertinggi beroperasi lebih cepat dari 1 Gbps. Seperti yang telah kita lihat, bagaimanapun, kasus khusus muncul di mana jaringan memiliki throughput kurang dari 1 Kbps.

Karena throughput dapat diukur dengan beberapa cara, seseorang harus berhati-hati untuk menentukan dengan tepat apa yang telah diukur. Ada beberapa kemungkinan:

- Kapasitas saluran tunggal
- Kapasitas agregat semua saluran
- Kapasitas teoritis dari perangkat keras yang mendasarinya
- Kecepatan data efektif yang dicapai oleh aplikasi (goodput)

Vendor sering mengiklankan kapasitas teoritis peralatan mereka dan throughput yang dicapai dalam kondisi optimal. Kapasitas perangkat keras sering disebut sebagai perkiraan throughput potensial karena kapasitas memberikan batas atas kinerja — tidak mungkin bagi pengguna untuk mengirim data lebih cepat daripada kecepatan di mana perangkat keras dapat mentransfer bit.

Pengguna tidak peduli dengan kapasitas perangkat keras yang mendasarinya — mereka hanya tertarik pada kecepatan transfer data. Pengguna biasanya menilai kecepatan data efektif yang dicapai aplikasi dengan mengukur jumlah data yang ditransfer per satuan waktu; istilah goodput kadang-kadang digunakan untuk menggambarkan ukuran. Tingkat goodput kurang dari kapasitas perangkat keras karena protokol memaksakan overhead — beberapa kapasitas jaringan tidak tersedia untuk data pengguna karena protokol:

- Kirim header paket, trailer, dan informasi kontrol
- Memaksakan batas pada ukuran jendela (menerima buffer)
- Gunakan protokol untuk menyelesaikan nama dan alamat
- Gunakan jabat tangan untuk memulai dan mengakhiri komunikasi
- Kurangi tingkat transmisi ketika kemacetan terdeteksi
- Mengirim ulang paket yang hilang

Kerugian menggunakan goodput sebagai ukuran muncul karena jumlah overhead tergantung pada tumpukan protokol yang digunakan. Selain protokol Transport, Internet, dan Layer 2, goodput bergantung pada protokol aplikasi. Misalnya, pertimbangkan untuk menggunakan File Transfer Protocol (FTP) untuk mengukur goodput di seluruh Ethernet. FTP menggunakan TCP, yang menggunakan IP. Selanjutnya, FTP tidak memampatkan data sebelum transmisi. Sebaliknya, FTP menempatkan data pengguna di segmen TCP, TCP merangkum setiap segmen dalam datagram IP, dan IP merangkum setiap datagram dalam bingkai Ethernet.

Jadi, setiap frame memiliki header Ethernet dan bidang CRC, header datagram IP, dan header TCP. Jika pengguna memilih aplikasi transfer file alternatif atau tumpukan protokol alternatif digunakan, goodput dapat berubah.

Poin Penting

Meskipun memberikan ukuran tingkat efektif di mana data dapat ditransfer melalui jaringan, goodput tergantung pada aplikasi.

9.4 Memahami Throughput dan Delay

Dalam praktiknya, terminologi yang digunakan oleh para profesional jaringan untuk menggambarkan throughput jaringan atau kapasitas jaringan dapat membingungkan. Misalnya, bab tentang komunikasi data mendefinisikan bandwidth saluran, dan menjelaskan hubungan antara bandwidth perangkat keras dan kecepatan data maksimum. Sayangnya, profesional jaringan sering menggunakan istilah bandwidth dan kecepatan sebagai sinonim untuk throughput. Jadi, orang mungkin mendengar seseorang mengatakan bahwa jaringan tertentu memiliki "kecepatan 1 Gbps." Atau, beberapa iklan menggunakan frasa “bandwidth 1 Gbps.” Dalam upaya untuk membedakan antara dua penggunaan bandwidth, insinyur cadangan bandwidth berarti bandwidth analog, dan menggunakan istilah bandwidth digital sebagai sinonim untuk throughput. Meskipun pernyataan seperti itu umum, mereka dapat membingungkan karena throughput, delay, dan bandwidth adalah properti yang terpisah.

Faktanya, throughput adalah ukuran kapasitas, bukan kecepatan. Untuk memahami hubungan tersebut, bayangkan sebuah jaringan menjadi jalan antara dua lokasi dan paket-paket yang melintasi jaringan menjadi mobil yang berjalan di jalan tersebut. Throughput menentukan berapa banyak mobil yang dapat memasuki jalan setiap detik, dan penundaan propagasi menentukan berapa lama waktu yang dibutuhkan satu mobil untuk menempuh jalan dari satu kota ke kota lain. Misalnya, sebuah jalan yang dapat menerima satu mobil setiap lima detik memiliki throughput 0,2 mobil per detik. Jika sebuah mobil membutuhkan 30 detik untuk melintasi seluruh jalan, jalan tersebut memiliki tundaan rambat 30 detik. Sekarang pertimbangkan apa yang terjadi jika jalur kedua dibuka di jalan (yaitu, kapasitasnya berlipat ganda). Dua mobil bisa masuk setiap lima detik, jadi kecepatannya naik dua kali lipat menjadi 0,4 mobil per detik. Tentu saja, penundaan 30 detik tidak akan berubah karena setiap mobil masih harus melintasi seluruh jarak.

Poin Penting

Penundaan propagasi menentukan waktu satu bit tetap transit di jaringan. Throughput, yang menentukan berapa banyak bit yang dapat masuk ke jaringan per satuan waktu, mengukur kapasitas jaringan.

Analogi jalan membantu menjelaskan pepatah: menambahkan lebih banyak lajur ke jalan akan meningkatkan jumlah mobil yang dapat memasuki jalan per satuan waktu, tetapi tidak akan mengurangi total waktu yang dibutuhkan untuk melintasi jalan tersebut. Jaringan mengikuti pola yang sama: menambahkan lebih banyak jalur transmisi paralel akan meningkatkan throughput jaringan, tetapi penundaan propagasi, yang bergantung pada jarak yang terbentang, tidak akan berkurang.

9.5 Jitter

Ukuran jaringan ketiga menjadi penting karena jaringan digunakan untuk transmisi suara dan video real-time. Ukuran, yang dikenal sebagai jitter jaringan, menilai varians dalam penundaan. Dua jaringan dapat memiliki rata-rata delay yang sama, tetapi nilai jitter yang berbeda. Khususnya, jika semua paket yang melintasi jaringan tertentu memiliki penundaan yang sama persis, D, jaringan tidak memiliki jitter. Namun, jika paket bergantian antara penundaan D+ε dan D–ε, jaringan memiliki penundaan rata-rata yang sama, tetapi memiliki jitter bukan nol.

Untuk memahami mengapa jitter itu penting, pertimbangkan untuk mengirim suara melalui jaringan. Di sisi pengirim, sinyal analog diambil sampelnya dan didigitalkan dan nilai digital delapan bit

dipancarkan setiap 125 detik. Sampel dikumpulkan ke dalam paket, yang kemudian ditransfer melalui jaringan. Di sisi penerima, nilai digital diekstraksi dan diubah kembali ke output analog. Jika jaringan memiliki nol jitter (yaitu, setiap paket membutuhkan waktu yang sama persis untuk transit jaringan), output audio akan sama persis dengan input aslinya; jika tidak, output akan cacat. Ada dua pendekatan umum untuk menangani jitter:

- Rancang jaringan isokron tanpa jitter
- Gunakan protokol yang mengkompensasi jitter

Sistem telepon tradisional menggunakan pendekatan pertama: sistem telepon menerapkan jaringan isokron yang menjamin penundaan di semua jalur adalah sama. Jadi, jika data digital dari panggilan telepon ditransmisikan melalui dua jalur, perangkat keras dikonfigurasi sehingga kedua jalur memiliki penundaan yang sama persis.

Transmisi suara atau video melalui Internet mengambil pendekatan kedua: meskipun jaringan yang mendasari mungkin memiliki jitter yang substansial, aplikasi suara dan video bergantung pada protokol waktu nyata untuk mengkompensasi jitter†. Karena menggunakan protokol waktu nyata jauh lebih murah daripada membangun jaringan isokron, perusahaan telepon melonggarkan persyaratan ketat untuk isokron. Tentu saja, sebuah protokol tidak dapat mengkompensasi jitter yang berubah-ubah — jika varians dalam penundaan menjadi berlebihan, output akan terpengaruh. Jadi, bahkan ketika menggunakan pendekatan kedua, penyedia layanan berusaha meminimalkan jitter di jaringan mereka.

9.6 Hubungan antara Delay dan Throughput

Secara teori, delay dan throughput dari sebuah jaringan adalah independen. Namun, dalam praktiknya, mereka dapat dikaitkan. Untuk memahami alasannya, pikirkan analogi jalan yang dibahas di atas. Jika mobil memasuki jalan pada interval waktu yang sama, mobil yang melaju di sepanjang jalan dengan kecepatan seragam diberi jarak pada interval yang seragam. Jika sebuah mobil melambat karena suatu alasan (misalnya, di persimpangan), orang lain di belakangnya juga akan melambat, menyebabkan kemacetan lalu lintas sementara. Mobil yang masuk ke jalan saat terjadi kemacetan akan mengalami tundaan yang lebih lama dibandingkan mobil yang melaju di jalan yang tidak macet. Situasi serupa terjadi di jaringan. Jika router memiliki antrian paket yang menunggu saat paket baru tiba, paket baru akan ditempatkan di bagian ekor antrian, dan harus menunggu saat router meneruskan paket sebelumnya. Jika terjadi kemacetan, paket-paket akan mengalami penundaan yang lebih lama daripada data yang masuk ke jaringan yang tidak aktif.

9.6.1 Pemanfaatan Sebagai Estimasi Keterlambatan

Ilmuwan komputer telah mempelajari hubungan antara penundaan dan kemacetan, dan telah menemukan bahwa dalam banyak kasus, penundaan yang diharapkan dapat diperkirakan dari persentase kapasitas jaringan yang digunakan saat ini. Jika D 0 menunjukkan penundaan saat jaringan idle, dan U adalah nilai antara 0 dan 1 yang menunjukkan penggunaan saat ini, penundaan efektif, D, diberikan dengan rumus sederhana:

$$D = \frac{D_0}{(1 - U)}$$

Ketika jaringan benar-benar menganggur, U adalah nol, dan penundaan efektif adalah D 0. Ketika jaringan beroperasi pada 1/2 kapasitasnya, penundaan efektif berlipat ganda. Saat lalu lintas mendekati kapasitas jaringan (yaitu, saat U mendekati 1), penundaan mendekati tak terhingga. Meskipun rumus hanya memberikan perkiraan penundaan efektif, kita dapat menyimpulkan:

> *Throughput dan delay tidak sepenuhnya independen. Saat lalu lintas di jaringan komputer meningkat, penundaan meningkat; jaringan yang beroperasi hampir 100% dari kapasitas throughputnya mengalami penundaan yang parah.*

Dalam praktiknya, manajer jaringan memahami bahwa pemanfaatan yang sangat tinggi dapat menghasilkan penundaan yang membawa bencana. Dengan demikian, sebagian besar manajer bekerja untuk menjaga pemanfaatan tetap rendah, dan mengukur lalu lintas di setiap jaringan secara konstan. Ketika rata-rata atau puncak pemanfaatan mulai naik di atas ambang batas yang telah ditetapkan, manajer meningkatkan kapasitas jaringan. Misalnya, jika pemanfaatan menjadi tinggi pada Ethernet 100 Mbps, manajer mungkin memilih untuk menggantinya dengan Gigabit Ethernet. Atau, manajer mungkin memilih untuk membagi jaringan menjadi dua, menempatkan setengah host di satu jaringan dan setengah host di jaringan lain (pembagian seperti itu sangat mudah dengan sakelar VLAN).

Seberapa tinggi seharusnya ambang batas pemanfaatan? Tidak ada jawaban yang sederhana; banyak manajer memilih nilai konservatif. Misalnya, salah satu ISP utama yang menjalankan jaringan backbone besar tetap menggunakan semua sirkuit digitalnya di bawah 50%. Lainnya menetapkan ambang batas pada 80% untuk menghemat uang. Bagaimanapun, manajer umumnya setuju bahwa jaringan tidak boleh dioperasikan di atas 90% dari kapasitas.

9.6.2 Produk Delay-Throughput

Setelah delay dan throughput jaringan diketahui, dimungkinkan untuk menghitung kuantitas menarik lainnya, produk delay-throughput†. Untuk memahami arti dari produk delay-throughput, pikirkan analogi jalan: ketika mobil memasuki jalan dengan kecepatan tetap T mobil per detik dan dibutuhkan mobil D detik untuk melintasi jalan, maka T × D mobil tambahan akan memasuki jalan pada saat mobil pertama telah melakukan perjalanan lengkap. Dengan demikian, total mobil T×D bisa berada di jalan. Dalam hal jaringan, jumlah bit perjalanan melalui jaringan setiap saat diberikan oleh:

$$\text{Bit dalam jaringan} = D \times T$$

di mana D adalah delay yang diukur dalam detik, dan T adalah throughput yang diukur dalam bit per detik.

Poin Penting

> *Produk dari delay dan throughput mengukur volume data yang dapat hadir pada jaringan. Sebuah jaringan dengan throughput T dan delay D dapat memiliki total bit T × D dalam perjalanan setiap saat.*

Produk delay-throughput penting untuk jaringan apapun dengan delay yang lama atau throughput yang besar karena mempengaruhi transmisi — aplikasi pengirim dapat mengirimkan volume data yang besar sebelum tujuan menerima bit pertama.

9.7 Mengukur Delay, Throughput, dan Jitter

Teknik yang digunakan untuk mengukur throughput dan jitter relatif mudah. Untuk menilai throughput, pengirim mentransfer sejumlah besar data. Penerima mencatat waktu dari awal data tiba sampai semua data tiba, dan menghitung throughput sebagai jumlah data yang dikirim per unit waktu. Teknik untuk mengukur jitter dikenal sebagai paket kereta: pengirim memancarkan serangkaian paket dengan kecil, penundaan tetap antara paket. Biasanya, paket di kereta dikirim secara berurutan. Penerima mencatat waktu di mana setiap paket tiba, dan menggunakan urutan waktu untuk menghitung perbedaan penundaan. Tidak seperti pengukuran throughput atau jitter, pengukuran delay yang tepat pada jalur dari host A ke host B memerlukan kedua host yang memiliki jam yang disinkronkan.

Selanjutnya, untuk mengukur delay pada jarak pendek (misalnya, LAN), jam harus sangat akurat. Alih-alih menggunakan jam yang disinkronkan, banyak alat pengukuran jaringan memilih pendekatan yang lebih mudah: ukur waktu pulang pergi dan bagi dua. Misalnya, ping dapat digunakan.

Mengukur kinerja jaringan bisa sangat sulit karena empat alasan:

- Rute bisa asimetris
- Kondisi berubah dengan cepat
- Pengukuran dapat mempengaruhi kinerja
- Lalu lintas padat

Poin pertama menjelaskan mengapa tidak mungkin menggunakan waktu pulang pergi untuk memperkirakan penundaan. Perutean asimetris berarti bahwa penundaan sepanjang jalur dari B ke A dapat berbeda secara substansial dari penundaan sepanjang jalur dari A ke B. Jadi, setengah dari waktu pulang pergi mungkin tidak memberikan ukuran yang akurat.

Poin kedua menjelaskan mengapa ukuran kinerja jaringan yang akurat bisa sulit diperoleh: kondisi berubah dengan cepat. Misalnya, pertimbangkan jaringan bersama. Jika hanya satu host yang mengirim data, host akan menikmati delay yang rendah, throughput yang tinggi, dan jitter yang rendah. Saat host lain mulai menggunakan jaringan, utilisasi meningkat, yang akan meningkatkan delay dan jitter serta menurunkan throughput. Selanjutnya, karena kondisi berubah dengan cepat, penundaan dapat sangat bervariasi hanya dalam satu detik. Jadi, bahkan jika pengukuran dilakukan setiap sepuluh detik, pengukuran dapat melewatkan perubahan besar dalam kinerja.
Poin ketiga menunjukkan bahwa mengirim lalu lintas uji untuk mengukur jaringan dapat memengaruhi kinerja jaringan. Di tempat pengujian penelitian PlanetLab, misalnya, begitu banyak peneliti menggunakan ping untuk mengukur kinerja sehingga lalu lintas ping sepenuhnya mendominasi lalu lintas lainnya. Situasi menjadi sangat parah sehingga administrator menetapkan kebijakan untuk mencegah penggunaan ping.

Poin keempat mendasar: jaringan data menunjukkan perilaku bursty, yang berarti lalu lintas tidak merata. Jika kita mempertimbangkan lalu lintas yang dikirim oleh komputer host tertentu, pola burstiness terlihat jelas: sebagian besar host tetap diam sampai pengguna menjalankan aplikasi yang berkomunikasi melalui Internet. Saat pengguna memasukkan URL di browser web, browser mengambil semua bagian halaman, dan kemudian berhenti berkomunikasi hingga pengguna meminta halaman lain. Demikian pula, jika pengguna mengunduh email, komputer host berkomunikasi dengan sistem email, mengunduh salinan kotak surat pengguna, dan kemudian menunggu pengguna.

Menariknya, lalu lintas data agregat juga meledak. Orang mungkin berharap bahwa burstiness adalah fenomena lokal dan ketika lalu lintas dari jutaan pengguna Internet digabungkan, hasilnya akan

menjadi pola penggunaan yang mulus. Lagi pula, tidak semua pengguna membaca email pada waktu yang sama; jadi, saat satu pengguna mengunduh, pengguna lain mungkin membaca email yang diunduh sebelumnya. Memang, pengukuran jaringan telepon suara menunjukkan bahwa lalu lintas telepon dari jutaan pengguna menghasilkan agregat yang halus. Namun, ketika lalu lintas dari satu juta pengguna Internet digabungkan, hasilnya bukanlah agregat yang mulus. Sebaliknya, agregat meledak dalam arti bahwa total lalu lintas memiliki titik puncak dan titik rendah. Faktanya, ahli statistik mengatakan bahwa lalu lintas data serupa, yang berarti bahwa lalu lintas dianalogikan dengan fraktal, di mana profil statistik yang sama terlihat pada perincian apa pun. Jadi, jika suatu perusahaan memeriksa LAN, lalu lintas dari host lokal akan muncul bursty. Jika ISP perantara mengukur lalu lintas dari seribu pengguna atau ISP besar mengukur lalu lintas dari sepuluh juta pengguna, lalu lintas akan memiliki jumlah absolut yang besar, tetapi akan menunjukkan pola statistik keseluruhan yang sama dengan lalu lintas di LAN.

Poin Penting

Tidak seperti lalu lintas telepon suara, lalu lintas data bersifat bursty. Lalu lintas data dikatakan serupa diri karena kumpulan lalu lintas data menunjukkan pola burstiness yang sama.

9.8 Pengukuran Pasif, Paket Kecil, dan NetFlow

Manajer jaringan yang mengukur jaringan membedakan antara dua bentuk pengukuran:

- Aktif
- Pasif

Kami telah membahas kelemahan teknik pengukuran aktif: dengan menyuntikkan lalu lintas ke dalam jaringan, lalu lintas pengukuran dapat mengubah kinerja jaringan. Alternatifnya adalah pengukuran pasif yang memantau jaringan dan menghitung paket, tetapi tidak menyuntikkan lalu lintas tambahan. Misalnya, ISP dapat menghitung byte yang ditransfer melalui tautan dalam jumlah waktu tertentu untuk menghasilkan perkiraan pemanfaatan tautan. Artinya, ISP mengatur stasiun monitor pasif yang mengamati jaringan selama interval waktu dan mengumpulkan total byte di semua paket.

Menariknya, ISP dapat memilih untuk mengukur jumlah paket yang dikirim serta jumlah byte data. Untuk memahami alasannya, perhatikan bahwa karena pemanfaatan tautan diukur sebagai persentase kapasitas dan kapasitas diukur dalam bit per detik, ISP perlu mengukur total bit data yang dikirim per satuan waktu. Namun, kapasitas switch dan router diukur dalam paket per detik. Artinya, karena router atau switch melakukan penerusan hop berikutnya sekali per paket, upaya komputasi yang dikeluarkan sebanding dengan jumlah paket yang diproses daripada jumlah bit dalam paket. Jika aliran data tiba pada 1 Gbps, switch atau router melakukan lebih sedikit pekerjaan jika aliran dibagi menjadi beberapa paket besar daripada jika aliran dibagi menjadi banyak paket kecil. Vendor peralatan jaringan memahami konsep tersebut, dan beberapa vendor membuat klaim kinerja tentang kecepatan data daripada kecepatan paket (yaitu, mereka mengukur kinerja produk mereka menggunakan paket besar).

Poin Penting

Untuk menilai pemanfaatan tautan, ISP mengukur total data yang ditransfer melalui tautan per satuan waktu; untuk menilai dampak pada router atau switch, ISP mengukur jumlah paket yang ditransfer per satuan waktu.

Salah satu teknik pengukuran pasif yang paling banyak digunakan awalnya dibuat oleh Cisco dan sekarang menjadi standar IETF: NetFlow. Router yang mengimplementasikan NetFlow secara statistik mengambil sampel paket sesuai dengan parameter yang ditetapkan oleh administrator jaringan (mis., sampel satu dari setiap seribu paket). Informasi diekstraksi dari header setiap paket sampel, informasi diringkas, dan ringkasan dikirim ke sistem manajemen jaringan di mana ia diproses (seringkali, data disimpan pada disk untuk analisis nanti). Biasanya, NetFlow mengekstrak alamat IP sumber dan tujuan, tipe datagram, dan nomor port protokol. Untuk memastikan bahwa itu pasif, router yang menjalankan NetFlow harus mengirim ringkasan NetFlow melalui port manajemen khusus daripada merutekannya melalui salah satu jaringan yang menangani data pengguna.

9.9 Quality Of Servic (QoS)

Rekanan dari pengukuran jaringan adalah penyediaan jaringan: merancang jaringan untuk menyediakan tingkat layanan tertentu. Sisa bab ini membahas mekanisme yang dapat digunakan untuk mengimplementasikan jaminan layanan. Secara garis besar, topik tersebut dikenal dengan istilah Quality of Service (QoS).

Untuk memahami QoS, pertimbangkan kontrak antara penyedia layanan dan pelanggan. Kontrak paling sederhana mendefinisikan layanan dengan menentukan kecepatan data yang dijamin oleh penyedia. Misalnya, penyedia yang menawarkan koneksi DSL ke Internet mungkin menjamin kecepatan data 2,2 Mbps. Kontrak yang lebih kompleks mendefinisikan layanan berjenjang, di mana tingkat layanan yang diterima tergantung pada jumlah yang dibayarkan. Misalnya, penyedia mungkin memilih pendekatan prioritas yang menjamin paket dari pelanggan yang berlangganan tingkat layanan platinum akan memiliki prioritas di atas paket dari pelanggan yang berlangganan layanan tingkat perak.

Pelanggan korporat besar seringkali menuntut jaminan layanan yang lebih ketat. Industri keuangan biasanya membuat kontrak layanan dengan batasan penundaan antara lokasi tertentu. Misalnya, perusahaan pialang mungkin memerlukan kontrak layanan yang menetapkan paket harus ditransfer dari kantor utama perusahaan ke Bursa Efek New York dalam waktu kurang dari 10 milidetik; perusahaan yang mencadangkan seluruh pusat data mereka setiap malam mungkin memerlukan kontrak layanan yang menjamin throughput tidak kurang dari 1 Gbps pada koneksi TCP yang digunakan untuk pencadangan.

9.10 Butir Halus dan Butir Kasar QoS

Bagaimana penyedia menentukan jaminan QoS, dan teknologi apa yang digunakan penyedia untuk menerapkan QoS? Gambar 9.3 mencantumkan dua pendekatan umum yang telah diusulkan untuk spesifikasi layanan. Seperti yang ditunjukkan gambar, pendekatannya berbeda dalam perinciannya dan apakah penyedia atau pelanggan memilih parameter.

Deskripsi	Deskripsi
Fine-Grain	Penyedia memungkinkan pelanggan untuk menyatakan persyaratan QoS spesifik untuk contoh komunikasi yang diberikan; pelanggan membuat permintaan setiap kali aliran dibuat (misalnya, untuk setiap koneksi TCP)

Coarse-Grain	Coarse-Grain Penyedia menentukan beberapa kelas layanan yang luas yang masing-masing cocok untuk satu jenis lalu lintas; pelanggan harus memasukkan semua lalu lintas ke dalam kelas

Gambar 9.3 Dua pendekatan yang telah diusulkan untuk spesifikasi layanan QoS.

9.10.1 Fine-Grain QoS

Sebagian besar pekerjaan awal QoS muncul dari perusahaan telepon. Perancang mengasumsikan jaringan data berorientasi koneksi yang dimodelkan setelah sistem telepon: ketika pelanggan perlu berkomunikasi dengan situs jarak jauh (misalnya, server web), pelanggan akan membuat koneksi. Selanjutnya, para perancang mengasumsikan pelanggan akan mengeluarkan persyaratan QoS untuk setiap koneksi, dan penyedia akan menghitung biaya sesuai dengan jarak yang terbentang dan QoS yang digunakan.

Perusahaan telepon memasukkan banyak fitur QoS dalam desain Asynchronous Transmission Mode (ATM). Meskipun ATM tidak bertahan dan penyedia umumnya tidak mengenakan biaya untuk setiap koneksi, beberapa terminologi yang dibuat ATM untuk QoS butiran halus masih bertahan dengan sedikit modifikasi. Alih-alih menentukan QoS pada koneksi, kami sekarang menggunakan istilah aliran. Aliran umumnya mengacu pada komunikasi lapisan transport seperti koneksi TCP, satu set paket UDP yang berjalan di antara sepasang aplikasi, atau panggilan telepon VoIP. Gambar 9.4 mencantumkan empat kategori utama layanan yang ada di ATM, dan menjelaskan bagaimana mereka berhubungan dengan arus.

Sjngkatan	Keterangan
CBR / Constant Bit Rate	Data memasuki aliran dengan kecepatan tetap, seperti data dari panggilan suara digital yang masuk tepat 64 Kbps
VBR / Variable Bit Rate	Data memasuki aliran pada kecepatan variabel dalam batas statistik yang ditentukan
ABR / Available Bit Rate	Aliran setuju untuk menggunakan kecepatan data apa pun yang tersedia pada waktu terte
UBR / Unspecified Bit Rate	Tidak ada kecepatan bit yang ditentukan untuk aliran; aplikasi puas dengan layanan upaya terbaik

Gambar 9.4 Empat kategori utama layanan QoS.

Seperti yang ditunjukkan gambar, layanan CBR sesuai untuk aliran yang mentransfer data dengan kecepatan tetap, dengan suara digital sebagai contoh kanonik. Layanan VBR sesuai untuk aliran yang menggunakan pengkodean tingkat variabel. Misalnya, beberapa codec video mengirim pengkodean diferensial, di mana jumlah data yang dikirim untuk sebuah frame sebanding dengan perbedaan antara frame sebelumnya dan frame saat ini. Dalam kasus seperti itu, pelanggan dapat menentukan kecepatan data rata-rata yang diharapkan serta kecepatan data maksimum dan lamanya waktu kecepatan maksimum akan terjadi. VBR meminta pengguna untuk menentukan:

- Kecepatan Bit Berkelanjutan (SBR)
- Kecepatan Bit Puncak (PBR)

- Ukuran Semburan Berkelanjutan (SBS)
- Ukuran Semburan Puncak (PBS)

Layanan ABR menyiratkan berbagi: pelanggan bersedia membayar berapa pun jumlah layanan yang tersedia. Jika pelanggan lain mengirim data, jumlah yang tersedia akan lebih rendah (dan mungkin penyedia akan mengenakan biaya lebih sedikit). Terakhir, layanan UBR berarti pelanggan tidak mau membayar biaya yang lebih tinggi dan puas dengan layanan upaya terbaik.

Ketika QoS Internet pertama kali dipertimbangkan, perusahaan telepon berpendapat bahwa layanan halus akan dibutuhkan sebelum kualitas panggilan telepon suara melalui jaringan paket dapat diterima. Akibatnya, selain bekerja di ATM, komunitas peneliti mulai mengeksplorasi QoS yang halus di Internet. Penelitian tersebut dikenal dengan nama Integrated Services (IntServ).

9.10.2 QoS Butir Kasar dan Kelas Layanan

Alternatif untuk QoS butiran halus adalah pendekatan butiran kasar di mana lalu lintas dibagi ke dalam kelas dan parameter QoS ditetapkan ke kelas daripada aliran individu. Untuk memahami motivasi untuk pendekatan butiran kasar, perlu untuk mempertimbangkan implementasi QoS pada router inti. Koneksi ke router masing-masing dapat beroperasi pada 10 Gbps, yang berarti paket tiba dengan kecepatan yang sangat tinggi; diperlukan perangkat keras khusus untuk melakukan penerusan karena prosesor konvensional terlalu lambat. Selanjutnya, karena membawa lalu lintas di antara ISP utama, router inti dapat menangani jutaan aliran simultan. QoS membutuhkan banyak sumber daya tambahan. Router harus mempertahankan status untuk jutaan aliran, dan harus melakukan perhitungan yang kompleks untuk setiap paket. Akses memori memperlambat pemrosesan. Selain itu, router harus mengalokasikan sumber daya saat aliran dimulai, dan membatalkan alokasi saat aliran berakhir.

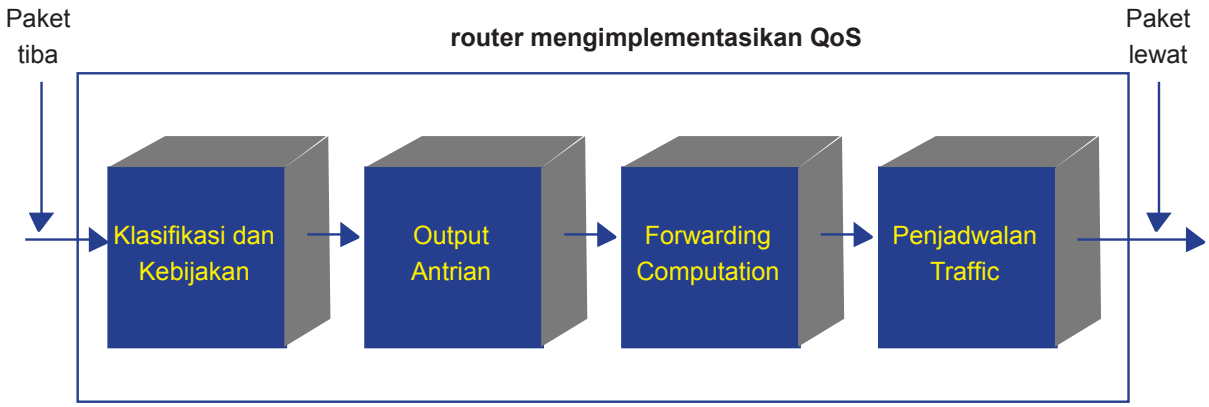
Setelah bertahun-tahun melakukan penelitian tentang Layanan Terpadu dan pembuatan beberapa protokol, komunitas peneliti dan IETF menyimpulkan bahwa pendekatan butiran halus umumnya tidak praktis dan tidak perlu. Di satu sisi, rata-rata pengguna tidak akan memiliki pemahaman yang cukup tentang QoS untuk memilih parameter. Lagi pula, persyaratan throughput apa yang akan ditentukan seseorang untuk koneksi ke situs web biasa? Di sisi lain, router inti memiliki kekuatan pemrosesan yang tidak mencukupi untuk mengimplementasikan QoS per aliran. Dengan demikian, sebagian besar pekerjaan pada QoS berkonsentrasi pada pendefinisian beberapa kelas layanan yang luas daripada mencoba menyediakan QoS ujung ke ujung untuk setiap aliran individu.

Poin Penting

Meskipun bertahun-tahun penelitian dan standar bekerja, pendekatan halus untuk QoS telah diturunkan ke beberapa kasus khusus.

9.11 Implementasi QoS

Gambar 9.5 mengilustrasikan empat langkah yang digunakan switch atau router untuk mengimplementasikan QoS.



Gambar 9.5 Empat langkah kunci yang digunakan untuk mengimplementasikan QoS.

Klasifikasi Dan Pemolisian. Ketika sebuah paket tiba, router mengklasifikasikan paket dengan menetapkan paket pengidentifikasi aliran. Untuk sistem butiran halus, pengidentifikasi menentukan koneksi individu; untuk sistem butiran kasar, pengidentifikasi menentukan kelas lalu lintas. Setelah pengenal telah ditetapkan, router melakukan pemolisian, yang berarti bahwa router memverifikasi bahwa paket tidak melanggar parameter untuk aliran. Khususnya, jika pelanggan mengirim data lebih cepat dari tarif maksimum yang pelanggan bayar, polisi mulai membuang paket. Salah satu teknik yang digunakan untuk pemolisian adalah Random Early Discard (RED) di mana paket pada aliran tertentu dijatuhkan secara probabilistik. Antrian dibuat untuk aliran, dan ukuran antrian saat ini digunakan untuk menentukan kemungkinan penurunan. Ketika antrian kurang dari setengah penuh, probabilitas diatur ke nol. Ketika antrian benar-benar penuh, probabilitas diatur ke satu. Pada ukuran antrian di antaranya, probabilitasnya berbanding lurus dengan jumlah paket dalam antrian. Menggunakan RED membantu menghindari masalah siklik yang disebabkan oleh tail drop di mana semua paket yang masuk dibuang begitu antrian terisi, banyak sesi TCP masing-masing mundur dan mulai lambat, lalu lintas meningkat hingga antrian terisi lagi, dan siklus berulang.

Komputasi Penerusan. Saat menghitung next-hop, router atau switch dapat menggunakan pengidentifikasi aliran. Dalam beberapa kasus, pengidentifikasi aliran menentukan jalur yang harus diikuti (misalnya, semua lalu lintas suara dikirim ke port 54 ke sakelar suara). Dalam kasus lain, pengidentifikasi aliran diabaikan dan alamat tujuan di setiap paket digunakan untuk memilih hop berikutnya. Detail yang tepat dari penerusan bergantung pada tujuan sakelar atau router tertentu dan kebijakan QoS manajer.

Antrian Keluaran. Sebagian besar implementasi QoS membuat satu set antrian untuk setiap port keluaran. Setelah komputasi penerusan memilih port keluaran untuk paket, mekanisme antrian keluaran menggunakan pengidentifikasi aliran untuk menempatkan paket di salah satu antrian yang terkait dengan port. Sistem butiran kasar biasanya menggunakan satu antrian per kelas. Jadi, jika seorang manajer menetapkan delapan kelas QoS, setiap port keluaran akan memiliki delapan antrian. Sebuah sistem fine-grain sering memiliki satu antrian per koneksi, dengan antrian yang diatur dalam hierarki. Misalnya, satu chip prosesor jaringan menyediakan 256.000 antrian yang diatur dalam hierarki multi-level.

Penjadwalan Lalu Lintas. Penjadwal lalu lintas mengimplementasikan kebijakan QoS dengan memilih paket untuk dikirim setiap kali port tidak digunakan. Misalnya, seorang manajer mungkin menentukan bahwa tiga pelanggan masing-masing menerima 25% dari kapasitas dan semua pelanggan lain berbagi kapasitas yang tersisa. Untuk menerapkan kebijakan tersebut, penjadwal lalu lintas mungkin menggunakan empat antrian dan pendekatan round-robin untuk memilih paket. Jadi, jika semua pelanggan mengirim data, tiga pelanggan yang ditunjuk masing-masing akan menerima seperempat dari kapasitas, seperti yang ditentukan.

Algoritma pemilihan paket yang lebih canggih dapat digunakan untuk mengimplementasikan pembagian proporsional yang kompleks. Kompleksitas muncul karena penjadwal lalu lintas harus mempertahankan kebijakan jangka panjang meskipun paket tiba dalam jumlah besar. Jadi, penjadwal lalu lintas harus beradaptasi dengan situasi di mana antrian yang diberikan untuk sementara melebihi kecepatan data yang diberikan asalkan rata-rata jangka panjang memenuhi batas yang ditentukan. Demikian pula, penjadwal lalu lintas harus beradaptasi dengan situasi di mana satu atau lebih antrian kosong sementara dengan membagi kapasitas yang tidak terpakai di antara antrian lainnya.

Banyak algoritma penjadwalan lalu lintas telah diusulkan dan dianalisis. Tidak mungkin membuat algoritme praktis yang mencapai kesempurnaan; masing-masing adalah kompromi antara keadilan dan overhead komputasi. Gambar 9.6 daftar algoritma manajemen lalu lintas yang telah diusulkan dan dipelajari.

Algoritma	Deskripsi
Leaky Bucket	Mengizinkan antrian untuk mengirim paket dengan kecepatan tetap dengan menambah penghitung paket secara berkala dan menggunakan penghitung untuk mengontrol transmisi
Token Bucket	Mengizinkan antrian untuk mengirim data dengan kecepatan tetap dengan menambah penghitung byte secara berkala dan menggunakan penghitung untuk mengontrol transmisi
Weighted Round Robin	Memilih paket dari sekumpulan antrian sesuai dengan sekumpulan bobot yang membagi kapasitas menjadi persentase tetap, dengan asumsi ukuran paket seragam
Deficit Round Robin	Varian dari pendekatan round-robin yang memperhitungkan byte yang dikirim daripada paket yang ditransfer, dan memungkinkan defisit sementara yang disebabkan oleh paket besar

Gambar 9.6 Contoh algoritma penjadwalan lalu lintas.

9.12 Teknologi QoS Internet

IETF telah merancang serangkaian teknologi dan protokol yang terkait dengan QoS. Tiga upaya penting adalah:

- RSVP dan COPS
- DiffServ
- MPLS

RSVP dan COPS. Saat menjelajahi IntServ, IETF mengembangkan dua protokol untuk menyediakan QoS: Resource ReSerVation Protocol (RSVP) dan protokol Common Open Policy Services

(COPS). RSVP adalah versi QoS yang halus. Dengan demikian, RSVP diperlukan untuk setiap sesi TCP atau UDP. Untuk menggunakan RSVP, aplikasi mengirimkan permintaan yang menentukan QoS yang diinginkan. Setiap router di sepanjang jalur dari sumber ke tujuan menyimpan sumber daya yang diminta dan meneruskan permintaan ke router berikutnya. Akhirnya, host tujuan harus menyetujui permintaan tersebut. Ketika setiap hop di sepanjang jalur telah setuju untuk memenuhi permintaan, pengidentifikasi aliran dibuat dan dikembalikan. Lalu lintas dapat dikirim di sepanjang jalur yang dipesan. COPS adalah protokol pendamping untuk RSVP yang digunakan untuk menentukan dan menegakkan kebijakan. Sebuah router yang mengimplementasikan pemolisian menggunakan COPS untuk berkomunikasi dengan server kebijakan dan memperoleh informasi tentang parameter aliran. Karena dirancang untuk menyediakan QoS per aliran yang halus, RSVP jarang digunakan.

DiffServ. Setelah meninggalkan IntServ dan QoS fine-grain, IETF membuat Differentiated Services (DiffServ) untuk mendefinisikan mekanisme QoS kasar. Upaya DiffServ menghasilkan definisi tentang bagaimana kelas dapat ditentukan dan bagaimana bidang JENIS LAYANAN dalam header IPv4 atau IPv6 dapat digunakan untuk menentukan kelas datagram. Meskipun berbagai ISP telah bereksperimen dengan DiffServ, teknologi ini tidak diterima secara luas.

MPLS. Bab 19 menjelaskan MultiProtocol Label Switching (MPLS) sebagai mekanisme komunikasi berorientasi koneksi yang dibangun di atas IP. Untuk menggunakan MPLS, seorang manajer mengonfigurasi jalur penerusan melalui serangkaian router berkemampuan MPLS. Di salah satu ujung jalur, setiap datagram dienkapsulasi dalam header MPLS dan disuntikkan ke jalur MPLS; di ujung lain, setiap datagram diekstraksi, header MPLS dihapus, dan datagram diteruskan ke tujuannya. Dalam banyak kasus, kebijakan penjadwalan lalu lintas ditetapkan ke jalur MPLS, yang berarti bahwa ketika datagram dimasukkan ke jalur tertentu, parameter QoS ditetapkan untuk datagram. Dengan demikian, ISP mungkin menyiapkan jalur MPLS untuk data suara yang terpisah dari jalur MPLS yang digunakan untuk data lain.

9.13 Ringkasan

Dua ukuran utama kinerja jaringan adalah penundaan, waktu yang dibutuhkan untuk mengirim bit dari satu komputer ke komputer lain, dan throughput, jumlah bit per detik yang dapat ditransmisikan melalui jaringan. Meskipun throughput biasa disebut kecepatan, throughput adalah ukuran kapasitas jaringan. Produk delay-throughput mengukur jumlah data yang dapat transit pada saat tertentu. Penundaan dan throughput tidak independen — karena throughput mendekati 100% dari kapasitas, penundaan meningkat dengan cepat.

Jitter, ukuran varians dalam penundaan, menjadi penting dalam jaringan data. Jitter rendah dapat dicapai dengan jaringan isochronous atau dengan protokol yang menangani transmisi audio dan video real-time; Internet menggunakan pendekatan protokol.

Mengukur kinerja jaringan bisa jadi sulit. Rute asimetris berarti jam yang disinkronkan diperlukan untuk mengukur penundaan; lalu lintas yang padat berarti kinerja dapat berubah dengan cepat. Karena lalu lintas tambahan dari pengukuran dapat mengubah kondisi jaringan, banyak manajer lebih memilih teknologi pengukuran pasif, seperti NetFlow.

Baik QoS butiran halus dan butiran kasar telah dipelajari; upaya halus umumnya telah ditinggalkan. Kategori layanan yang ditentukan ATM, dan akronimnya masih digunakan: Constant, Variable, Available, dan Unspecified Bit Rate (CBR, VBR, ABR, dan UBR).

Untuk mengimplementasikan QoS, switch atau router mengklasifikasikan dan mengatur data yang masuk, meneruskan dan menempatkan setiap paket pada antrian keluaran, dan menggunakan pengatur lalu lintas untuk memilih paket yang akan dikirim ketika port keluaran menjadi bebas. Beberapa algoritma penjadwalan lalu lintas telah diusulkan dan dianalisis; masing-masing merupakan tradeoff antara keadilan optimal dan overhead komputasi.

IETF mendefinisikan RSVP dan COPS sebagai bagian dari upaya IntServ; ketika penekanan bergeser dari QoS butiran halus, IETF mendefinisikan DiffServ. IETF juga mendefinisikan MPLS sebagai teknologi rekayasa lalu lintas. Parameter QoS dapat dikaitkan dengan setiap terowongan MPLS, yang berarti bahwa setelah datagram diklasifikasikan, asosiasi MPLS-nya mendefinisikan parameter QoS-nya.

Latihan

1. Sebutkan dan jelaskan tiga ukuran utama kinerja jaringan.
2. Berikan lima jenis keterlambatan beserta penjelasannya masing-masing.
3. Apakah Anda mengharapkan penundaan akses lebih lama pada LAN atau WAN? Keterlambatan antrian? Mengapa?
4. Bagaimana throughput dapat diukur?
5. Nama apa yang digunakan untuk bentuk throughput yang paling berarti bagi pengguna?
6. Berikan contoh pemrosesan yang membuat goodput kurang dari kapasitas saluran.
7. Memberikan penjelasan tentang delay dan throughput dalam hal bit yang ditransmisikan.
8. Penundaan atau throughput mana yang memberikan batas paling mendasar pada kinerja? Mengapa?
9. Gunakan ping untuk mengukur latensi jaringan ke situs lokal dan jauh. Berapakah penundaan Internet minimum dan maksimum yang dapat Anda temukan?
10. Jika seseorang mem-ping alamat IP 127.0.0.1, latensinya sangat rendah. Menjelaskan.
11. Unduh salinan program ttcp dan gunakan untuk mengukur throughput di Ethernet lokal. Apa goodputnya? Perkirakan pemanfaatan tautan yang dicapai.
12. Bandingkan throughput jaringan 100 Mbps dan jaringan 1 Gbps.
13. pa itu jitter, dan apa dua pendekatan yang digunakan untuk mengatasi jitter?
14. Profesional terkadang merujuk pada "lutut" di kurva penundaan. Untuk memahami apa artinya, plot penundaan efektif untuk nilai pemanfaatan antara 0 dan 0,95. Dapatkah Anda menemukan nilai pemanfaatan yang kurvanya tampak meningkat tajam?
15. Berapa banyak data yang dapat “dalam penerbangan” antara stasiun bumi pengirim, satelit, dan stasiun penerima? Untuk mengetahuinya, hitung produk delay-throughput untuk jaringan satelit GEO yang beroperasi pada 3 Mbps. Asumsikan bahwa satelit mengorbit pada 20.000 mil di atas bumi, dan transmisi radio merambat dengan kecepatan cahaya.
16. Mengapa pengukuran kinerja jaringan sulit?
17. Bagaimana lalu lintas data berbeda dari lalu lintas suara
18. Jelaskan mengapa ISP menghitung jumlah paket yang diterima per satuan waktu, bukan hanya jumlah byte yang diterima per satuan waktu.

19. Apa saja dua jenis QoS?
20. Perkirakan daya komputasi yang diperlukan untuk mengimplementasikan QoS butiran halus di inti Internet: asumsikan tautan 10 Gbps mengirimkan paket 1000 byte dan N operasi aritmatika per paket, dan hitung jumlah operasi yang perlu dilakukan prosesor per detik .
21. Sebutkan empat kategori utama QoS yang diturunkan dari ATM, dan berikan artinya masing-masing.
22. Pertimbangkan browser web. Jenis QoS apa yang sesuai untuk aliran tipikal di mana browser mengunduh halaman web? Mengapa?
23. Jika dua pengguna membuat sesi obrolan melalui Internet, kategori QoS apa yang akan mereka gunakan?
24. Empat parameter apa yang digunakan untuk mengkarakterisasi aliran VBR?
25. Jelaskan empat langkah yang digunakan untuk mengimplementasikan QoS.
26. Jika ISP Anda menggunakan ember bocor untuk menjadwalkan transmisi paket, apakah throughput Anda akan lebih tinggi dengan paket besar atau paket kecil? Menjelaskan.
27. Apa itu DiffServ?
9. Bagaimana penerusan MPLS berbeda dari penerusan IP konvensional

Bab 10 Multimedia dan IP Telephony (VoIP)

Bab ini akan membahas tentang:

- Transfer multimedia melalui Internet.
- Bagaimana multimedia dapat dikirim melalui mekanisme komunikasi upaya terbaik
- Protokol tujuan umum untuk lalu lintas waktu nyata, dan mempertimbangkan transmisi panggilan telepon suara secara rinci.

10.1 Transmisi Data Real-Time dan Pengiriman Best-Effort

Kami menggunakan istilah multimedia untuk merujuk pada data yang berisi audio atau video, dan mungkin termasuk teks. Ungkapan multimedia real-time mengacu pada data multimedia yang harus direproduksi pada kecepatan yang sama persis dengan yang ditangkap (misalnya, program berita televisi yang mencakup audio dan video dari peristiwa yang sebenarnya).

Muncul pertanyaan, bagaimana Internet dapat digunakan untuk transmisi real-time multimedia? Untuk memahami kesulitannya, ingatlah bahwa Internet menawarkan layanan pengiriman dengan upaya terbaik. Dengan demikian, paket dapat hilang, tertunda, atau dikirim tidak sesuai pesanan — jika audio atau video didigitalkan, dikirim melalui Internet tanpa perlakuan khusus, dan kemudian ditampilkan tepat saat tiba, output yang dihasilkan tidak dapat diterima. Sistem multimedia awal memecahkan masalah dengan membuat jaringan komunikasi yang dirancang khusus untuk menangani audio atau video. Jaringan telepon analog menggunakan jaringan isokron untuk menyediakan reproduksi audio berkualitas tinggi, dan sistem televisi kabel analog dirancang untuk mengirimkan banyak saluran video siaran tanpa gangguan atau kehilangan.

Alih-alih membutuhkan jaringan yang mendasarinya untuk menangani transmisi waktu nyata, Internet menggunakan dukungan protokol tambahan. Menariknya, masalah yang paling signifikan untuk ditangani adalah jitter, bukan packet loss. Untuk mengetahui alasannya, pertimbangkan siaran web langsung. Jika sebuah protokol menggunakan timeout-and-retransmission untuk mengirim ulang paket,

paket yang ditransmisikan ulang akan datang terlambat untuk berguna — penerima akan memutar video dan audio dari paket yang berurutan, dan tidak masuk akal untuk memasukkan cuplikan webcast yang terlewatkan sebelumnya.

Poin Penting

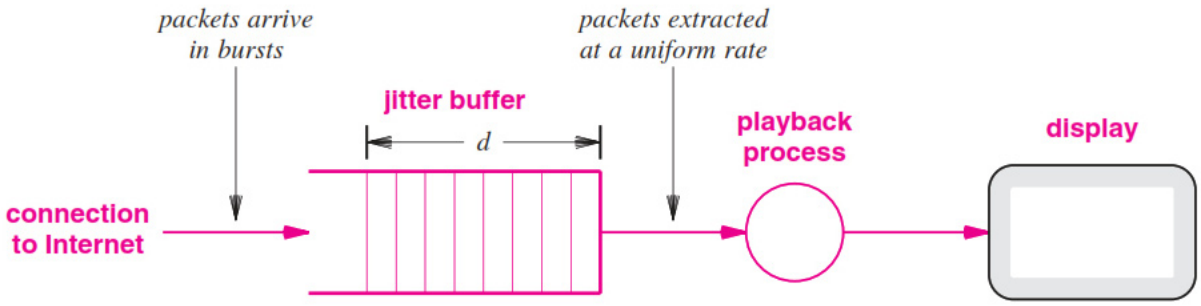
Tidak seperti protokol transport konvensional, protokol yang mentransfer data real-time hanya menangani masalah jitter, dan tidak mengirimkan kembali paket yang hilang.

10.2 Pemutaran Tertunda dan Buffer Jitter

Untuk mengatasi jitter dan mencapai pemutaran data real-time yang mulus, dua teknik utama digunakan:

- Stempel waktu. Pengirim memberikan stempel waktu untuk setiap bagian data. Penerima menggunakan stempel waktu untuk menangani paket yang tidak sesuai pesanan dan untuk menampilkan data dalam urutan waktu yang benar.
- penyangga jitter. Untuk mengakomodasi jitter (yaitu, perbedaan kecil dalam penundaan), penerima menyimpan data dan menunda pemutaran.

Implementasi buffer jitter sangat mudah. Penerima menyimpan daftar item data, dan menggunakan stempel waktu untuk mengurutkan daftar. Sebelum memulai pemutaran, penerima menunda selama d unit waktu, yang berarti data yang diputar adalah d unit waktu di belakang data yang datang. Jadi, jika paket yang diberikan tertunda kurang dari d, isi paket akan ditempatkan di buffer sebelum dibutuhkan untuk pemutaran. Dengan kata lain, item dimasukkan ke dalam buffer jitter dengan beberapa variasi kecepatan, tetapi proses pemutaran mengekstrak data dari buffer jitter dengan kecepatan tetap. Gambar 10.1 mengilustrasikan pengorganisasian sistem pemutaran waktu nyata.



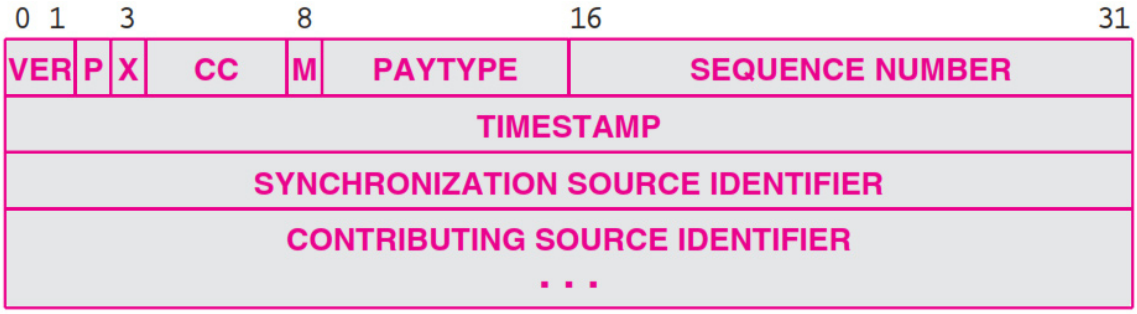
Gambar 10.1 Ilustrasi buffer jitter dengan delay d.

10.3 Protokol Transportasi Waktu Nyata (RTP)

Dalam paket protokol Internet, Protokol Transportasi Waktu Nyata (RTP) menyediakan mekanisme yang digunakan untuk mengirimkan data waktu nyata melalui Internet. Istilah Transport adalah keliru karena RTP berada di atas lapisan transport. Jadi, terlepas dari namanya, orang harus menganggap RTP sebagai protokol transfer.

RTP tidak memastikan pengiriman data tepat waktu, dan tidak menyertakan buffer jitter atau mekanisme pemutaran. Sebagai gantinya, ia menyediakan tiga item di setiap paket yang mengizinkan penerima untuk mengimplementasikan buffer jitter:

- Nomor urut yang memungkinkan penerima untuk menempatkan paket yang masuk dalam urutan yang benar dan untuk mendeteksi paket yang hilang
- Stempel waktu yang memungkinkan penerima memutar data dalam paket pada waktu yang tepat dalam aliran multimedia
- Serangkaian pengidentifikasi sumber yang memungkinkan penerima mengetahui sumber data



Gambar 10.2 mengilustrasikan bagaimana nomor urut, stempel waktu, dan bidang pengenal sumber muncul di header paket RTP.

Field VER memberikan nomor versi RTP, yang saat ini 2. Field P menentukan apakah payload adalah zero-padded (beberapa pengkodean memerlukan ukuran blok tetap). Bidang X menentukan apakah ekstensi header ada, dan CC memberikan jumlah sumber yang telah digabungkan untuk menghasilkan aliran seperti yang dijelaskan di bawah ini. M adalah bit penanda yang dapat digunakan untuk menandai beberapa frame. Secara khusus, beberapa pengkodean video mengirim bingkai penuh diikuti oleh serangkaian perubahan tambahan; bit M hanya diset jika paket RTP membawa bingkai penuh. Bidang PAYTYPE menentukan jenis muatan; penerima menggunakan nilai PAYTYPE untuk menafsirkan sisa paket.

Setiap paket menyertakan NOMOR URUTAN; urutannya bertambah satu untuk setiap paket. Seperti TCP, pengirim memilih urutan awal acak untuk membantu menghindari masalah replay. Bidang TIMESTAMP yang tidak bergantung pada urutan memberikan informasi kepada penerima tentang waktu pemutaran. Menjaga stempel waktu agar tidak bergantung pada urutan adalah penting dalam kasus di mana waktu tidak secara linier terkait dengan urutan paket (misalnya, pengkodean video ukuran variabel yang mengirimkan lebih sedikit paket ketika gambar tidak berubah dengan cepat).

RTP TIMESTAMP tidak mengkodekan tanggal dan waktu. Sebaliknya, RTP memilih stempel waktu awal acak, dan kemudian membuat setiap stempel waktu berturut-turut relatif terhadap nilai awal. Selanjutnya, RTP tidak menentukan apakah waktu diukur dalam detik, milidetik, atau unit lain — jenis muatan menentukan granularitas cap waktu. Tidak peduli berapa perincian waktu yang digunakan, pengirim harus menambah waktu secara terus menerus, bahkan ketika tidak ada paket yang dikirim (misalnya, jika codec menekan transmisi selama periode diam dari aliran audio).

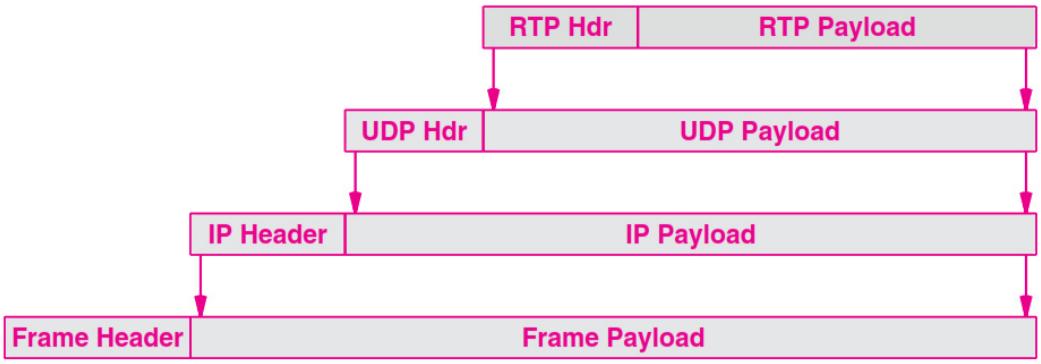
Dua bidang SYNCHRONISATION SOURCE IDENTIFIER dan CONTRIBUTING SOURCE IDENTIFIER mengidentifikasi sumber data. Alasan sumber harus diidentifikasi muncul dari mekanisme pengiriman multicast: host dapat menerima data dari berbagai sumber dan dapat menerima banyak salinan dari paket yang diberikan. Alasan beberapa sumber diidentifikasi muncul dari teknik yang dikenal

sebagai pencampuran di mana sistem perantara menggabungkan data dari beberapa aliran waktu nyata untuk menghasilkan aliran baru. Misalnya, mixer dapat menggabungkan aliran video dan audio yang terpisah dari sebuah film, dan kemudian melakukan multicast pada aliran gabungan tersebut.

10.4 RTP Enkapsulasi

RTP menggunakan UDP untuk transportasi pesan. Jadi, setiap pesan RTP dienkapsulasi dalam datagram UDP untuk transmisi melalui Internet. Gambar 10.3 mengilustrasikan tiga tingkat enkapsulasi yang digunakan ketika pesan RTP ditransfer melalui satu jaringan.

Karena RTP menggunakan enkapsulasi UDP, pesan yang dihasilkan dapat dikirim melalui siaran atau multicast. Multicast sangat berguna untuk penyampaian program hiburan yang menarik bagi khalayak yang besar. Misalnya, jika penyedia kabel menawarkan program televisi atau acara olahraga, beberapa pelanggan dapat menonton secara bersamaan. Dalam kasus seperti itu, alih-alih mengirim salinan pesan ke setiap pelanggan, RTP memungkinkan penyedia untuk menjangkau pelanggan dengan menggandakan salinan pesan RTP di setiap subnet logis. Jika multicast yang diberikan mencapai rata-rata N pelanggan, jumlah lalu lintas akan dikurangi dengan faktor N.



Gambar 10.3 Tiga level enkapsulasi yang digunakan dengan RTP.

10.5 IP Telepon

Istilah IP telephony† atau Voice over IP (VoIP) digunakan untuk menggambarkan salah satu aplikasi multimedia yang paling luas. Perusahaan telepon di seluruh dunia mengganti sakelar telepon tradisional dengan router IP. Motivasinya ekonomis: biaya router jauh lebih murah daripada sakelar telepon tradisional. Perusahaan juga mulai menggunakan telepon IP karena alasan ekonomi: mengirim data dan suara dalam datagram IP menurunkan biaya karena infrastruktur jaringan yang mendasarinya digunakan bersama — satu set peralatan, kabel, dan koneksi jaringan cukup untuk semua komunikasi, termasuk panggilan telepon.

Ide dasar di balik IP telephony sangat mudah: sampel audio terus-menerus, konversikan setiap sampel ke bentuk digital, kirim aliran digital yang dihasilkan melintasi jaringan IP dalam bentuk paket, dan konversikan aliran kembali ke analog untuk pemutaran. Namun, banyak detail memperumit tugas. Pengirim tidak dapat menunggu untuk mengisi paket besar karena hal itu akan menunda transmisi beberapa detik. Sistem harus menangani pengaturan panggilan: ketika penelepon memanggil, sistem harus menerjemahkan nomor telepon ke alamat IP, dan menemukan pihak yang ditentukan. Saat

panggilan dimulai, pihak yang dipanggil harus menerima dan menjawab panggilan tersebut. Demikian pula, ketika panggilan berakhir, kedua pihak harus sepakat tentang cara mengakhiri komunikasi.

Komplikasi yang paling signifikan muncul karena IP telephony berusaha untuk menjadi kompatibel ke belakang dengan Public Switched Telephone Network (PSTN) yang ada. Artinya, alih-alih membatasi panggilan ke telepon IP, mekanisme memungkinkan penelepon atau penerima panggilan untuk menggunakan telepon di mana saja di PSTN, termasuk lokasi internasional atau koneksi seluler. Dengan demikian, sistem telepon IP harus disiapkan untuk menangani panggilan yang berasal dari PSTN dan berakhir di telepon IP, atau sebaliknya. Pengguna mengharapkan sistem telepon IP untuk menyediakan layanan telepon yang ada seperti penerusan panggilan, panggilan tunggu, pesan suara, panggilan konferensi, dan ID pemanggil. Selain itu, bisnis yang saat ini mengoperasikan Private Branch Exchange (PBX) mungkin memerlukan sistem telepon IP untuk menawarkan layanan yang setara dengan PBX.

10.6 Pensinyalan dan Standar Pensinyalan VoIP

Dua kelompok telah menciptakan standar untuk IP telephony: International Telecommunications Union (ITU), yang mengontrol standar telepon, dan Internet Engineering Task Force (IETF), yang mengontrol standar TCP/IP. Setelah mempertimbangkan komponen konseptual dari sistem telepon IP, kami akan meninjau protokol yang telah dipilih masing-masing kelompok.

Untungnya, kedua kelompok sepakat tentang dasar-dasar penyandian dan transmisi audio:

- Audio dikodekan menggunakan Pulse Code Modulation (PCM)
- RTP digunakan untuk mentransfer audio digital

Kompleksitas utama telepon IP (dan alasan mengapa banyak standar telah diusulkan) terletak pada pengaturan panggilan dan manajemen panggilan. Dalam terminologi telepon, proses membangun dan mengakhiri panggilan dikenal sebagai pensinyalan, dan mencakup pemetaan nomor telepon ke suatu lokasi, menemukan rute ke pihak yang dipanggil, dan menangani detail lain seperti penerusan panggilan. Mekanisme yang digunakan dalam sistem telepon tradisional untuk menangani manajemen panggilan dikenal sebagai Signaling System 7 (SS7).

Salah satu pertanyaan mendasar tentang telepon IP berpusat pada pendekatan yang akan diambil untuk pensinyalan — haruskah sistem pensinyalan dipusatkan seperti sistem telepon saat ini, atau haruskah didistribusikan seperti pemetaan saat ini dari nama domain ke alamat IP? Pendukung pendekatan terdistribusi berpendapat bahwa seharusnya dua telepon IP, pada titik sembarang di Internet, untuk menemukan satu sama lain dan berkomunikasi persis seperti aplikasi Internet saat ini (yaitu, telepon IP bertindak sebagai server untuk menerima panggilan masuk, dan sebagai klien untuk melakukan panggilan keluar). Dalam pendekatan terdistribusi, tidak ada infrastruktur lebih lanjut yang diperlukan di luar DNS dan layanan penerusan IP yang saat ini tersedia untuk komunikasi data. Pendekatan terdistribusi sangat relevan untuk sistem telepon IP lokal (misalnya, sistem yang memungkinkan panggilan antara dua telepon IP dalam satu perusahaan). Pendukung pendekatan terpusat berpendapat bahwa model telepon konvensional bekerja paling baik karena memberi perusahaan telepon kendali atas pengaturan panggilan memungkinkan mereka untuk memberikan jaminan layanan.

Agar kompatibel dengan telepon yang ada, protokol baru harus dapat berinteraksi dengan SS7, baik untuk melakukan panggilan keluar maupun menerima panggilan masuk. Saat perdebatan tentang pendekatan dasar berlanjut, empat set protokol pensinyalan diusulkan untuk digunakan dengan telepon IP: IETF mengusulkan Session Initiation Protocol (SIP) dan Media Gateway Control Protocol (MGCP), ITU mengusulkan satu set besar dan komprehensif protokol di bawah payung umum H.323, dan kedua kelompok bersama-sama mengusulkan Megaco (H.248).

Poin Penting

Proses penyiapan dan penghentian panggilan dikenal sebagai pensinyalan; beberapa protokol pensinyalan telah diusulkan untuk digunakan dengan telepon IP.

10.7 Komponen Sistem Telepon IP

Gambar 10.4 mencantumkan empat komponen utama sistem telepon IP, dan Gambar 10.5 menggambarkan bagaimana mereka digunakan untuk menghubungkan jaringan.

Komponen	Cara Kerja
IP telephone	Beroperasi seperti telepon konvensional, tetapi menggunakan IP untuk mengirim suara digital
Media Gateway Controller	Menyediakan kontrol dan koordinasi antara telepon IP untuk layanan seperti pengaturan panggilan, penghentian panggilan, dan penerusan panggilan
Media Gateway	Menyediakan koneksi antara dua jaringan yang menggunakan penyandian berbeda, dan diterjemahkan sebagai panggilan lewat di antara mereka
Signaling Gateway	Terhubung ke dua jaringan yang menggunakan mekanisme pensinyalan berbeda, dan menerjemahkan permintaan dan tanggapan manajemen panggilan

Gambar 10.4 Empat blok bangunan utama dari sistem telepon IP.

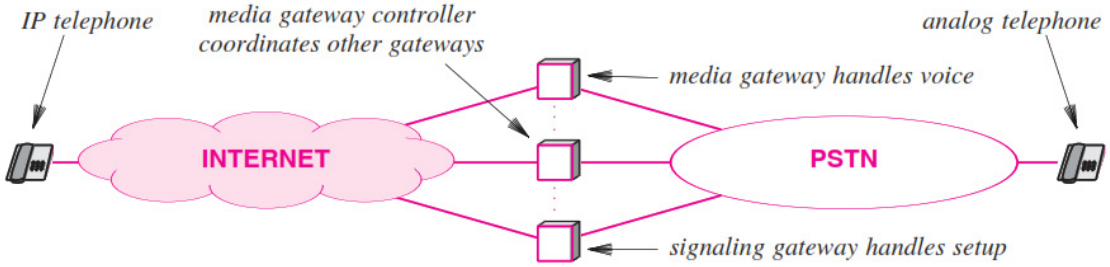
Telepon IP terhubung ke jaringan, menggunakan IP untuk semua komunikasi, dan menawarkan antarmuka telepon tradisional yang memungkinkan pengguna untuk melakukan atau menerima panggilan telepon. Telepon IP dapat berupa unit perangkat keras yang berdiri sendiri (yaitu telepon konvensional), atau dapat terdiri dari komputer dengan mikrofon, speaker, dan perangkat lunak telepon IP. Sambungan antara telepon IP dan seluruh dunia dapat terdiri dari jaringan kabel atau nirkabel (misalnya, Ethernet atau 802.11b).

Media Gateway Controller, yang juga dikenal sebagai Gatekeeper atau Softswitch, menyediakan kontrol dan koordinasi keseluruhan antara sepasang telepon IP, memungkinkan penelepon untuk menemukan callee atau mengakses layanan seperti penerusan panggilan.

Media Gateway menyediakan terjemahan audio saat panggilan melewati batas antara jaringan IP dan PSTN atau batas antara dua jaringan IP yang menggunakan penyandian berbeda. Misalnya, gateway media pada batas antara PSTN dan Internet memindahkan audio digital antara penyandian

TDM yang digunakan pada rangkaian suara konvensional dan penyandian paket yang digunakan di Internet.

Signaling Gateway juga mencakup batas antara sepasang jaringan yang berbeda, dan menyediakan terjemahan dari operasi signaling, memungkinkan kedua belah pihak untuk memulai panggilan (misalnya, untuk memungkinkan telepon IP di Internet untuk melakukan panggilan ke telepon di PSTN). Pengontrol gateway media mengoordinasikan pengoperasian media dan gateway pensinyalan. Gambar 10.5 mengilustrasikan bagaimana komponen digunakan untuk menghubungkan Internet dan PSTN.



Gambar 10.5 Koneksi antar komponen telepon IP.

Konsep dan terminologi yang didefinisikan di atas menyajikan pandangan telepon IP yang lugas dan agak disederhanakan yang berasal dari kerja di IETF dan ITU pada Megaco dan Media Gateway Control Protocol (MGCP). Implementasi praktis dari layanan telepon IP lebih kompleks. Bagian selanjutnya memberikan contoh.

10.7.1 Terminologi dan Konsep SIP

Session Initiation Protocol (SIP) meminimalkan kebutuhan akan protokol tambahan dengan menggunakan protokol yang ada bila memungkinkan. Misalnya, SIP menggunakan Sistem Nama Domain untuk memetakan nomor telepon ke alamat IP. Akibatnya, SIP mendefinisikan tiga elemen baru yang membentuk sistem sinyal:

- Agen pengguna
- Server Lokasi
- Server Dukungan (proxy, redirect, registrar)

- Agen pengguna. Dokumen SIP merujuk ke perangkat yang membuat atau mengakhiri panggilan telepon sebagai agen pengguna. Agen pengguna SIP dapat diimplementasikan di telepon IP, komputer laptop, atau gateway PSTN yang memungkinkan telepon IP melakukan panggilan ke PSTN. Agen pengguna terdiri dari dua bagian: Klien Agen Pengguna yang melakukan panggilan keluar, dan sebuah Server Agen Pengguna yang menangani panggilan masuk.
- Server Lokasi. Server lokasi SIP mengelola database informasi tentang setiap pengguna seperti sekumpulan alamat IP, layanan tempat pengguna berlangganan, dan preferensi pengguna. Server lokasi dihubungi selama pengaturan panggilan untuk mendapatkan informasi tentang lokasi atau lokasi yang akan menerima panggilan tertentu.

- Server proxy. SIP mencakup konsep proxy yang dapat meneruskan permintaan dari agen pengguna ke lokasi lain. Proxy menangani perutean yang optimal, dan menerapkan kebijakan (misalnya, memastikan bahwa pemanggil berwenang untuk melakukan panggilan).
- Alihkan Server. SIP menggunakan server pengalihan untuk menangani tugas-tugas seperti penerusan panggilan dan koneksi 800 nomor. Server pengalihan menerima permintaan dari agen pengguna, dan mengembalikan lokasi alternatif untuk dihubungi oleh agen pengguna.
- Server Pendaftar. SIP menggunakan server pencatat untuk menerima permintaan pendaftaran dan memperbarui database yang dikonsultasikan oleh server lokasi. Pencatat bertanggung jawab untuk mengautentikasi permintaan pendaftaran dan memastikan bahwa basis data yang mendasarinya tetap konsisten.

10.7.2 H.323 Terminologi dan Konsep

Standar H.323 dari ITU, yang mendefinisikan terminologi alternatif dan konsep tambahan, berfokus pada interaksi PSTN. Meskipun sangat luas dan mencakup banyak detail, H.323 dapat diringkas sebagai berikut:

- Terminal. Terminal H.323 menyediakan fungsi telepon IP, yang juga dapat mencakup fasilitas untuk transmisi video dan data.
- Penjaga gerbang. Penjaga gerbang H.323 menyediakan fungsi lokasi dan pensinyalan, dan mengoordinasikan pengoperasian gerbang yang menyediakan koneksi ke PSTN.
- Pintu gerbang. H.323 menggunakan satu gerbang untuk menghubungkan sistem telepon IP dengan PSTN; gateway menangani pensinyalan dan terjemahan media.
- Unit Kontrol Multipoint (MCU). MCU menyediakan layanan seperti konferensi multipoint.

10.7.3 Terminologi dan Konsep ISC

Karena ITU dan IETF melahirkan beberapa variasi terminologi dan konsep, vendor membentuk International Softswitch Consortium (ISC) untuk membuat model fungsional yang seragam dan komprehensif yang menggabungkan semua model telepon IP ke dalam satu kerangka kerja. Untuk melakukannya, ISC mendefinisikan fungsionalitas yang mungkin diperlukan, termasuk pensinyalan antara berbagai jenis sistem, terjemahan pengkodean, dukungan untuk layanan seperti penerusan panggilan, dan fungsi manajemen seperti akuntansi dan penagihan. ISC kemudian mendefinisikan daftar fungsi yang cukup untuk semua situasi:

- Fungsi Pengontrol Gateway Media (MGC-F). MGC-F menyimpan informasi status di titik akhir; menyediakan logika panggilan dan kontrol panggilan.
- Fungsi Agen Panggilan (CA-F). CA-F adalah subset dari MGC-F yang mempertahankan status panggilan. Contoh CA-F adalah SIP, H.323, dan Q.931.
- Fungsi Antar Kerja (IW-F). IW-F adalah subset dari MGC-F yang menangani pensinyalan antara jaringan heterogen seperti SS7 dan SIP.
- Fungsi Perutean dan Fungsi Akuntansi (R-F/A-F). R-F menangani perutean panggilan untuk MGC-F, dan A-F mengumpulkan informasi yang digunakan untuk akuntansi dan penagihan.
- Fungsi Gerbang Sinyal (SG-F). SG-F menangani pensinyalan antara IP jaringan dan PSTN.
- Access Gateway Signaling Function (AGS-F). AGS-F menangani pensinyalan antara jaringan IP dan jaringan akses circuit-switched seperti PSTN.
- Fungsi Server Aplikasi (AS-F). AS-F menangani serangkaian layanan aplikasi seperti pesan suara.

- Fungsi Kontrol Layanan (SC-F). SC-F dipanggil ketika AS-F harus mengontrol (mis., ubah) logika layanan (mis., instal pemetaan baru).
- Fungsi Gateway Media (MG-F). MG-F menangani terjemahan audio digital antara dua bentuk, dan mungkin juga mencakup deteksi peristiwa seperti apakah telepon dalam keadaan off-hook dan pengenalan sinyal Dual Tone Multi-Frequency (DTMF), standar pensinyalan audio yang dikenal sebagai Sentuh pengodean nada.
- Fungsi Server Media (MS-F). MS-F memanipulasi aliran paket media atas nama aplikasi AS-F.

10.8 Ringkasan Protokol dan Layering

Karena beberapa grup telah mengusulkan protokol untuk telepon IP, protokol yang bersaing ada di sebagian besar lapisan tumpukan protokol. Gambar 10.6 mencantumkan beberapa protokol yang diusulkan beserta posisinya dalam model referensi 5 lapis Internet.

<table>
<tr><th>Layer</th><th>Proses</th><th>Pengguna</th><th>Data Pengguna</th><th>Support</th><th>Rute</th><th>Signal Transport</th></tr>
<tr><td>5</td><td>H.323
Megaco
MGCP
SIP</td><td>RTP</td><td>T.120</td><td>RTCP
RTSP
NTP
SDP</td><td>ENUM
TRIP</td><td>SIGTRAN</td></tr>
<tr><td>4</td><td>TCP
UDP</td><td>UDP</td><td>TCP</td><td colspan="2">TCP
UDP</td><td>SCTP</td></tr>
<tr><td>3</td><td colspan="6">IP, RSVP, and IGMP</td></tr>
</table>

Gambar 10.6 Ringkasan protokol telepon IP.

10.9 H.323 Karakteristik

Alih-alih protokol tunggal, standar H.323, yang dibuat oleh ITU, terdiri dari seperangkat protokol yang bekerja sama untuk menangani semua aspek komunikasi telepon. Yang menarik dari H.323 adalah:

- Menangani semua aspek panggilan telepon digital
- Termasuk pensinyalan untuk mengatur dan mengelola panggilan
- Memungkinkan transmisi video dan data saat panggilan sedang berlangsung
- Mengirim pesan biner yang ditentukan oleh ASN.1 dan dikodekan menggunakan Basic Encoding Rules (BER)
- Menggabungkan protokol untuk keamanan
- Menggunakan unit perangkat keras khusus yang dikenal sebagai Unit Kontrol Multipoint
- untuk mendukung panggilan konferensi
- Mendefinisikan server untuk menangani tugas-tugas seperti resolusi alamat (yaitu, pemetaan nomor telepon pihak yang dipanggil ke dalam alamat IP), otentikasi, otorisasi (yaitu, menentukan apakah pengguna diizinkan untuk mengakses layanan yang diberikan), akuntansi, dan fitur, seperti penerusan panggilan.

10.10 H.323 Pelapisan

Protokol H.323 menggunakan TCP dan UDP untuk transportasi — audio dapat berjalan melalui UDP, sementara transfer data dilakukan melalui TCP. Gambar 10.7 mengilustrasikan layering dasar dalam standar H.323.

Layer	Signaling	Registration	Audio	Video	Data	Security
5	H.225.0-Q.931 H.250-Annex G H.245 H.250	H.225.9-RAS	G.711 H.263 G.722 G.723 G.728	H.261 H.323	T.120	H.235
4	TCP, UDP	UDP	RTP, RTCP		TCP	TCP, UDP
3	IP, RSVP, and IGMP					

Gambar 10.7 Pelapisan protokol utama dalam standar H.323.

10.11 Karakteristik dan Metode SIP

Sorotan Protokol Inisiasi Sesi (SIP) IETF adalah:

- Beroperasi pada lapisan aplikasi
- Mencakup semua aspek pensinyalan, termasuk lokasi pihak yang dipanggil, pemberitahuan dan pengaturan (yaitu, dering telepon), penentuan ketersediaan (yaitu, apakah pihak tersebut menerima panggilan), dan penghentian
- Menyediakan layanan seperti penerusan panggilan
- Mengandalkan multicast untuk panggilan konferensi
- Memungkinkan kedua belah pihak untuk menegosiasikan kemampuan dan memilih media dan parameter yang akan digunakan.

URI SIP berisi nama pengguna dan nama domain tempat pengguna dapat ditemukan. Misalnya, pengguna bernama Smith yang bekerja di Somecompany, Inc. mungkin diberi SIP URI:

sip:smith@somecompany.com

SIP mendefinisikan enam jenis pesan dasar dan tujuh ekstensi. Jenis pesan dasar dikenal sebagai metode. Gambar 10.8 mencantumkan metode SIP dasar.

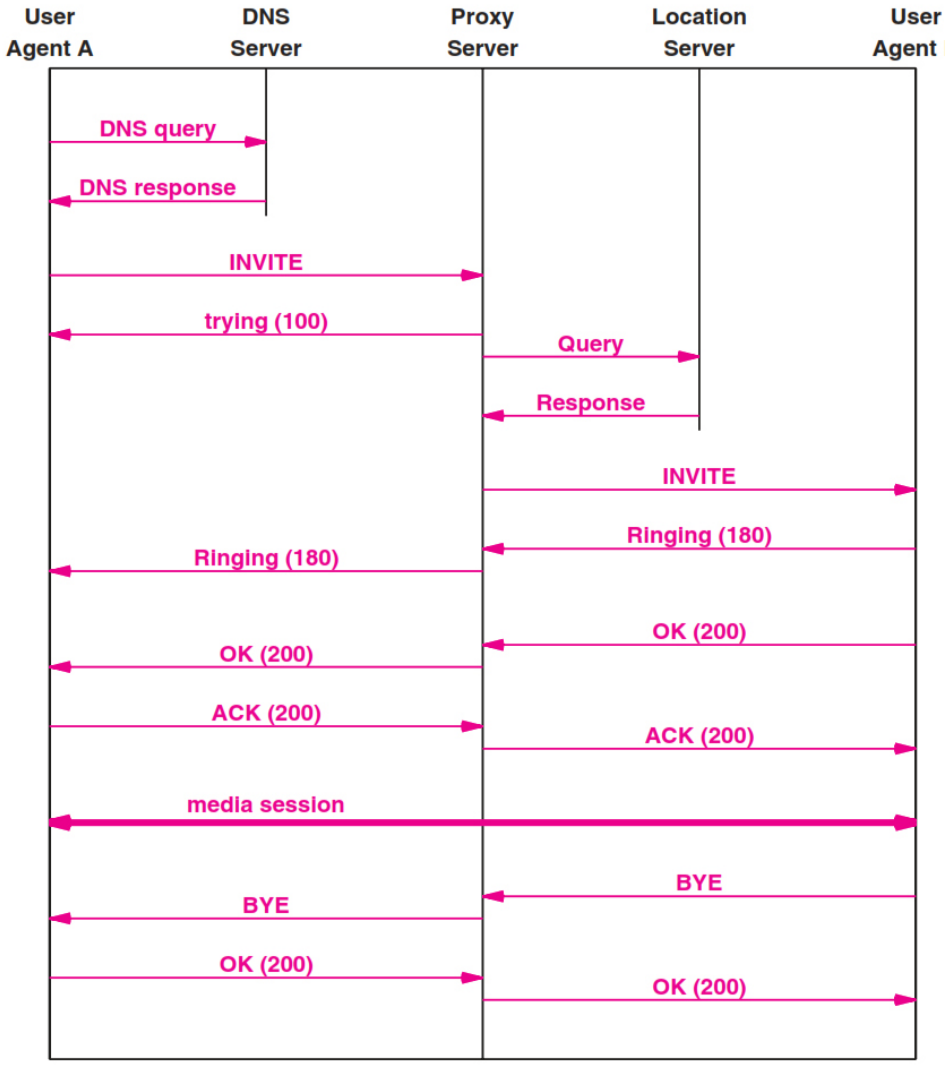
Metode	Keterangan
INVITE	Pembuatan sesi: titik akhir diundang untuk berpartisipasi dalam sesi
ACK	Tanggapan Pengakuan terhadap INVITE
BYE	Pemutusan sesi: panggilan berakhi
CANCEL	Pembatalan permintaan yang tertunda (tidak berpengaruh jika permintaan telah diselesaikan)

REGISTER	Pendaftaran lokasi pengguna (yaitu, URL tempat pengguna dapat dihubungi)
OPTIONS	Permintaan untuk menentukan kemampuan pihak yang dipanggil

Gambar 10.8 Enam metode dasar yang digunakan SIP.

10.12 Contoh Sesi SIP

Contoh pesan yang dikirim selama sesi SIP akan memperjelas beberapa detail dan membantu menjelaskan gagasan umum di balik sebagian besar telepon IP. Gambar 10.9 mencantumkan urutan pesan yang dikirim ketika agen pengguna, A, menghubungi server DNS, dan kemudian berkomunikasi dengan server proxy, yang memanggil server lokasi†. Setelah panggilan dibuat, kedua telepon IP berkomunikasi secara langsung. Akhirnya, SIP digunakan untuk mengakhiri panggilan.



Gambar 10.9 Contoh pesan yang dipertukarkan oleh SIP untuk mengatur panggilan telepon.

Biasanya, agen pengguna dikonfigurasi dengan alamat IP dari satu atau lebih server DNS (digunakan untuk memetakan nama domain dalam URI SIP ke alamat IP) dan satu atau lebih server

proxy. Demikian pula, setiap server proxy dikonfigurasi dengan alamat satu atau lebih server lokasi. Jadi, jika server tertentu tidak tersedia, SIP dapat menemukan alternatif dengan cepat.

10.13 Pemetaan dan Perutean Nomor Telepon

Bagaimana seharusnya pengguna telepon IP diberi nama dan lokasi? PSTN mengikuti standar ITU E.164 untuk nomor telepon, dan SIP menggunakan alamat IP. Masalah menemukan pengguna rumit karena beberapa jenis jaringan mungkin terlibat. Misalnya, pertimbangkan jaringan terintegrasi yang terdiri dari dua jaringan PSTN yang saling terhubung oleh jaringan IP. Desainer mendefinisikan dua sub masalah: menemukan pengguna di jaringan terintegrasi, dan menemukan rute yang efisien ke pengguna. IETF telah mengusulkan dua protokol yang sesuai dengan pemetaan yang diperlukan untuk dua sub masalah:

- ENUM — mengubah nomor telepon menjadi URI
- TRIP — menemukan pengguna dalam jaringan terintegrasi

ENUM. Protokol IETF ENUM (kependekan dari E.164 NUMbers) memecahkan masalah mengubah nomor telepon E.164 menjadi Uniform Resource Identifier (URI). Intinya, ENUM menggunakan Domain Name System untuk menyimpan pemetaan. Nomor telepon diubah menjadi nama domain khusus di domain:

e164.arpa

Konversi terdiri dari memperlakukan nomor telepon sebagai string, membalikkan string, dan menulis digit individu sebagai segmen nama domain. Misalnya, nomor telepon 1-800-555-1234 menghasilkan nama domain:

4.3.2.1.5.5.5.0.0.8.1.e164.arpa

Pemetaan ENUM dapat 1-ke-1 seperti skema penomoran telepon konvensional, atau dapat 1-ke-banyak, yang berarti telepon meja dan ponsel pengguna dapat diberi nomor telepon yang sama. Ketika nomor sesuai dengan beberapa host, server DNS mengembalikan daftar host bersama dengan protokol yang digunakan untuk mencapai masing-masing; Agen Pengguna melanjutkan untuk menghubungi host pada daftar sampai host merespons.

TRIP. Protokol IETF Telephone Routing over IP (TRIP) memecahkan masalah menemukan pengguna dalam jaringan terintegrasi. Server lokasi atau elemen jaringan lainnya dapat menggunakan TRIP untuk mengiklankan rute. Jadi, dua server lokasi menggunakan TRIP untuk menginformasikan satu sama lain tentang rute eksternal yang mereka ketahui masing-masing. Karena tidak bergantung pada protokol pensinyalan, TRIP dapat digunakan dengan SIP atau mekanisme pensinyalan lainnya.

TRIP membagi dunia menjadi satu set IP Telephone Administrative Domains (ITADs). Intinya, iklan TRIP mengidentifikasi titik jalan keluar — server lokasi menginformasikan server lokasi lain tentang jalur ke gateway pensinyalan yang terhubung ke ITAD lain. Karena telepon IP masih baru dan informasi perutean dapat berubah di masa mendatang, TRIP dirancang agar dapat diperluas.

10.14 Ringkasan

Protokol Transport Real-Time mengakomodasi transfer multimedia real-time melalui Internet. Pesan RTP menyertakan nomor urut dan stempel waktu terpisah serta identifikasi sumber data. Penerima menggunakan cap waktu untuk menempatkan data dalam buffer jitter sebelum pemutaran. RTP dienkapsulasi dalam UDP untuk transmisi, yang memungkinkan multicasting dan broadcasting. Tidak ada transmisi ulang yang digunakan karena paket yang diterima di luar jendela pemutaran tidak dapat diputar.

Istilah IP telephony dan VoIP mengacu pada panggilan telepon suara digital yang ditransmisikan melalui Internet. Salah satu tantangan terbesar dalam membangun sistem telepon IP muncul dari kompatibilitas ke belakang — gateway harus ditemukan yang menghubungkan sistem telepon IP ke PSTN tradisional. Gateway harus menyediakan terjemahan media (yaitu, terjemahan di antara pengkodean suara digital) dan pensinyalan (yaitu, terjemahan pengaturan panggilan).

ITU dan IETF masing-masing telah menciptakan standar untuk telepon IP. Standar ITU H.323 mencakup banyak protokol yang menyediakan pengaturan dan manajemen panggilan, otorisasi dan akuntansi, dan layanan pengguna seperti penerusan panggilan, serta transmisi suara, video, dan data melalui panggilan telepon. SIP standar IETF menyediakan kemampuan pensinyalan yang mencakup lokasi pengguna, pengaturan panggilan, dan memungkinkan setiap pihak untuk menentukan kemampuan. SIP menggunakan satu set server yang menangani berbagai aspek pensinyalan: Server Nama Domain, server proxy, dan server lokasi. Internet Softswitch Consortium (ISC) telah menetapkan kerangka kerja tambahan yang dimaksudkan untuk mencakup semua model telepon IP.

Dua protokol IETF tambahan menyediakan fungsi dukungan. ENUM menggunakan Sistem Nama Domain untuk memetakan nomor telepon E.164 ke dalam Uniform Resource Identifier (biasanya SIP URI). TRIP menyediakan perutean di antara domain administratif telepon IP; server lokasi SIP dapat menggunakan TRIP untuk menginformasikan server lokasi lain tentang gateway yang membentuk titik keluar jaringan.

Latihan

1. Mendefinisikan data multimedia. Apa dua teknik yang digunakan untuk mengatasi jitter?
2. Jelaskan bagaimana buffer jitter memungkinkan pemutaran aliran audio bahkan jika Internet memperkenalkan jitter.
3. Jika pesan RTP dicegat saat melintasi Internet, dapatkah bidang stempel waktu ditafsirkan? Jika demikian, bagaimana? Jika tidak, mengapa tidak?
4. Karena berjalan dalam UDP, pesan RTP dapat diduplikasi. Apakah penerima perlu menyimpan salinan semua pesan yang diterima sebelumnya untuk menentukan apakah pesan masuk adalah duplikat? Mengapa atau mengapa tidak?
5. RTP berisi protokol pendamping yang dikenal sebagai Real-Time Control Protocol (RTCP) yang memungkinkan penerima melaporkan kualitas pesan yang diterima ke pengirim. Bagaimana pengkodean video adaptif menggunakan status pesan yang diterima?

6. Jika suara diubah ke bentuk digital menggunakan PCM, berapa bit data yang akan dihasilkan dalam satu setengah detik?
7. Perpanjang latihan sebelumnya. Perkirakan ukuran (dalam oktet) dari datagram IP yang membawa seperempat detik audio yang dikodekan dalam PCM, ditempatkan dalam paket RTP, dan dienkapsulasi dalam UDP. Petunjuk: RFC 1889 mendefinisikan ukuran header RTP.
8. Aspek telepon IP mana yang ditangani oleh H.323?
9. Ketika H.323 digunakan untuk mengirim data bersama dengan audio atau video, protokol transport mana yang digunakan?
10. Apa enam metode dasar yang digunakan dengan SIP?
11. Baca RFC tentang SIP, dan ubah Gambar 10.9 untuk menunjukkan pesan yang dipertukarkan saat penerusan panggilan terjadi. Petunjuk: lihat pesan pengalihan SIP.
12. Apa tujuan dari protokol ENUM dan TRIP?
13. Pertimbangkan pengoperasian telepon IP dan telepon analog. Mana yang lebih baik selama masa perang? Mengapa?
14. Cari domain e164.arpa. Organisasi mana yang bertanggung jawab atas domain tersebut?

Bab 11 Keamanan Jaringan

Bab ini akan membahas tentang:

- Aspek penting dari keamanan jaringan
- Jenis kejahatan yang telah dilakukan melalui Internet
- Aspek-aspek kunci keamanan, dan menjelaskan teknologi yang digunakan untuk meningkatkan keamanan jaringan

11.1 Eksploitasi dan Serangan Kriminal

Setiap kali teknologi baru muncul, penjahat bertanya bagaimana mereka bisa menggunakan teknologi itu untuk melakukan kejahatan. Internet tidak terkecuali — seperti yang diketahui sebagian besar pengguna, Internet telah digunakan untuk kegiatan kriminal seperti yang dilaporkan di media. Meskipun kejahatan Internet, seperti penipuan dan pencurian identitas, dapat mempengaruhi individu, kejahatan yang paling signifikan menimbulkan ancaman bagi bisnis. Selain pencurian barang atau jasa secara langsung, bisnis sangat memperhatikan ancaman terhadap kelangsungan hidup perusahaan dalam jangka panjang. Dengan demikian, kerusakan reputasi, hilangnya kepercayaan pelanggan, kekayaan intelektual yang dicuri, dan pencegahan akses pelanggan semuanya penting bagi bisnis.

Beberapa pertanyaan muncul mengenai keamanan:

- Apa masalah dan ancaman keamanan Internet utama?
- Aspek teknis protokol apa yang dieksploitasi oleh penjahat?
- Apa saja aspek kunci dari keamanan?
- Teknologi apa yang tersedia untuk membantu meningkatkan keamanan?

Beberapa masalah keamanan utama yang ada di Internet antara lain :

Phishing

Phising adalah upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang menjadi sasaran phising adalah data pribadi (nama, usia, alamat), data akun (username dan password), dan data finansial (informasi kartu kredit, rekening).

Misrepresentation

Membuat klaim palsu atau berlebihan tentang barang atau jasa, atau mengirimkan produk palsu atau inferior

Scams

Berbagai bentuk tipu daya yang dimaksudkan untuk menipu pengguna yang naif agar menginvestasikan uang atau bersekongkol dengan kejahatan

Denial of Service

Dengan sengaja memblokir situs Internet tertentu untuk mencegah atau menghalangi kegiatan bisnis dan perdagangan

Loss of Control

Seorang penyusup memperoleh kendali atas sistem komputer dan menggunakan sistem tersebut untuk melakukan kejahatan

Loss of Data

Kehilangan kekayaan intelektual atau informasi bisnis kepemilikan lainnya yang berharga

Saat mempertimbangkan keamanan, penting untuk membedakan antara kejahatan konvensional yang dilakukan dengan menggunakan Internet secara insidental dan kejahatan yang khusus untuk Internet. Misalnya, pertimbangkan kejahatan di mana penjahat menggunakan telepon VoIP untuk berkomunikasi dengan rekan konspirator, penipuan di mana penjahat dengan sengaja menipu dan menipu korban yang tidak menaruh curiga, atau insiden di mana penjahat menggunakan Internet untuk memesan alat yang digunakan untuk melakukan kejahatan. Meskipun lembaga penegak hukum harus menangani masing-masing, kasus seperti itu tidak ada hubungannya dengan teknologi jaringan — orang dapat dengan mudah menemukan mekanisme komunikasi alternatif yang dapat digunakan sebagai pengganti Internet. Dua dari kejahatan paling luas yang dialami di Internet adalah kejahatan konvensional yang terjadi saat menggunakan Internet: kesalahan penyajian barang yang ditawarkan dalam lelang adalah bentuk iklan palsu, dan kegagalan mengirimkan barang yang dibeli melalui lelang dianalogikan dengan pesanan pos konvensional. tipuan.

Diskusi kita akan fokus pada cara penjahat mengeksploitasi teknologi dan teknologi yang telah diciptakan untuk membuat kejahatan menjadi lebih sulit atau mahal. Beberapa teknik khusus yang digunakan penyerang, antara lain :

Wiretapping

Membuat salinan paket saat melintasi jaringan untuk mendapatkan informasi

Replay

Mengirim paket yang diambil dari sesi sebelumnya (mis., Paket kata sandi dari login sebelumnya)

Buffer overflow

Mengirim lebih banyak data daripada yang diharapkan penerima untuk menyimpan nilai dalam variabel di luar buffer

Address Spoofing

Memalsukan alamat sumber IP dalam sebuah paket untuk mengelabui penerima agar memproses paket

Name Spoofing

Menggunakan salah ejaan nama terkenal atau meracuni server nama dengan pengikatan yang salah

DoS and DDoS

Membanjiri situs dengan paket untuk mencegah situs tersebut berhasil menjalankan bisnis normal

SYN flood

Mengirim aliran segmen TCP SYN acak untuk menguras rangkaian koneksi TCP penerima

Key Breaking

Secara otomatis menebak kunci dekripsi atau kata sandi untuk mendapatkan akses tidak sah ke data

Port Scanning

Mencoba terhubung ke setiap port protokol yang mungkin pada host untuk menemukan kerentanan

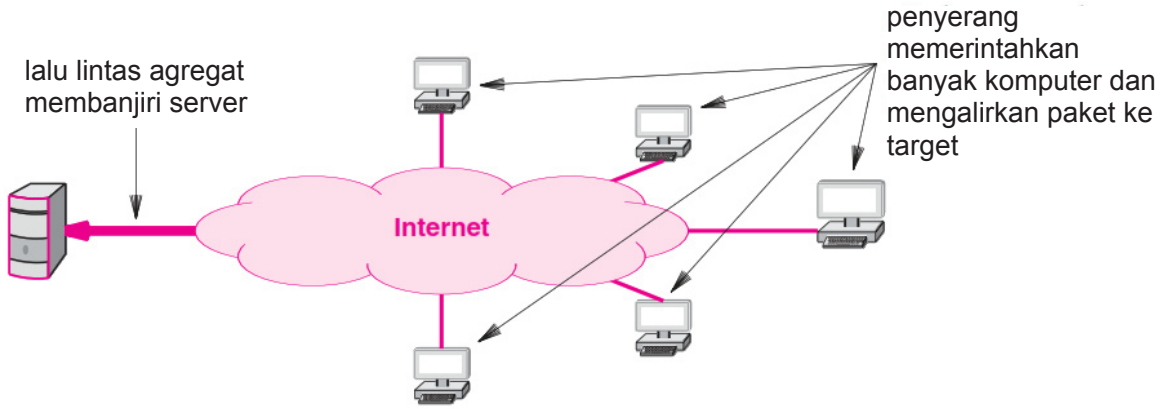
Packet interception

Menghapus paket dari Internet yang memungkinkan substitusi dan serangan man-in-the middle

Penyadapan dan teknik replay terkait sudah jelas. Menariknya, buffer overflow adalah salah satu kelemahan sistem komputer yang paling banyak dimanfaatkan. Ini adalah gejala rekayasa yang buruk: seorang programmer gagal untuk memeriksa ukuran buffer saat melakukan operasi input. Serangan tipikal mengirim paket jumbo (lebih besar dari izin standar) atau mengirim urutan paket back-to-back yang meluap buffer input.

Serangan spoofing digunakan untuk menyamar sebagai host tepercaya. Bentuk paling sederhana dari alamat spoofing menggunakan ARP: penyerang menyiarkan balasan ARP yang mengikat alamat IP arbitrer, A, ke alamat MAC penyerang. Ketika setiap host di jaringan mengirimkan paket ke A, paket tersebut akan diteruskan ke penyerang. Bentuk spoofing lain melibatkan penggunaan protokol perutean untuk mengirim rute yang salah, mengirim pesan DNS yang menyimpan pengikatan yang salah di server DNS, dan menggunakan sedikit kesalahan ejaan nama domain terkenal untuk memberi kesan kepada pengguna bahwa mereka telah mencapai situs web terpercaya.

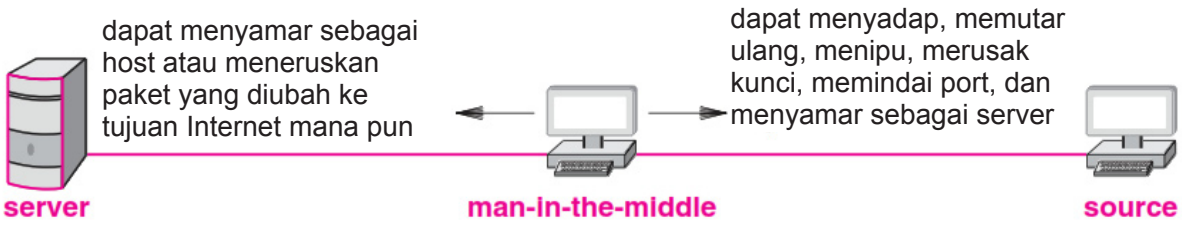
Serangan Denial of Service (DoS) membanjiri host (biasanya server web) dengan aliran paket. Meskipun server terus beroperasi, serangan itu secara efektif menghabiskan semua sumber daya, yang berarti bahwa pengguna lain mengalami penundaan yang lama atau koneksi mereka ditolak. Karena seorang manajer dapat melihat dan menonaktifkan aliran paket dari satu sumber, serangan Distributed Denial of Service (DDoS) mengatur sejumlah besar host di seluruh Internet untuk masing-masing mengirim aliran paket, seperti yang diilustrasikan Gambar 11.3. Biasanya, penyerang pertama-tama memerintahkan host di Internet, memuat perangkat lunak ke host, dan kemudian menggunakan host untuk menyerang server. Dengan demikian, tidak ada paket yang dikirim oleh DDoS yang datang langsung dari komputer penyerang.



Gambar 11.3 Ilustrasi serangan Distributed Denial of Service.

SYN flooding adalah teknik khusus yang digunakan untuk menolak layanan ke TCP — setiap paket yang masuk berisi pesan TCP SYN yang meminta koneksi TCP baru. Penerima mengalokasikan blok kontrol TCP untuk koneksi, mengirim SYN + ACK, dan menunggu respons. Akhirnya, semua blok kontrol dialokasikan, dan tidak ada koneksi lebih lanjut yang dapat dibuka.

Intersepsi Paket memungkinkan untuk meluncurkan serangan man-in-the-middle di mana perantara dapat memodifikasi paket saat mereka melewati dari sumber ke tujuan. Meskipun merupakan salah satu serangan yang paling sulit untuk direkayasa, intersepsi paket memiliki potensi kerusakan terbesar, seperti yang diilustrasikan pada Gambar 11.4.



Gambar 11.4 Konfigurasi man-in-the middle dan serangan yang diizinkan

11.2 Kebijakan Keamanan

Apa itu jaringan aman? Meskipun konsep jaringan aman menarik bagi sebagian besar pengguna, jaringan tidak dapat diklasifikasikan hanya sebagai aman atau tidak aman karena istilah tersebut tidak mutlak — setiap organisasi menentukan tingkat akses yang diizinkan atau ditolak. Misalnya, organisasi yang menyimpan rahasia dagang yang berharga mungkin perlu mencegah orang luar mengakses komputer organisasi. Sebuah organisasi yang memiliki situs web yang menyediakan informasi dapat mendefinisikan jaringan aman sebagai jaringan yang memungkinkan akses sewenang-wenang ke data, tetapi mencakup mekanisme yang mencegah orang luar mengubah data. Organisasi lain fokus pada menjaga kerahasiaan komunikasi: mereka mendefinisikan jaringan aman sebagai jaringan di mana tidak ada orang lain selain pengirim atau penerima yang dituju yang dapat mencegat dan membaca pesan. Akhirnya, sebuah organisasi besar mungkin memerlukan definisi keamanan yang kompleks yang memungkinkan akses ke data atau layanan yang dipilih dan mencegah akses atau modifikasi data dan layanan yang sensitif atau rahasia.

Karena tidak ada definisi mutlak dari jaringan aman, langkah pertama yang harus diambil organisasi untuk mencapai sistem yang aman adalah menentukan kebijakan keamanan organisasi. Kebijakan tidak menentukan bagaimana mencapai perlindungan. Sebaliknya, ia menyatakan dengan jelas dan jelas barang-barang yang harus dilindungi.

Kebijakan keamanan rumit karena melibatkan perilaku manusia serta fasilitas komputer dan jaringan (misalnya, pengunjung yang membawa Flash ROM keluar dari organisasi, jaringan nirkabel yang dapat dideteksi di luar gedung, atau karyawan yang bekerja di rumah). Menilai biaya dan manfaat dari berbagai kebijakan keamanan juga menambah kompleksitas. Secara khusus, kebijakan keamanan tidak dapat didefinisikan kecuali organisasi memahami nilai informasinya. Dalam banyak kasus, nilai informasi sulit untuk dinilai. Pertimbangkan, misalnya, database penggajian sederhana yang berisi catatan untuk setiap karyawan, jam kerja karyawan, dan tingkat pembayaran. Jika mereka dapat mengakses informasi tersebut, beberapa karyawan mungkin menjadi marah dan menuntut upah yang lebih tinggi atau mengancam untuk pergi. Jika pesaing memperoleh informasi tersebut, mereka mungkin menggunakannya untuk memikat karyawan. Lebih penting lagi, pesaing mungkin dapat menggunakan informasi dengan cara yang tidak terduga (misalnya, untuk menilai upaya yang dihabiskan untuk proyek tertentu).

Poin Penting

Merancang kebijakan keamanan jaringan dapat menjadi kompleks karena kebijakan rasional memerlukan organisasi untuk menghubungkan keamanan jaringan dan komputer dengan perilaku manusia dan untuk menilai nilai informasi.

Mendefinisikan kebijakan keamanan juga rumit karena setiap organisasi harus memutuskan aspek perlindungan mana yang paling penting, dan seringkali harus berkompromi antara keamanan dan kemudahan penggunaan. Misalnya, sebuah organisasi dapat mempertimbangkan:

- Integritas data. Integritas mengacu pada perlindungan dari perubahan: apakah data yang tiba di penerima identik dengan data yang dikirim?
- Ketersediaan Data. Ketersediaan mengacu pada perlindungan terhadap gangguan layanan: apakah data tetap dapat diakses untuk penggunaan yang sah?
- Kerahasiaan Data. Kerahasiaan mengacu pada perlindungan terhadap akses data yang tidak sah (misalnya, melalui pengintaian atau penyadapan): apakah data dilindungi dari akses yang tidak sah?
- Privacy. Privasi mengacu pada kemampuan pengirim untuk tetap anonim: apakah identitas pengirim terungkap?

11.3 Tanggung Jawab dan Kontrol

Selain item di atas, organisasi harus menentukan dengan tepat bagaimana tanggung jawab atas informasi ditugaskan atau dikendalikan. Masalah tanggung jawab atas informasi memiliki dua aspek:

- Akuntabilitas. Akuntabilitas mengacu pada bagaimana jejak audit disimpan: kelompok mana yang bertanggung jawab untuk setiap item data? Bagaimana grup menyimpan catatan akses dan perubahan?

- Otorisasi. Otorisasi mengacu pada tanggung jawab untuk setiap item informasi dan bagaimana tanggung jawab tersebut didelegasikan kepada orang lain: siapa yang bertanggung jawab atas tempat informasi berada, dan bagaimana orang yang bertanggung jawab menyetujui akses dan perubahan?

Isu kritis yang mendasari akuntabilitas dan otorisasi adalah kontrol — organisasi harus mengontrol akses ke informasi yang serupa dengan cara organisasi mengontrol akses ke sumber daya fisik seperti kantor, peralatan, dan persediaan. Aspek kunci dari kontrol menyangkut otentikasi, yang mengacu pada validasi identitas. Sebagai contoh, anggaplah sebuah organisasi menetapkan kebijakan otorisasi yang memberikan hak istimewa lebih kepada karyawan daripada pengunjung. Kebijakan otorisasi tidak ada artinya kecuali organisasi memiliki mekanisme otentikasi yang membedakan antara pengunjung dan karyawan. Otentikasi melampaui manusia untuk memasukkan komputer, perangkat, dan program aplikasi.

Poin Penting

Kebijakan otorisasi tidak ada artinya tanpa mekanisme otentikasi yang dapat dengan jelas memverifikasi identitas pemohon.

11.4 Teknologi Keamanan

Ada banyak produk keamanan yang melakukan berbagai fungsi baik untuk komputer individu maupun sekumpulan komputer dalam suatu organisasi. Gambar 11.5 merangkum teknik yang digunakan produk tersebut. Bagian selanjutnya menjelaskan masing-masing teknologi.

Teknik	Tujuan
Hashing	Integritas data
Encryption	Pribadi
Digital Signatures	Otentikasi pesan
Digital Certificates	Otentikasi pengirim
Firewalls	Integritas situs
Intrusion Detection Systems	Integritas situs
Deep Packet Inspection & Content Scanning	Integritas situs
Virtual Private Networks (VPNs)	Privasi data

Gambar 11.5 Teknik utama yang digunakan untuk menegakkan kebijakan keamanan.

11.5 Hashing: Mekanisme Integritas dan Otentikasi

Bab-bab sebelumnya membahas teknik seperti bit paritas, checksum, dan cyclic redundancy check (CRC) yang digunakan untuk melindungi data dari kerusakan yang tidak disengaja. Teknik tersebut tidak memberikan integritas data karena dua alasan. Pertama, malfungsi dapat mengubah checksum serta nilai data, yang berarti checksum yang diubah mungkin valid untuk data yang diubah. Kedua, jika perubahan data dihasilkan dari serangan yang direncanakan, penyerang dapat membuat checksum yang valid untuk data yang diubah. Oleh karena itu, mekanisme tambahan telah dibuat untuk menjamin integritas pesan terhadap perubahan yang disengaja.

Salah satu metode menyediakan kode otentikasi pesan (MAC) yang tidak dapat dihancurkan atau dipalsukan oleh penyerang. Skema pengkodean tipikal menggunakan mekanisme hashing kriptografi. Satu skema hashing bergantung pada kunci rahasia yang hanya diketahui oleh pengirim dan penerima. Pengirim mengambil pesan sebagai input, menggunakan kunci untuk menghitung hash, H, dan mengirimkan H bersama dengan pesan. H adalah string bit pendek, dan panjang H tidak tergantung pada ukuran pesan. Penerima menggunakan kunci untuk menghitung hash pesan, dan membandingkan hash dengan H. Jika keduanya setuju, pesan telah tiba dengan utuh. Penyerang, yang tidak memiliki kunci rahasia, tidak akan dapat mengubah pesan tanpa menimbulkan kesalahan. Jadi, H menyediakan otentikasi pesan karena penerima tahu bahwa pesan yang datang dengan hash yang valid adalah otentik.

11.6 Kontrol Akses dan Kata Sandi

Mekanisme kontrol akses mengontrol pengguna atau program aplikasi mana yang dapat mengakses data. Misalnya, beberapa sistem operasi menerapkan daftar kontrol akses (ACL) untuk setiap objek yang menentukan siapa yang diizinkan untuk mengakses objek. Di sistem lain, setiap pengguna diberi kata sandi untuk setiap sumber daya yang dilindungi. Ketika pengguna perlu mengakses sumber daya yang dilindungi, pengguna diminta untuk memasukkan kata sandi.

Saat memperluas daftar kontrol akses dan kata sandi di seluruh jaringan, langkah-langkah harus diambil untuk mencegah pengungkapan yang tidak disengaja. Misalnya, jika pengguna di satu lokasi mengirim kata sandi tidak terenkripsi melalui jaringan ke komputer di lokasi lain, siapa pun yang menyadap jaringan dapat memperoleh salinan kata sandi. Penyadapan sangat mudah ketika paket berjalan melintasi LAN nirkabel karena koneksi fisik tidak diperlukan - siapa pun dalam jangkauan transmisi dapat menangkap salinan setiap paket. Selain itu, langkah-langkah harus diambil untuk memastikan bahwa kata sandi tidak mudah ditebak karena jaringan memungkinkan penyerang untuk mengotomatiskan upaya untuk memecahkan kata sandi. Dengan demikian, manajer menerapkan aturan untuk memilih kata sandi seperti panjang minimum dan larangan menggunakan kata-kata umum (yaitu, kata-kata yang ditemukan dalam kamus).

11.7 Enkripsi: Teknik Keamanan Mendasar

Kriptografi merupakan alat yang fundamental dalam keamanan karena enkripsi dapat menjamin kerahasiaan data (kadang disebut privasi), keaslian pesan, integritas data, dan dapat mencegah serangan replay. Intinya, pengirim menerapkan enkripsi untuk mengacak bit pesan sedemikian rupa sehingga hanya penerima yang dituju yang dapat menguraikannya. Seseorang yang mencegat salinan pesan terenkripsi tidak akan dapat mengekstrak informasi. Selanjutnya, pesan terenkripsi dapat mencakup informasi seperti panjang pesan; penyerang tidak dapat memotong pesan tanpa ditemukan.
Terminologi yang digunakan dengan enkripsi mendefinisikan empat item:

- Plaintext — pesan asli sebelum dienkripsi
- Cyphertext — pesan setelah dienkripsi
- Kunci enkripsi — string bit pendek yang digunakan untuk mengenkripsi pesan
- Kunci dekripsi — string bit pendek yang digunakan untuk mendekripsi pesan

Seperti yang akan kita lihat, dalam beberapa teknologi, kunci enkripsi dan kunci dekripsi adalah identik; pada orang lain, mereka berbeda.

Secara matematis, kami menganggap enkripsi sebagai fungsi, enkripsi, yang membutuhkan dua argumen: kunci, K1, dan pesan teks biasa untuk dienkripsi, M. Fungsi menghasilkan versi pesan terenkripsi, teks sandi C:

C = enkripsi (K1 , M)

Fungsi dekripsi membalikkan pemetaan untuk menghasilkan pesan asli†:

M = mendekripsi (K2 , C)

Secara matematis, dekripsi adalah kebalikan dari enkripsi:

M = mendekripsi (K2 , mengenkripsi (K1 , M))

11.8 Enkripsi Kunci Pribadi

Banyak teknologi enkripsi yang ada, dan mereka dapat dibagi menjadi dua kategori besar yang ditentukan oleh cara mereka menggunakan kunci:

- Kunci Pribadi
- Kunci Publik

Dalam sistem kunci pribadi, setiap pasangan entitas yang berkomunikasi berbagi satu kunci yang berfungsi sebagai kunci enkripsi dan kunci dekripsi. Nama tersebut muncul karena kunci harus dirahasiakan — jika pihak ketiga memperoleh salinan kunci, pihak ketiga akan dapat mendekripsi pesan yang lewat di antara pasangan tersebut. Sistem kunci privat bersifat simetris dalam arti masing-masing pihak dapat mengirim atau menerima pesan. Untuk mengirim pesan, kunci digunakan untuk menghasilkan cyphertext, yang kemudian dikirim melalui jaringan. Ketika sebuah pesan tiba, pihak penerima menggunakan kunci rahasia untuk memecahkan kode cyphertext dan mengekstrak pesan asli (plaintext). Jadi, dalam sistem kunci privat, pengirim dan penerima masing-masing menggunakan kunci yang sama, K, yang artinya:

M = mendekripsi (K , mengenkripsi (K , M))

11.9 Enkripsi Kunci Publik

Alternatif utama untuk enkripsi kunci pribadi dikenal sebagai enkripsi kunci publik. Sistem kunci publik memberikan setiap entitas sepasang kunci. Untuk tujuan diskusi, kami akan mengasumsikan bahwa setiap entitas adalah pengguna tunggal. Salah satu kunci pengguna, yang disebut kunci pribadi, dirahasiakan, sementara yang lain, yang disebut kunci publik, diterbitkan bersama dengan nama pengguna, sehingga semua orang tahu nilai kuncinya. Fungsi enkripsi memiliki properti matematika bahwa pesan teks biasa yang dienkripsi dengan kunci publik tidak dapat didekripsi kecuali dengan kunci pribadi, dan pesan teks biasa yang dienkripsi dengan kunci pribadi tidak dapat didekripsi kecuali dengan kunci publik.

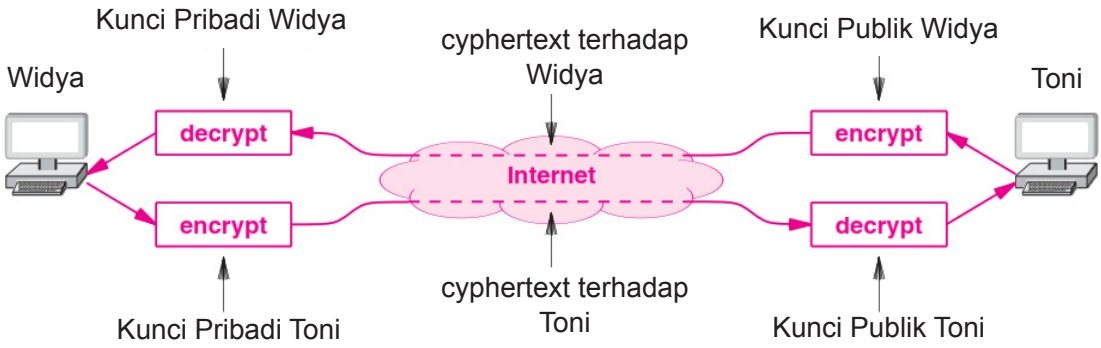
Hubungan antara enkripsi dan dekripsi dengan kedua kunci tersebut dapat dinyatakan secara matematis. Biarkan M menunjukkan pesan teks biasa, public_u1 menunjukkan kunci publik pengguna 1, dan private_u1 menunjukkan kunci pribadi pengguna 1. Fungsi enkripsi dapat dinyatakan sebagai:

M = dekripsi (public_u1 , enkripsi (private_u1, M))

dan

M = dekripsi (private_u1 , enkripsi (public_u1, M))

Gambar 11.6 mengilustrasikan mengapa sistem kunci publik diklasifikasikan sebagai asimetris dengan menunjukkan kunci yang digunakan untuk mengenkripsi pesan yang dikirim ke setiap arah.



Gambar 11.6 Ilustrasi asimetri dalam sistem enkripsi kunci publik.

Mengungkap kunci publik aman karena fungsi yang digunakan untuk enkripsi dan dekripsi memiliki properti satu arah. Artinya, memberi tahu seseorang kunci publik tidak memungkinkan orang tersebut memalsukan pesan yang dienkripsi dengan kunci privat.

Enkripsi kunci publik dapat digunakan untuk menjamin kerahasiaan. Pengirim yang menginginkan komunikasi tetap rahasia menggunakan kunci publik penerima untuk mengenkripsi pesan. Mendapatkan salinan cyphertext saat melewati jaringan tidak memungkinkan seseorang untuk membaca konten karena dekripsi memerlukan kunci pribadi penerima. Dengan demikian, skema memastikan bahwa data tetap rahasia karena hanya penerima yang dapat mendekripsi pesan.

11.10 Otentikasi dengan Tanda Tangan Digital

Mekanisme enkripsi juga dapat digunakan untuk mengotentikasi pengirim pesan. Teknik ini dikenal sebagai tanda tangan digital. Untuk menandatangani pesan, pengirim mengenkripsi pesan menggunakan kunci yang hanya diketahui oleh pengirim†. Penerima menggunakan fungsi kebalikan untuk mendekripsi pesan. Penerima tahu siapa yang mengirim pesan karena hanya pengirim yang memiliki kunci yang diperlukan untuk melakukan enkripsi. Untuk memastikan bahwa pesan terenkripsi tidak disalin dan dikirim ulang nanti, pesan asli dapat berisi waktu dan tanggal pesan dibuat.

Pertimbangkan bagaimana sistem kunci publik dapat digunakan untuk menyediakan tanda tangan digital. Untuk menandatangani pesan, pengirim mengenkripsi pesan menggunakan kunci pribadinya. Untuk memverifikasi tanda tangan, penerima mencari kunci publik pengirim dan menggunakannya untuk mendekripsi pesan. Karena hanya pengirim yang mengetahui kunci privat, hanya pengirim yang dapat mengenkripsi pesan yang dapat didekodekan dengan kunci publik.

Menariknya, sebuah pesan dapat dienkripsi dua kali untuk menjamin otentikasi dan kerahasiaan. Pertama, pesan ditandatangani dengan menggunakan kunci pribadi pengirim untuk mengenkripsinya. Kedua, pesan terenkripsi dienkripsi lagi menggunakan kunci publik penerima. Secara matematis, kedua langkah enkripsi tersebut dapat dinyatakan sebagai:

X = enkripsi (public_u2 , enkripsi (private_u1, M))

di mana M menunjukkan pesan teks biasa yang akan dikirim, X menunjukkan string teks sandi yang dihasilkan dari enkripsi ganda, private_u1 menunjukkan kunci pribadi pengirim, dan public_u2 menunjukkan kunci publik penerima.

Di sisi penerima, proses dekripsi adalah kebalikan dari proses enkripsi. Pertama, penerima menggunakan kunci pribadi mereka untuk mendekripsi pesan. Dekripsi menghapus satu tingkat enkripsi, tetapi membiarkan pesan ditandatangani secara digital. Kedua, penerima menggunakan kunci publik pengirim untuk mendekripsi pesan lagi. Proses tersebut dapat dinyatakan sebagai:

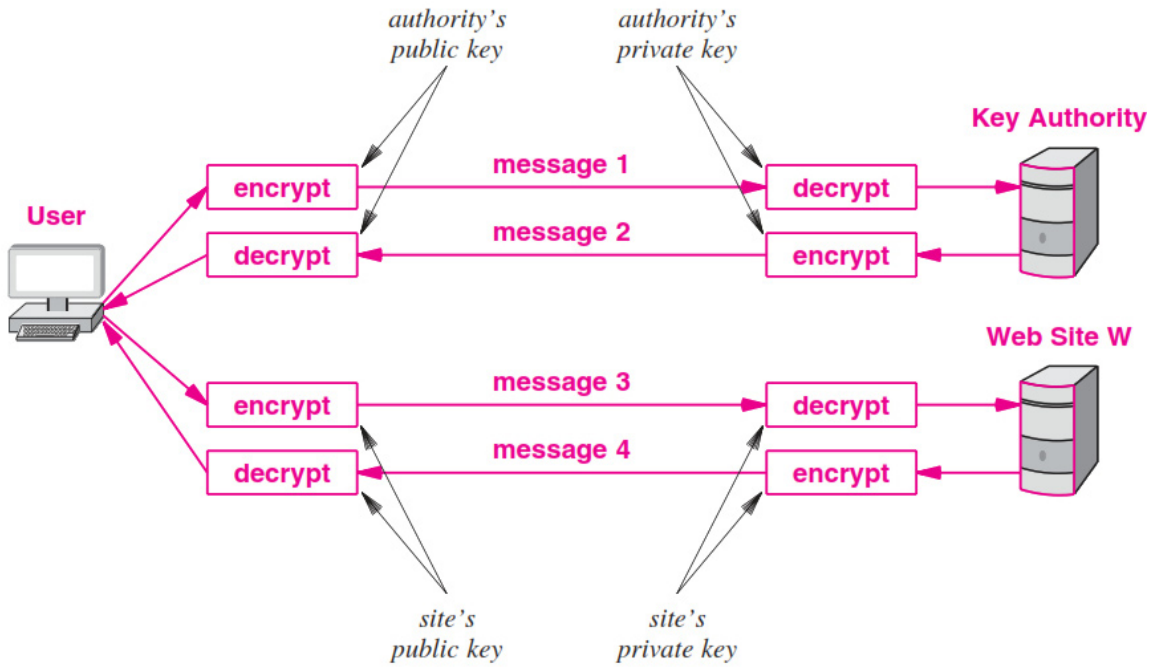
M = dekripsi (public_u1 , dekripsi (private_u2 , X))

di mana X menunjukkan cyphertext yang ditransfer melalui jaringan, M menunjukkan pesan plaintext asli, private_u2 menunjukkan kunci pribadi penerima, dan public_u1 menunjukkan kunci publik pengirim. Jika pesan yang bermakna dihasilkan dari kedua langkah tersebut, maka harus benar bahwa pesan tersebut bersifat rahasia dan autentik. Pesan harus telah mencapai penerima yang dituju karena hanya penerima yang dituju yang memiliki kunci pribadi yang benar yang diperlukan untuk menghapus enkripsi luar. Pesan harus asli karena hanya pengirim yang memiliki kunci pribadi yang diperlukan untuk mengenkripsi pesan sehingga kunci publik pengirim akan mendekripsinya dengan benar.

11.11 Otoritas Utama dan Sertifikat Digital

Salah satu pertanyaan mendasar seputar teknologi kunci publik muncul dari cara di mana kunci publik diperoleh. Meskipun dimungkinkan untuk menggunakan publikasi konvensional (analog dengan buku telepon), melakukannya tidak praktis dan rentan terhadap kesalahan karena manusia perlu memasukkan kunci ke komputer mereka secara manual. Timbul pertanyaan: dapatkah sistem otomatis dirancang untuk mendistribusikan kunci publik? Tentu saja, sistem distribusi harus aman — jika kunci publik yang diberikan kepada pengguna salah, keamanan rusak, dan enkripsi lebih lanjut tidak dapat dipercaya. Masalahnya dikenal sebagai masalah distribusi kunci, dan pembentukan sistem distribusi kunci yang layak telah menjadi hambatan untuk adopsi sistem kunci publik secara luas.

Beberapa mekanisme distribusi kunci telah diusulkan, termasuk yang menggunakan Sistem Nama Domain. Dalam setiap kasus, prinsip sederhana mendasari skema: dengan mengetahui satu kunci — kunci publik dari otoritas kunci — adalah mungkin untuk mendapatkan kunci publik lainnya dengan cara yang aman. Dengan demikian, seorang administrator hanya perlu mengkonfigurasi satu kunci publik. Gambar 11.7 mengilustrasikan pertukaran pesan ketika pengguna memutuskan untuk berinteraksi dengan situs web baru, W.



Gambar 11.7 Ilustrasi penggunaan otoritas kunci untuk mendapatkan kunci publik.

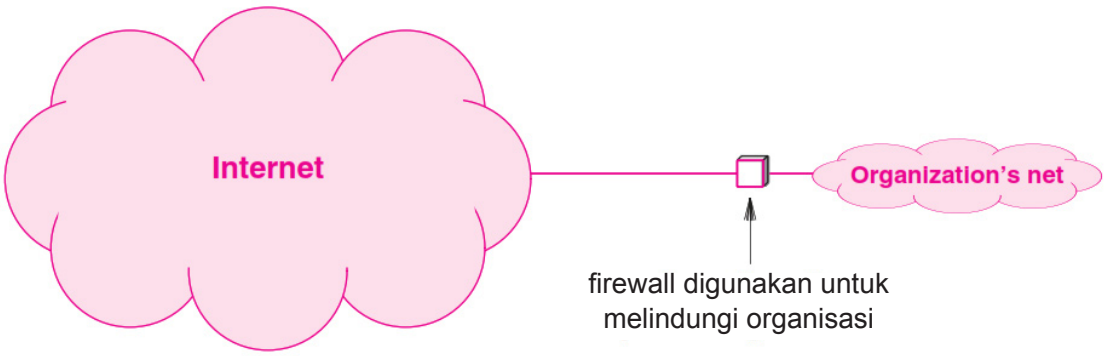
Pada gambar, sebuah situs perlu melakukan transaksi yang aman dengan situs web, W. Masing-masing dari empat pesan bersifat rahasia. Pesan 1 hanya dapat dibaca oleh otoritas kunci karena telah dienkripsi menggunakan kunci publik otoritas kunci yang terkenal. Pesan 2 pasti dihasilkan oleh otoritas kunci karena hanya otoritas kunci yang memiliki kunci privat yang cocok dengan kunci publik. Setelah pengguna memperoleh kunci publik untuk situs W, pengguna dapat mengirim permintaan rahasia dan mengetahui bahwa hanya situs web tertentu yang dapat menghasilkan respons (karena hanya situs yang memiliki kunci pribadi).

Meskipun banyak variasi yang mungkin, prinsip penting adalah:

Dimungkinkan untuk membuat sistem distribusi kunci yang aman yang hanya memerlukan konfigurasi manual dari satu kunci publik

11.12 Firewall

Meskipun teknologi enkripsi membantu memecahkan banyak masalah keamanan, teknologi kedua diperlukan. Dikenal sebagai firewall Internet†, teknologi ini membantu melindungi komputer dan jaringan organisasi dari lalu lintas Internet yang tidak diinginkan. Seperti firewall konvensional, firewall Internet dirancang untuk menjaga agar masalah di Internet tidak menyebar ke komputer organisasi. Firewall ditempatkan di antara organisasi dan seluruh Internet, dan semua paket yang masuk atau keluar dari organisasi melewati firewall. Gambar 11.8 mengilustrasikan arsitekturnya.



Gambar 11.8 Ilustrasi firewall pada jalur antara Internet dan organisasi.

Jika sebuah organisasi memiliki beberapa koneksi Internet, firewall harus ditempatkan pada masing-masing koneksi, dan semua firewall organisasi harus dikonfigurasi untuk menegakkan kebijakan keamanan organisasi. Selanjutnya, firewall itu sendiri harus aman dari gangguan. Un

Poin Penting

Semua lalu lintas yang memasuki organisasi melewati firewall
Semua lalu lintas yang meninggalkan organisasi melewati firewall
Firewall menerapkan kebijakan keamanan dan menjatuhkan paket yang tidak mematuhi kebijakan
Firewall itu sendiri kebal terhadap serangan keamanan

Firewall adalah alat keamanan terpenting yang digunakan untuk menangani koneksi antara dua organisasi yang tidak saling percaya. Dengan menempatkan firewall pada setiap koneksi jaringan eksternal, organisasi dapat menentukan batas aman yang mencegah pihak luar mengganggu komputer organisasi. Secara khusus, firewall dapat mencegah orang luar menemukan komputer dalam organisasi, membanjiri jaringan organisasi dengan lalu lintas yang tidak diinginkan, atau menyerang komputer dengan mengirimkan urutan IP datagram yang diketahui menyebabkan komputer berperilaku tidak semestinya (mis., mogok). Selain itu, firewall dapat mencegah ekspor data yang tidak diinginkan (misalnya, pengguna di organisasi secara tidak sengaja mengimpor virus yang mengirimkan salinan disk pengguna ke seseorang di luar organisasi).

Firewall memiliki keunggulan utama dibandingkan skema keamanan lainnya: ia memusatkan kontrol, dan dengan demikian meningkatkan keamanan secara dramatis. Untuk memberikan keamanan tanpa firewall, organisasi harus membuat setiap komputernya aman. Selanjutnya, setiap komputer harus menerapkan kebijakan yang sama. Biaya mempekerjakan staf untuk mengelola banyak komputer tinggi, dan organisasi tidak dapat bergantung pada pengguna individu untuk mengkonfigurasi komputer mereka dengan benar. Dengan firewall, seorang manajer dapat membatasi semua lalu lintas Internet ke satu set komputer kecil, dan menggunakan staf untuk mengkonfigurasi dan memantau set. Dalam kasus ekstrim, semua akses luar dapat dibatasi untuk satu komputer. Jadi, firewall memungkinkan organisasi untuk menghemat uang dan mencapai keamanan yang lebih baik.

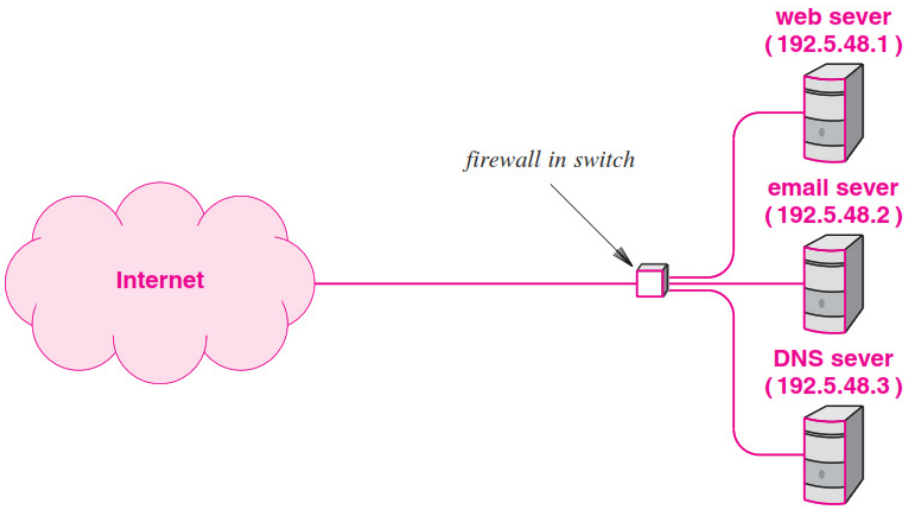
11.13 Implementasi Firewall dengan Filter Paket

Meskipun firewall dapat terdiri dari perangkat yang berdiri sendiri, sebagian besar firewall tertanam di sakelar atau router. Dalam kedua kasus tersebut, mekanisme dasar yang digunakan untuk membangun firewall dikenal sebagai filter paket. Filter terdiri dari mekanisme yang dapat dikonfigurasi yang memeriksa bidang di setiap header paket dan memutuskan apakah akan mengizinkan paket melewati router atau membuang paket. Seorang manajer mengkonfigurasi filter paket dengan menentukan paket mana yang dapat lewat di setiap arah. (Lebih aman untuk menentukan kumpulan paket yang diizinkan daripada menentukan kumpulan paket yang ditolak.)

Untuk TCP/IP, spesifikasi filter paket biasanya mencakup tipe bingkai 0800 (untuk IP), alamat sumber IP atau alamat tujuan (atau keduanya), tipe datagram, dan nomor port protokol. Misalnya, untuk mengizinkan orang luar mencapai server web organisasi, filter paket mungkin mengizinkan bingkai masuk yang berisi datagram IP yang membawa TCP dari alamat sumber IP arbitrer dan port sumber ke port tujuan 80 dan alamat IP tujuan yang sama dengan web alamat IP server.

Karena memungkinkan manajer untuk menentukan kombinasi alamat dan layanan sumber dan tujuan, filter paket di firewall memungkinkan manajer untuk mengontrol akses ke layanan tertentu pada komputer tertentu. Misalnya, seorang manajer mungkin memilih untuk mengizinkan lalu lintas masuk mengakses server web di satu komputer, server email di komputer lain, dan server DNS di komputer ketiga. Tentu saja, seorang manajer juga harus memasang aturan firewall yang mengizinkan paket balasan mengalir keluar dari situs. Gambar 11.9 mengilustrasikan konfigurasi firewall untuk situs tersebut.

Kemampuan untuk secara selektif mengizinkan paket untuk layanan tertentu berarti bahwa seorang manajer dapat dengan hati-hati mengontrol layanan yang terlihat secara eksternal. Jadi, bahkan jika pengguna secara tidak sengaja (atau sengaja) memulai server email di komputer mereka, orang luar tidak akan dapat menghubungi server.



Dir	Frame Type	IP Src	IP Dest	IP Type	Src Port	Dst Port
in	0800	*	192.5.48.1	TCP	*	80
in	0800	*	192.5.48.2	TCP	*	25
in	0800	*	192.5.48.3	TCP	*	53
in	0800	*	192.5.48.3	UDP	*	53
out	0800	192.5.48.1	*	TCP	80	*
out	0800	192.5.48.2	*	TCP	25	*
out	0800	192.5.48.3	*	TCP	53	*
out	0800	192.5.48.3	*	UDP	53	*

Gambar 11.9 Contoh konfigurasi firewall untuk situs dengan tiga server, dengan tanda bintang yang digunakan untuk menunjukkan entri wildcard yang cocok dengan nilai apa pun.

Poin Penting

Firewall menggunakan penyaringan paket untuk mencegah komunikasi yang tidak diinginkan. Setiap spesifikasi filter memberikan kombinasi bidang header, termasuk alamat IP sumber dan tujuan dan nomor port serta jenis protokol transport.

11.14 Sistem Deteksi Intrusi

Intrusion Detection System (IDS) memantau semua paket yang tiba di situs dan memberi tahu administrator situs jika pelanggaran keamanan terdeteksi. IDS memberikan lapisan tambahan kesadaran keamanan — bahkan jika firewall mencegah serangan, IDS dapat memberi tahu administrator situs bahwa ada masalah yang terjadi.

Sebagian besar IDS dapat dikonfigurasi untuk mengawasi jenis serangan tertentu. Misalnya, IDS dapat dikonfigurasi untuk mendeteksi serangan pemindaian port di mana penyerang mengirim datagram UDP ke port protokol UDP yang berurutan atau mencoba membuka koneksi TCP pada port protokol TCP yang berurutan. Demikian pula, IDS dapat dikonfigurasi untuk mendeteksi potensi serangan SYN flooding dengan mengamati SYN berulang dari sumber tertentu. Dalam beberapa kasus, IDS dan firewall saling berhubungan untuk menyediakan pemfilteran otomatis: alih-alih hanya memberi tahu administrator situs tentang masalah, IDS membuat aturan firewall yang memblokir paket yang menyebabkan masalah. Misalnya, jika IDS mendeteksi banjir SYN yang berasal dari sumber tertentu, IDS dapat menginstal aturan firewall yang memblokir paket dari sumber tersebut. Alasan menggunakan pendekatan otomatis adalah kecepatan

— manusia membutuhkan beberapa detik untuk merespons setelah diberi tahu tentang masalah dan pada jaringan gigabit, lebih dari 50.000 paket dapat tiba per detik. Oleh karena itu, diperlukan respon yang cepat untuk mencegah masalah menjadi berlebihan.

Perbedaan utama antara IDS dan firewall muncul karena IDS menyertakan informasi status. Tidak seperti firewall yang menerapkan aturan ke satu paket pada satu waktu, IDS dapat menyimpan riwayat paket. Jadi, meskipun firewall dapat menentukan apakah akan menerima paket SYN yang diberikan, IDS dapat mengamati bahwa banyak SYN datang dari satu sumber. Tentu saja, karena membutuhkan lebih banyak komputasi dan akses memori daripada firewall, IDS tidak dapat menangani banyak paket per detik.

11.15 Pemindaian Konten dan Inspeksi Paket Dalam

Meskipun dapat menangani banyak masalah keamanan, firewall memiliki batasan yang parah: firewall hanya memeriksa bidang dalam header paket. Artinya, firewall tidak dapat menguji muatan paket. Untuk melihat mengapa isi paket bisa menjadi penting, pertimbangkan virus komputer. Salah satu cara paling umum virus masuk ke dalam organisasi adalah melalui lampiran email — penyerang mengirim pesan email dengan program komputer sebagai lampiran. Jika pengguna yang tidak curiga membuka lampiran, program dapat menginstal perangkat lunak sewenang-wenang di komputer pengguna, termasuk malware† seperti virus.

Bagaimana sebuah situs dapat mencegah masalah seperti instalasi virus? Jawabannya terletak pada analisis isi. Ada dua jenis analisis isi:

- Pemindaian file
- Inspeksi Paket Dalam (DPI)

Pemindaian Berkas

Pendekatan paling mudah untuk menganalisis konten beroperasi pada seluruh file. Pemindaian file adalah teknik terkenal yang digunakan oleh perangkat lunak keamanan yang diinstal pada PC biasa. Intinya, pemindai file mengambil file sebagai input dan mencari pola byte yang menunjukkan masalah. Misalnya, banyak pemindai virus mencari string byte yang dikenal sebagai sidik jari. Artinya, perusahaan yang menjual pemindai virus mengumpulkan salinan virus, menempatkan masing-masing dalam file, menemukan urutan byte yang tidak umum, dan membuat daftar semua urutan. Saat pengguna menjalankan perangkat lunak pemindai virus, perangkat lunak mencari file di disk pengguna untuk melihat apakah ada file yang berisi urutan byte yang cocok dengan item dalam daftar. Pemindaian file berfungsi dengan baik untuk mengatasi masalah umum. Tentu saja, pemindaian file dapat menghasilkan positif palsu jika file biasa berisi string dalam daftar, dan dapat menghasilkan negatif palsu jika ada virus baru yang tidak berisi string apa pun dalam daftar.

Inspeksi Paket Dalam (DPI)

Bentuk kedua dari analisis konten beroperasi pada paket, bukan file. Artinya, alih-alih hanya memeriksa header dalam paket yang masuk ke situs, mekanisme DPI juga memeriksa data dalam muatan paket. Perhatikan bahwa DPI tidak mengecualikan pemeriksaan header — dalam banyak kasus, konten muatan tidak dapat ditafsirkan tanpa memeriksa bidang di header paket.

Sebagai contoh DPI, pertimbangkan serangan di mana sedikit kesalahan ejaan nama domain digunakan untuk mengelabui pengguna agar memercayai situs. Sebuah organisasi yang ingin mencegah serangan semacam itu dapat membuat daftar hitam sekumpulan URL yang dikenal sebagai risiko keamanan. Pendekatan proxy mengharuskan setiap pengguna di situs untuk mengonfigurasi browser mereka untuk menggunakan proxy web (yaitu, sistem web perantara yang memeriksa URL sebelum mengambil halaman yang diminta). Sebagai alternatif, filter Inspeksi Paket Dalam dapat diatur untuk memeriksa setiap paket keluar dan melihat permintaan HTTP ke salah satu situs yang masuk daftar hitam.

Kerugian utama DPI muncul dari overhead komputasi. Karena muatan paket dalam bingkai Ethernet bisa lebih dari dua puluh kali lebih besar dari header paket, DPI dapat memerlukan pemrosesan dua puluh kali lebih banyak daripada inspeksi header. Selanjutnya, muatan tidak dibagi menjadi bidang tetap, yang berarti bahwa mekanisme DPI harus mengurai konten selama inspeksi. Hasil dari:

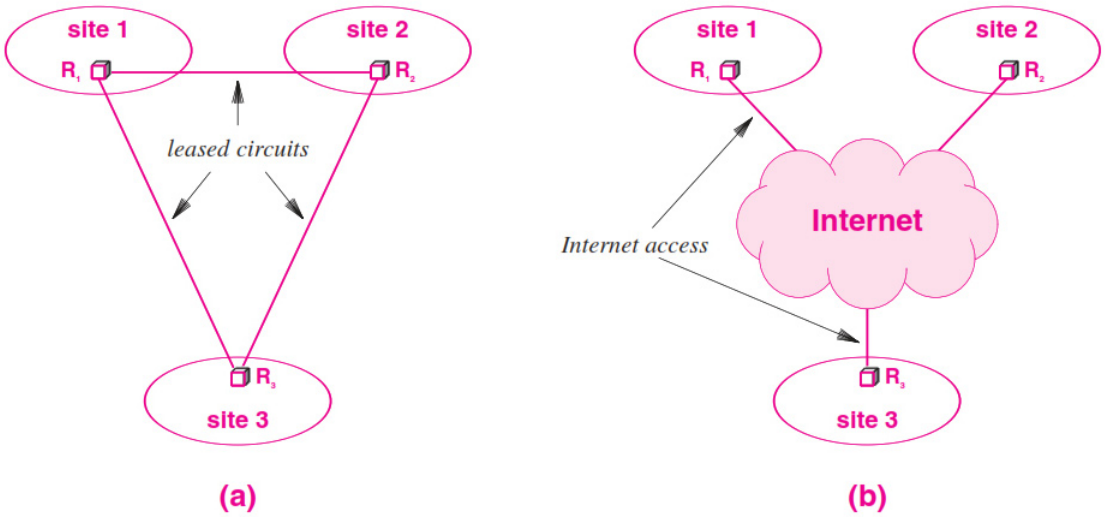
Karena mereka memeriksa muatan paket yang jauh lebih besar dari header paket dan tidak diatur ke dalam bidang tetap, mekanisme Inspeksi Paket Dalam terbatas pada jaringan berkecepatan rendah.

11.16 Virtual Private Networks (VPN)

Salah satu teknologi keamanan yang paling penting dan banyak digunakan menggunakan enkripsi untuk menyediakan akses aman ke intranet organisasi dari situs jarak jauh. Dikenal sebagai Virtual Private Network (VPN), teknologi ini awalnya dirancang untuk menyediakan interkoneksi berbiaya rendah di antara beberapa situs geografis suatu organisasi. Untuk memahami motivasi, pertimbangkan alternatif interkoneksi:

- Koneksi Jaringan Pribadi. Sebuah organisasi menyewa sirkuit data untuk menghubungkan situsnya. Setiap koneksi yang disewa meluas dari router di salah satu situs organisasi ke router di situs lain; data lewat langsung dari router di satu situs ke router di situs lain.
- Koneksi Internet Publik. Setiap situs kontrak dengan ISP lokal untuk layanan Internet. Data yang dikirim dari satu situs perusahaan ke situs lainnya melewati Internet.

Gambar 11.10 mengilustrasikan dua kemungkinan untuk sebuah organisasi dengan tiga lokasi.



Gambar 11.10 Situs yang dihubungkan oleh (a) sirkit sewaan dan (b) Internet.

Keuntungan utama menggunakan sirkit yang disewakan ke situs interkoneksi muncul karena jaringan yang dihasilkan sepenuhnya pribadi (yaitu, rahasia). Tidak ada organisasi lain yang memiliki akses ke sirkuit sewaan, jadi tidak ada organisasi lain yang dapat membaca data yang berpindah dari satu situs ke situs lainnya. Keuntungan utama menggunakan koneksi Internet adalah biaya rendah — alih-alih membayar saluran untuk menghubungkan situs, organisasi hanya perlu membayar layanan Internet di setiap situs. Sayangnya, Internet tidak dapat menjamin kerahasiaan. Saat berjalan dari sumber ke tujuan, datagram melewati jaringan perantara yang dapat dibagikan. Akibatnya, orang luar mungkin dapat memperoleh salinan datagram dan memeriksa isinya.

VPN menggabungkan yang terbaik dari kedua pendekatan dengan menggunakan Internet untuk mentransfer data antar situs dan mengambil langkah tambahan untuk memastikan bahwa data tidak

dapat diakses oleh orang luar. Artinya, sebagai ganti koneksi sewaan yang mahal, VPN menggunakan enkripsi — semua paket yang diteruskan antara situs organisasi dienkripsi sebelum dikirim.

Untuk membuat VPN lebih tahan terhadap serangan, organisasi dapat menggunakan router khusus untuk fungsi VPN dan menggunakan firewall untuk melarang router VPN menerima paket yang tidak sah. Misalnya, asumsikan masing-masing router pada Gamba 11.10b didedikasikan untuk fungsi VPN (yaitu, asumsikan situs memiliki router tambahan yang menangani lalu lintas normal ke dan dari Internet). Sebuah firewall yang melindungi router VPN di situs 1 dapat membatasi semua paket masuk untuk memiliki alamat sumber IP router VPN di situs 2 atau router VPN di situs 3. Demikian pula, firewall di masing-masing dari dua situs lainnya membatasi paket masuk di situs itu. Pembatasan membantu membuat sistem yang dihasilkan lebih kebal terhadap serangan spoofing dan DoS.

11.17 Penggunaan Teknologi VPN untuk Telecommuting

Meskipun awalnya dirancang untuk menghubungkan situs, teknologi VPN telah menjadi sangat populer di kalangan karyawan yang melakukan telekomunikasi (yaitu, bekerja dari lokasi yang jauh). Ada dua bentuk VPN:

- Perangkat yang berdiri sendiri
- perangkat lunak VPN

Perangkat yang berdiri sendiri

Organisasi mengeluarkan karyawan perangkat fisik yang kadang-kadang disebut router VPN. Perangkat terhubung ke Internet, secara otomatis membuat komunikasi yang aman ke server VPN di situs organisasi, dan menyediakan koneksi Jaringan Area Lokal di mana pengguna dapat menghubungkan komputer dan telepon IP. Logikanya, perangkat VPN memperluas jaringan organisasi ke situs pengguna, memungkinkan komputer yang terhubung ke perangkat VPN untuk beroperasi seolah-olah mereka terhubung ke jaringan perusahaan. Jadi, ketika komputer pengguna melakukan booting dan memperoleh alamat IP, alamat tersebut akan dikeluarkan oleh server DHCP di organisasi. Demikian pula, tabel penerusan di komputer pengguna diatur seolah-olah komputer berada di situs organisasi — setiap kali komputer mengirim paket, VPN mengenkripsi paket dan mengirimkan versi terenkripsi melalui Internet ke organisasi. Setiap kali sebuah paket tiba dari organisasi, perangkat VPN mendekripsi paket dan mengirimkan hasilnya ke komputer pengguna.

Perangkat Lunak VPN

Meskipun perangkat yang berdiri sendiri berfungsi dengan baik untuk karyawan yang bekerja di rumah atau di kantor jarak jauh, perangkat tersebut tidak praktis bagi karyawan yang bepergian. Untuk menangani kasus seperti itu, organisasi menggunakan perangkat lunak VPN yang berjalan di komputer pribadi pengguna. Seorang pengguna terhubung ke Internet, dan kemudian meluncurkan aplikasi VPN. Saat dimulai, aplikasi VPN menyela dirinya sendiri dalam koneksi ke Internet. Artinya, perangkat lunak VPN mengatur untuk menangkap semua paket keluar dan masuk. Itu mengenkripsi setiap paket keluar dan mengirimkan paket terenkripsi ke server VPN perusahaan, dan mendekripsi setiap paket yang masuk.

11.18 Enkripsi Paket Vs. Tunneling

Diskusi VPN di atas menimbulkan pertanyaan menarik: bagaimana seharusnya data dienkripsi untuk transmisi di Internet? Ada tiga opsi utama:

- Enkripsi Muatan
- Tunneling IP-dalam-IP
- Tunneling IP-dalam-TCP

Enkripsi Muatan

Untuk menjaga kerahasiaan isi datagram, pendekatan enkripsi muatan mengenkripsi area muatan datagram, tetapi membiarkan header tidak tersentuh. Karena bidang header tidak dienkripsi, orang luar akan dapat mempelajari alamat sumber dan tujuan yang digunakan serta nomor port protokol. Sebagai contoh, anggaplah chief financial officer (CFO) berada di satu tempat dan presiden perusahaan di tempat lain. Lebih lanjut misalkan CFO mengirim pesan email singkat kepada presiden setiap kali berita keuangan bagus, tapi penjelasan panjang kapan berita keuangan tidak bagus. Orang luar mungkin dapat mengamati bahwa segera setelah pesan singkat mengalir di antara dua komputer tertentu, harga saham meningkat.

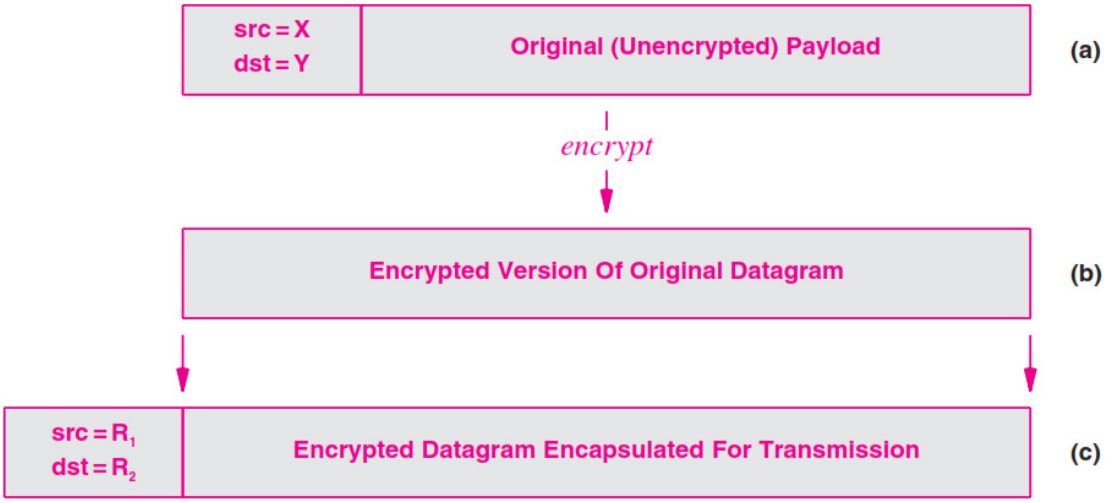
Tunneling IP-dalam-IP

Beberapa VPN menggunakan pendekatan tunneling IP-in-IP yang membuat informasi header tetap tersembunyi saat datagram melewati Internet dari satu situs ke situs lainnya. Ketika menemukan datagram keluar, perangkat lunak VPN pengirim mengenkripsi seluruh datagram, termasuk header, dan menempatkan hasilnya di dalam datagram lain untuk transmisi. Sebagai contoh, perhatikan koneksi pada Gambar 11.10. Misalkan komputer X di situs 1 membuat datagram untuk komputer Y di situs 2. Datagram diteruskan melalui situs 1 ke router R1 (yaitu, router yang menghubungkan situs 1 ke Internet). Fasilitas VPN di R1 mengenkripsi datagram asli dan mengenkapsulasinya dalam datagram baru untuk transmisi ke router R2, router di situs 2. Ketika datagram yang dienkapsulasi tiba, perangkat lunak VPN di R2 mendekripsi payload untuk mengekstrak datagram asli, dan kemudian meneruskannya ke tujuan Y. Gambar 11.11 mengilustrasikan enkapsulasi.

Pada gambar, (a) menunjukkan datagram asli, (b) menunjukkan cyphertext hasil enkripsi, dan (c) menunjukkan datagram luar yang dikirim dari R1 ke R2. Perhatikan bahwa alamat internal disembunyikan karena semua datagram yang melintasi Internet antara situs 1 dan 2 mencantumkan router R1 dan R2 sebagai alamat sumber dan tujuan.

Poin Penting

Ketika VPN menggunakan enkapsulasi IP-in-IP, semua bidang dalam datagram asli dienkripsi, termasuk header asli.



Gambar 11.11 Ilustrasi enkapsulasi IP-in-IP yang digunakan dengan VPN.

Tunneling IP-dalam-TCP

Alternatif ketiga yang mungkin digunakan untuk menjaga kerahasiaan data melibatkan penggunaan Tunneling TCP. Artinya, dua pihak membuat koneksi TCP, dan kemudian menggunakan koneksi tersebut untuk mengirim datagram terenkripsi. Ketika datagram harus dikirim, seluruh datagram dienkripsi, header kecil ditambahkan untuk menandai batas antara datagram, dan hasilnya dikirim melalui koneksi TCP. Biasanya, header terdiri dari integer dua byte yang menentukan panjang datagram. Di ujung lain koneksi TCP, perangkat lunak VPN penerima membaca header, dan kemudian membaca jumlah byte tambahan yang ditentukan untuk mendapatkan datagram. Setelah seluruh cyphertext untuk datagram telah diterima, penerima mendekripsi dan memproses datagram asli.

Keuntungan utama menggunakan IP-in-TCP daripada IP-in-IP muncul dari pengiriman yang andal: TCP memastikan bahwa semua datagram yang dikirim antara dua situs tiba dengan andal dan berurutan. Kerugian utama menggunakan IP-in-TCP adalah pemblokiran head-of-line: karena semua datagram harus dikirimkan secara berurutan, jika satu segmen TCP hilang atau tertunda, TCP tidak dapat mengirimkan data dari segmen yang berurutan, bahkan jika mereka memiliki tiba dengan benar. Jika kita menganggap VPN sebagai mentransfer antrian paket, seluruh antrian tetap diblokir sampai datagram pertama dikirimkan.

Masalah terakhir muncul terkait tunneling VPN: kinerja. Ada tiga aspek:

- Latensi
- Throughput
- Overhead Dan Fragmentasi

Latensi

Untuk memahami masalah latensi, pertimbangkan sebuah organisasi di Pantai Barat Amerika Serikat, dan asumsikan seorang karyawan melakukan perjalanan ke Pantai Timur, sekitar 3.000 mil jauhnya. Ingatlah bahwa perangkat lunak VPN hanya mentransfer datagram kembali ke organisasi

asal — setelah mencapai organisasi, datagram harus dirutekan ke tujuannya. Misalnya, jika karyawan menelusuri halaman web, setiap permintaan harus berpindah dari lokasi karyawan saat ini ke server VPN organisasi, dan dari sana ke server web. Balasan harus melakukan perjalanan kembali ke server VPN organisasi, dan akhirnya ke karyawan di lokasi terpencil. Latensi yang diperlukan untuk mengakses sumber daya yang dekat dengan karyawan sangat tinggi karena datagram harus berjalan dari karyawan melintasi VPN ke organisasi di Pantai Barat dan kembali ke sumber daya di Pantai Timur. Akibatnya, perjalanan pulang pergi membutuhkan datagram untuk melakukan empat lintasan benua.

Throughput

Masalah lain dengan VPN konvensional muncul dari throughput yang tersedia di Internet. Masalahnya bisa menjadi penting saat menggunakan aplikasi yang telah dirancang untuk LAN berkecepatan tinggi. Di beberapa organisasi, misalnya, halaman web yang digunakan karyawan untuk bisnis internal perusahaan berisi grafik yang ekstensif. LAN di situs menyediakan throughput yang cukup untuk mempercepat pengunduhan halaman web. Untuk pengguna jarak jauh yang terhubung melalui VPN, throughput yang rendah dapat membuat menunggu halaman web menjadi frustasi.

Overhead Dan Fragmentasi

Aspek kinerja ketiga muncul karena tunneling menambahkan overhead ke datagram. Untuk memahami masalahnya, misalkan sebuah situs menggunakan Ethernet dan aplikasi telah membuat datagram yang panjangnya 1500 byte (yaitu, datagram persis sebesar MTU jaringan). Ketika router VPN merangkum datagram terenkripsi dalam datagram IP lain, setidaknya dua puluh byte tambahan ditambahkan untuk header datagram luar. Datagram yang dihasilkan melebihi jaringan MTU, dan akan terfragmentasi sebelum transmisi. Karena kedua fragmen harus tiba sebelum datagram dapat diproses, kemungkinan delay atau loss lebih tinggi.

11.19 Teknologi Keamanan

Berbagai teknologi keamanan telah diciptakan untuk digunakan di Internet. Sorotan meliputi:

- PGP (*Pretty Good Privacy*). Sistem kriptografi yang dapat digunakan aplikasi untuk mengenkripsi data sebelum transmisi. PGP dikembangkan di MIT, dan sangat populer di kalangan ilmuwan komputer.
- SSH (*Secure Shell*). Protokol lapisan aplikasi untuk login jarak jauh yang menjamin kerahasiaan dengan mengenkripsi data sebelum dikirim melalui Internet.
- SSL (*Secure Socket Layer*). Sebuah teknologi yang awalnya dirancang oleh Netscape Communications yang menggunakan enkripsi untuk menyediakan otentikasi dan kerahasiaan. Perangkat lunak SSL cocok antara aplikasi dan API soket, dan mengenkripsi data sebelum dikirim melalui Internet. SSL digunakan pada koneksi web untuk memungkinkan pengguna melakukan transaksi keuangan dengan aman (misalnya, mengirim nomor kartu kredit ke server web).
- TLS (*Transport Layer Security*). Dirancang oleh IETF di akhir 1990-an sebagai penerus SSL, TLS dibangun di atas versi 3 SSL. Baik SSL dan TLS tersedia untuk digunakan dengan HTTPS.

- IPsec (*IP security*). Standar keamanan yang digunakan dengan datagram IP. IPsec menggunakan teknik kriptografi, dan memungkinkan pengirim untuk memilih otentikasi (yaitu, memvalidasi pengirim dan penerima datagram) atau kerahasiaan (yaitu, mengenkripsi muatan datagram).
- RADIUS (*Remote Authentication Dial-In User Service*). Sebuah protokol yang digunakan untuk menyediakan otentikasi terpusat, otorisasi, dan akuntansi. RADIUS populer dengan ISP yang memiliki pengguna dialup dan dengan sistem VPN yang menyediakan akses ke pengguna jarak jauh.
- WEP (*Wired Equivalent Privacy*). Awalnya bagian dari standar LAN nirkabel Wi-Fi† digunakan untuk menjaga kerahasiaan transmisi. Para peneliti di U.C. Berkeley telah menunjukkan bahwa WEP memiliki beberapa kelemahan. Dengan demikian, pengganti telah dikembangkan bernama WPA (Wi-Fi Protected Access).

11.20 Ringkasan

Jaringan komputer dan internet dapat digunakan untuk kegiatan kriminal; ancaman utama termasuk phishing, misrepresentasi, penipuan, penolakan layanan, kehilangan kendali, dan kehilangan data. Teknik yang digunakan dalam serangan meliputi: penyadapan, pemutaran ulang, buffer overflow, spoofing alamat dan nama, DoS dengan paket dan SYN flooding, pemecahan kunci, pemindaian port, dan intersepsi paket.

Setiap organisasi perlu menetapkan kebijakan keamanan yang menentukan aspek integritas data (perlindungan terhadap perubahan), ketersediaan data (perlindungan terhadap gangguan layanan), dan kerahasiaan atau privasi data (perlindungan terhadap pengintaian dan penemuan). Selain itu, organisasi harus mempertimbangkan akuntabilitas (yaitu, bagaimana jejak audit disimpan) dan otorisasi (yaitu, bagaimana tanggung jawab atas informasi diteruskan dari satu orang ke orang lain).

Serangkaian teknologi yang telah dibuat untuk menyediakan berbagai aspek keamanan meliputi: enkripsi, hashing, tanda tangan dan sertifikat digital, firewall, sistem deteksi intrusi, inspeksi paket mendalam, pemindaian konten, dan Jaringan Privat Virtual. Enkripsi adalah salah satu teknologi paling mendasar yang digunakan dalam banyak mekanisme keamanan.

Enkripsi kunci pribadi menggunakan satu kunci untuk mengenkripsi dan mendekripsi pesan; pengirim dan penerima harus merahasiakan kunci tersebut. Sistem enkripsi kunci publik menggunakan sepasang kunci; satu kunci dirahasiakan dan yang lainnya (kunci publik) diiklankan secara luas. Tanda tangan digital menggunakan enkripsi untuk mengotentikasi pesan. Otoritas kunci dapat mengeluarkan sertifikat untuk memvalidasi kunci publik.

Firewall melindungi situs dari serangan dengan membatasi paket yang dapat masuk atau keluar. Untuk mengkonfigurasi firewall, seorang manajer merancang seperangkat aturan yang memberikan nilai spesifik untuk bidang header paket. Sistem Deteksi Intrusi yang menyimpan informasi status dapat mengidentifikasi serangan seperti SYN berulang.

Virtual Private Networks (VPNs) memberikan manfaat kerahasiaan dan biaya rendah. Teknologi VPN memungkinkan karyawan untuk melakukan telecommuting. Untuk menjaga kerahasiaan informasi, pengirim dapat mengenkripsi payload, menggunakan tunneling IP-in-IP, atau menggunakan tunneling

IP-in-TCP. Tunneling memiliki keuntungan mengenkripsi header paket serta muatannya. Beberapa aplikasi tidak bekerja dengan baik melalui VPN karena VPN memiliki penundaan yang lebih lama, throughput yang lebih rendah, dan overhead yang lebih tinggi daripada koneksi langsung.

Banyak teknologi keamanan yang ada. Contohnya meliputi: PGP, SSH, SSL, TLS, HTTPS, IPsec, RADIUS, dan WEP.

Latihan

1. Buat daftar masalah keamanan utama di Internet, dan berikan deskripsi singkat masing-masing.
2. Sebutkan teknik yang digunakan dalam serangan keamanan.
3. Misalkan penyerang menemukan cara untuk menyimpan pengikatan arbitrer di server DNS lokal Anda. Bagaimana penyerang dapat menggunakan kelemahan seperti itu untuk mendapatkan informasi rekening bank Anda?
4. Serangan DoS sering mengirimkan segmen TCP SYN. Bisakah penyerang juga membuat serangan DoS dengan mengirimkan segmen data TCP? Menjelaskan.
5. Jika kata sandi berisi delapan huruf besar dan kecil serta angka, berapa banyak kemungkinan kata sandi yang mungkin diperlukan penyerang untuk mencoba mendapatkan akses?
6. Mengapa membuat kebijakan keamanan sulit?
7. Misalkan sebuah perusahaan menyusun kebijakan keamanan yang menetapkan bahwa hanya personel SDM yang berwenang untuk melihat file penggajian. Mekanisme seperti apa yang dibutuhkan untuk mengimplementasikan kebijakan tersebut? Menjelaskan.
8. Sebutkan dan jelaskan delapan teknik keamanan dasar
9. Apa yang dimaksud dengan daftar kontrol akses (ACL), dan bagaimana ACL digunakan?
10. Apa yang dimaksud dengan kriptografi?
11. Baca tentang Data Encryption Standard (DES). Kunci ukuran apa yang harus digunakan untuk data yang sangat penting?
12. Misalkan teman Anda memiliki kunci publik dan pribadi untuk digunakan dengan enkripsi kunci publik. Dapatkah teman Anda mengirimi Anda pesan rahasia (yaitu, pesan yang hanya dapat Anda baca)? Mengapa atau mengapa tidak?
13. Jika Anda dan seorang teman masing-masing memiliki sepasang kunci publik dan pribadi untuk sistem enkripsi kunci publik, bagaimana Anda dan teman Anda dapat melakukan komunikasi sehari-hari tanpa tertipu oleh serangan replay?
14. Bagaimana dua pihak dapat menggunakan enkripsi kunci publik untuk menandatangani kontrak yang kemudian dikirim ke pihak ketiga?
15. Apa yang dimaksud dengan sertifikat digital?
16. Apa itu firewall, dan di mana firewall dipasang?
17. Banyak produk firewall komersial memungkinkan manajer untuk menentukan paket yang akan ditolak serta paket yang akan diterima. Apa kerugian dari konfigurasi yang memungkinkan penolakan?
18. Tulis ulang konfigurasi firewall pada Gambar 11.9 untuk memungkinkan pihak luar melakukan ping ke masing-masing dari tiga server.
19. Tulis ulang konfigurasi firewall pada Gambar 11.9 untuk memindahkan server email ke komputer yang menjalankan server web.
20. Baca tentang sistem IDS komersial, dan buat daftar serangan yang dapat dideteksi sistem.

21. Pertimbangkan sistem DPI yang mencari string K byte di setiap paket. Jika sebuah paket berisi 1486 byte payload, berapa jumlah kasus terburuk dari perbandingan yang harus dilakukan untuk memeriksa paket dengan asumsi algoritma pencocokan langsung?
22. Mengapa inspeksi paket mendalam tidak digunakan pada jaringan berkecepatan tertinggi?
23. Apa dua tujuan dari sistem VPN?
24. Apa tiga cara VPN dapat mentransfer data melalui Internet?
25. Ketika VPN menggunakan tunneling IP-in-IP, apa yang mencegah penyerang membaca header datagram asli?
26. Dalam beberapa sistem VPN, pengirim menambahkan sejumlah bit nol secara acak ke datagram sebelum enkripsi, dan penerima membuang bit tambahan setelah datagram didekripsi. Jadi, satu-satunya efek dari padding acak adalah membuat panjang datagram terenkripsi tidak tergantung pada panjang versi yang tidak terenkripsi. Mengapa panjang penting?
27. Sebutkan delapan teknologi keamanan yang digunakan di Internet, dan jelaskan tujuan masing-masing.
28. Baca tentang kerentanan dalam protokol WEP. Bagaimana protokol WPA menghindari masalah?

Bab 12 Manajemen Jaringan (SNMP)

Bab ini akan membahas tentang:

- Aplikasi jaringan dengan mempertimbangkan manajemen jaringan.
- Model konseptual yang digunakan dalam industri, dan menggunakan model tersebut untuk menjelaskan ruang lingkup kegiatan manajemen
- Paradigma umum yang digunakan oleh sistem manajemen, dan menjelaskan fungsionalitas yang disediakan oleh sistem tersebut

12.1 Mengelola Intranet

Manajer jaringan, kadang-kadang disebut administrator jaringan, adalah orang yang bertanggung jawab untuk merencanakan, menginstal, mengoperasikan, memantau, dan mengendalikan sistem perangkat keras dan perangkat lunak yang membentuk jaringan komputer atau intranet. Seorang manajer merencanakan jaringan yang memenuhi persyaratan kinerja, memantau operasi, mendeteksi dan memperbaiki masalah yang membuat komunikasi tidak efisien atau tidak mungkin, dan bekerja untuk menghindari kondisi yang akan menghasilkan masalah lagi. Karena kegagalan perangkat keras atau perangkat lunak dapat menyebabkan masalah, manajer jaringan harus memantau keduanya.

Manajemen jaringan bisa sulit karena tiga alasan. Pertama, di sebagian besar organisasi, intranet bersifat heterogen — intranet berisi komponen perangkat keras dan perangkat lunak yang diproduksi oleh banyak perusahaan. Kedua, teknologi terus berubah, artinya perangkat dan layanan baru terus bermunculan. Ketiga, kebanyakan intranet berukuran besar, yang berarti beberapa bagian dari intranet jauh dari yang lain. Mendeteksi penyebab masalah komunikasi di perangkat jarak jauh bisa sangat sulit.

Manajemen jaringan juga sulit karena banyak mekanisme jaringan yang dirancang untuk mengatasi masalah secara otomatis. Protokol perutean melewati kegagalan dan kehilangan paket yang terputus-putus dapat luput dari perhatian karena TCP secara otomatis mentransmisi ulang. Sayangnya, pemulihan kesalahan otomatis memiliki konsekuensi. Pengiriman ulang paket menggunakan bandwidth

jaringan yang dapat digunakan untuk mengirim data baru. Demikian pula, kegagalan perangkat keras yang tidak terdeteksi dapat menjadi kritis jika jalur pencadangan juga gagal.

Poin Penting

Meskipun perangkat keras jaringan dan perangkat lunak protokol mengandung mekanisme untuk secara otomatis merutekan kegagalan atau mengirimkan kembali paket yang hilang, manajer jaringan perlu mendeteksi dan memperbaiki masalah mendasar.

12.2 FCAPS: Model Standar Industri

Industri jaringan menggunakan model FCAPS untuk mengkarakterisasi ruang lingkup manajemen jaringan. Singkatan ini berasal dari rekomendasi M.3400 yang diterbitkan oleh International Telecommunications Union (ITU)†. FCAPS diperluas menjadi daftar lima aspek manajemen. Gambar 12.1 merangkum model.

Huruf	Keterangan
F	Fault detection and correction
C	Configuration and operation
A	Accounting and billing
P	Performance assessment and optimization
S	Security assurance and protection

Gambar 12.1 Model manajemen jaringan FCAPS.

Fault detection and correction

Deteksi kesalahan merupakan bagian utama dari aspek operasional manajemen jaringan. Seorang manajer memonitor peralatan jaringan untuk mendeteksi masalah, dan mengambil langkah-langkah yang tepat untuk memperbaiki masalah tersebut. Kemungkinan kesalahan termasuk kegagalan perangkat lunak (misalnya, sistem operasi crash pada server), kegagalan link (misalnya, seseorang secara tidak sengaja memotong serat optik), dan kegagalan peralatan (misalnya, catu daya gagal pada router).

Seringkali, pengguna melaporkan kegagalan dengan mengutip gejala tingkat tinggi seperti "Saya baru saja kehilangan akses ke disk bersama." Manajer harus menyelidiki untuk menentukan apakah masalahnya terletak pada perangkat lunak, keamanan (misalnya, kata sandi baru), server, atau tautan. Kami mengatakan bahwa seorang manajer melakukan analisis akar penyebab. Seringkali, seorang manajer dapat menentukan penyebabnya dengan menghubungkan banyak laporan. Misalnya, jika banyak pengguna di satu situs tiba-tiba mulai mengeluh bahwa berbagai layanan tidak tersedia, manajer mungkin curiga bahwa masalahnya terletak pada koneksi bersama yang digunakan semua layanan.

Configuration and operation

Tampaknya konfigurasi adalah aspek sepele dari manajemen jaringan karena konfigurasi hanya perlu dilakukan sekali — setelah dibuat, konfigurasi dapat disimpan sehingga perangkat secara otomatis menginstal konfigurasi selama reboot. Faktanya, konfigurasi rumit karena tiga alasan. Pertama, jaringan berisi banyak perangkat dan layanan, dan konfigurasi harus konsisten di semua perangkat.

Kedua, ketika peralatan dan layanan baru ditambahkan atau kebijakan berubah, manajer jaringan harus mempertimbangkan semua konfigurasi untuk memastikan seluruh jaringan menerapkan perubahan dengan benar. Ketiga, alat saat ini memungkinkan manajer untuk mengkonfigurasi perangkat individu dan protokol individu; tidak ada cara mudah untuk mengkonfigurasi satu set perangkat heterogen.

Accounting and billing

Di banyak intranet perusahaan, akuntansi dan penagihan adalah hal yang sepele. Korporasi membebankan biaya menjalankan jaringan ke rekening pusat, seperti biaya tenaga listrik atau layanan telepon. Namun, dalam jaringan ISP, akuntansi dan penagihan dapat menghabiskan lebih banyak waktu manajer daripada aspek manajemen lainnya. Misalnya, jika ISP menawarkan layanan berjenjang dengan batasan lalu lintas yang dapat dikirim, sistem harus memperhitungkan lalu lintas setiap pelanggan secara terpisah. Seringkali, perjanjian layanan menentukan bahwa biaya yang dibayarkan pelanggan bergantung pada ukuran seperti total byte yang dikirim pelanggan per hari. Dengan demikian, penting untuk mengukur semua lalu lintas pelanggan dan menyimpan catatan terperinci yang dapat digunakan untuk menghasilkan tagihan.

Performance assessment and optimization

Seorang manajer melakukan dua jenis penilaian kinerja: penilaian diagnostik untuk mendeteksi masalah dan inefisiensi dan penilaian tren yang memungkinkan manajer untuk mengantisipasi kebutuhan peningkatan kapasitas. Penilaian diagnostik mencari cara untuk memaksimalkan pemanfaatan jaringan yang ada. Misalnya, jika manajer menemukan jalur dengan pemanfaatan rendah, manajer mungkin mencari cara untuk mengalihkan lalu lintas ke jalur tersebut. Penilaian tren mencari cara untuk meningkatkan kinerja jaringan untuk memenuhi kebutuhan masa depan. Misalnya, sebagian besar manajer melihat pemanfaatan pada tautan antara organisasi mereka dan Internet, dan membuat rencana untuk meningkatkan kapasitas tautan ketika pemanfaatan rata-rata naik di atas 50%.

Security assurance and protection

Karena melintasi lapisan tumpukan protokol dan mencakup beberapa perangkat, keamanan adalah salah satu aspek yang paling sulit dari manajemen jaringan. Secara khusus, keamanan mengikuti analogi tautan terlemah: seluruh keamanan situs dapat dikompromikan jika konfigurasi salah pada satu perangkat. Selain itu, karena penyerang terus-menerus menemukan cara baru untuk merusak keamanan, jaringan yang aman pada waktu tertentu dapat dikompromikan di kemudian hari kecuali jika manajer membuat perubahan.

12.3 Contoh Elemen Jaringan

Sistem manajemen jaringan menggunakan istilah umum elemen jaringan untuk merujuk ke perangkat, sistem, atau mekanisme jaringan apa pun yang dapat dikelola. Meskipun banyak elemen jaringan terdiri dari perangkat fisik, definisi tersebut mencakup layanan seperti DNS. Gambar 12.2 mencantumkan contoh elemen jaringan.

Manageable Network Elements	
Layer 2 Switch	IP router
VLAN Switch	Firewall
Wireless Access Point	Digital Circuit (CSU/DSU)
Head-End DSL Modem	DSLAM
DHCP Server	DNS Server
Web Server	Load Balancer

Gambar 12.2 Contoh elemen jaringan yang harus dikelola.

Industri menggunakan istilah manajemen elemen untuk merujuk pada konfigurasi dan pengoperasian elemen jaringan individual. Sayangnya, sebagian besar alat yang tersedia hanya menyediakan manajemen elemen. Jadi, untuk membuat layanan ujung ke ujung, seorang manajer harus mengonfigurasi setiap elemen jaringan di sepanjang jalur. Misalnya, untuk membuat terowongan MPLS di beberapa router, seorang manajer harus mengkonfigurasi setiap router secara independen. Demikian pula, untuk menerapkan kebijakan di seluruh jaringan, seorang manajer harus mengonfigurasi setiap elemen.

Tentu saja, mudah bagi manusia untuk membuat kesalahan saat mengonfigurasi banyak perangkat, yang membuat manajemen elemen rentan terhadap kesalahan konfigurasi. Lebih penting lagi, untuk mendiagnosis kesalahan, seorang manajer harus memeriksa satu sistem pada satu waktu.

Poin Penting

Karena hanya mengizinkan seorang manajer untuk mengkonfigurasi, memantau, atau mengontrol satu elemen jaringan pada satu waktu, sistem manajemen elemen membutuhkan banyak tenaga dan rentan terhadap kesalahan.

12.4 Alat Manajemen Jaringan

Alat manajemen jaringan dapat diklasifikasikan ke dalam dua belas kategori yang mencirikan tujuan umumnya:

- Pengujian Lapisan Fisik
- Jangkauan dan Konektivitas
- Analisis Paket
- Penemuan Jaringan
- Interogasi Perangkat
- Pemantauan Acara
- Pemantauan Kinerja
- Analisis Aliran
- Rekayasa Perutean Dan Lalu Lintas
- Konfigurasi
- Penegakan Keamanan
- Perencanaan Jaringan

Pengujian lapisan fisik mencakup pengujian sensor pembawa yang ditemukan pada banyak kartu antarmuka LAN dan pengukur kekuatan nirkabel yang digunakan untuk mengukur kekuatan sinyal RF. Ping memberikan contoh terbaik dari alat jangkauan, dan banyak digunakan oleh manajer jaringan. Sebuah penganalisis paket, juga disebut penganalisis protokol, menangkap dan menampilkan paket atau statistik tentang paket; penganalisis Ethereal tersedia untuk diunduh. Alat penemuan jaringan menghasilkan peta jaringan dengan menyelidik perangkat.

Seringkali, seorang manajer menggunakan peta seperti itu untuk menemukan elemen di jaringan, dan kemudian menggunakan alat interogasi perangkat untuk mengakses setiap elemen. Alat pemantauan peristiwa menghasilkan peringatan — biasanya, seorang manajer mengonfigurasi perangkat untuk mengirim peringatan ketika ambang batas tertentu dilewati (misalnya, pemanfaatan tautan mencapai 80%), dan alat pemantauan menampilkan peringatan di tempat kerja manajer. Alat pemantauan kinerja merencanakan kinerja dari waktu ke waktu untuk membantu manajer melihat tren.

Alat analisis aliran, seperti penganalisis NetFlow, juga membantu manajer melihat tren. Alih-alih hanya melaporkan lalu lintas secara keseluruhan, penganalisis aliran dapat membantu manajer melihat perubahan jenis lalu lintas tertentu (misalnya, peningkatan lalu lintas VoIP).
Perutean, rekayasa lalu lintas, dan alat konfigurasi terkait. Masing-masing membantu seorang manajer mengendalikan elemen. Alat perutean mengontrol konfigurasi dan pemantauan protokol pembaruan perutean dan tabel penerusan yang dihasilkan dari perubahan perutean. Alat rekayasa lalu lintas fokus pada konfigurasi dan pemantauan terowongan MPLS dan parameter QoS terkait. Alat konfigurasi tujuan umum memungkinkan manajer untuk menginstal atau mengubah konfigurasi dalam elemen. Secara khusus, beberapa alat konfigurasi mengotomatiskan tugas berulang membuat perubahan dalam satu set elemen (biasanya identik).

Misalnya, jika aturan firewall berubah dan situs memiliki beberapa firewall, alat konfigurasi otomatis (seringkali skrip Perl) dapat menginstal perubahan yang sama di masing-masing firewall. Banyak alat keamanan yang ada, dan mengontrol berbagai elemen keamanan. Beberapa alat keamanan memungkinkan manajer untuk menentukan kebijakan, dan alat tersebut mencoba mengonfigurasi perangkat untuk menerapkan kebijakan atau mencoba mengukur perangkat untuk memastikan bahwa kebijakan tersebut berlaku. Manajer dapat menggunakan alat keamanan lain untuk menguji keamanan — alat tersebut mencoba menyerang perangkat atau layanan, dan melaporkan kepada manajer apakah serangan itu berhasil. Perencanaan jaringan itu kompleks, dan alat perencanaan termasuk yang paling canggih. Misalnya, ada alat yang menjalankan algoritme pemrograman linier untuk membantu manajer mengoptimalkan arsitektur jaringan atau merencanakan manajemen lalu lintas. Alat juga ada yang membantu manajer menilai kelemahan (misalnya, mengidentifikasi tempat di jaringan di mana dua atau lebih kegagalan perangkat keras akan memutuskan pengguna dari Internet).

Poin Penting

Ada berbagai macam alat yang membantu manajer mengonfigurasi, mengukur, mendiagnosis, dan menganalisis jaringan.

12.5 Aplikasi Manajemen Jaringan

Sebagian besar alat yang dijelaskan di atas beroperasi melalui jaringan. Artinya, seorang manajer tetap berada di satu lokasi dan menggunakan teknologi jaringan untuk berkomunikasi dengan elemen jaringan tertentu. Anehnya, manajemen jaringan tidak didefinisikan sebagai bagian integral dari protokol lapisan rendah. Sebaliknya, protokol yang digunakan untuk memantau dan mengontrol perangkat jaringan beroperasi pada tingkat aplikasi. Ketika seorang manajer perlu berinteraksi dengan perangkat keras tertentu, manajer menjalankan program aplikasi yang bertindak sebagai klien, dan program aplikasi pada perangkat jaringan bertindak sebagai server. Klien dan server menggunakan protokol transport konvensional seperti UDP atau TCP untuk berinteraksi. Selain itu, alih-alih membangun jaringan terpisah, sebagian besar manajer mengirim lalu lintas manajemen melalui jaringan produksi.

Untuk menghindari kebingungan antara program aplikasi yang dipanggil pengguna dan aplikasi yang disediakan untuk manajer jaringan, sistem manajemen jaringan menghindari istilah klien dan server. Sebaliknya, aplikasi klien yang berjalan di komputer manajer disebut manajer, dan server yang berjalan di perangkat jaringan disebut agen.

Menggunakan protokol transport konvensional untuk membawa lalu lintas manajemen mungkin tampak tidak efektif karena kegagalan baik pada protokol atau perangkat keras yang mendasarinya dapat mencegah paket dari perjalanan ke atau dari perangkat, sehingga tidak mungkin untuk mengontrol perangkat saat terjadi kegagalan. Beberapa operator jaringan memasang perangkat keras terpisah untuk menangani pengelolaan perangkat yang sangat kritis (misalnya, modem dialup terpasang langsung ke router berkecepatan tinggi sebagai cadangan untuk digunakan manajer jika jaringan utama tidak dapat dilewati). Dalam praktiknya, sistem seperti itu jarang diperlukan. Menggunakan protokol aplikasi untuk manajemen jaringan berfungsi dengan baik karena dua alasan. Pertama, dalam kasus di mana kegagalan perangkat keras mencegah komunikasi, seorang manajer dapat berkomunikasi dengan perangkat yang tetap berfungsi, dan menggunakan keberhasilan atau kegagalan untuk membantu menemukan masalah. Kedua, menggunakan protokol transport konvensional berarti paket manajer akan tunduk pada kondisi yang sama seperti lalu lintas normal. Jadi, jika penundaannya tinggi, manajer akan segera mengetahuinya.

12.6 Protokol Manajemen Jaringan Sederhana

Protokol standar yang digunakan untuk manajemen jaringan dikenal sebagai Simple Network Management Protocol (SNMP); standar saat ini adalah versi 3, tertulis SNMPv3. Protokol SNMP mendefinisikan dengan tepat bagaimana seorang manajer berkomunikasi dengan agen. Misalnya, SNMP mendefinisikan format permintaan yang dikirim manajer ke agen dan format balasan yang dikembalikan agen. Selain itu, SNMP mendefinisikan arti yang tepat dari setiap kemungkinan permintaan dan balasan. Secara khusus, SNMP menetapkan bahwa pesan SNMP dikodekan menggunakan standar yang dikenal sebagai Notasi Sintaks Abstrak.1 (ASN.1).

Meskipun detail lengkap penyandian ASN.1 berada di luar cakupan teks ini, contoh sederhana akan membantu menjelaskan penyandian: pertimbangkan untuk mengirim bilangan bulat antara agen dan manajer. Untuk mengakomodasi nilai yang besar tanpa membuang ruang pada setiap transfer, ASN.1 menggunakan kombinasi panjang dan nilai untuk setiap objek yang ditransfer. Misalnya, bilangan bulat antara 0 dan 255 dapat ditransfer dalam satu oktet. Bilangan bulat dalam rentang 256 hingga 65535 membutuhkan dua oktet, sedangkan bilangan bulat yang lebih besar membutuhkan tiga atau lebih oktet. Untuk mengkodekan bilangan bulat, ASN.1 mengirimkan sepasang nilai: panjang, L, diikuti oleh L oktet yang berisi bilangan bulat. Untuk mengizinkan pengkodean bilangan bulat besar yang

sewenang-wenang, ASN.1 juga memungkinkan panjang untuk menempati lebih dari satu oktet; panjang diperpanjang biasanya tidak diperlukan untuk bilangan bulat yang digunakan dengan SNMP. Gambar 12.3 mengilustrasikan pengkodean.

Decimal Integer	Hexadecimal Equivalent	Length Byte	Bytes Of Value (in hex)
27	1B	01	1B
792	318	02	03 18
24,567	5FF7	02	5F F7
190,345	2E789	03	02 E7 89

Gambar 12.3 Contoh pengkodean ASN.1 untuk bilangan bulat.

12.7 Paradigma Fetch-Store SNMP

Protokol SNMP tidak mendefinisikan sekumpulan besar perintah. Sebaliknya, protokol menggunakan paradigma fetch-store di mana ada dua operasi dasar: fetch, digunakan untuk mendapatkan nilai dari perangkat, dan store, digunakan untuk menetapkan nilai dalam perangkat. Setiap objek yang dapat diambil atau disimpan diberi nama yang unik; perintah yang menentukan operasi pengambilan atau penyimpanan harus menentukan nama objek.

Harus jelas bagaimana operasi pengambilan dapat digunakan untuk memantau perangkat atau memperoleh statusnya: sekumpulan objek status harus didefinisikan dan diberi nama. Untuk mendapatkan informasi status, seorang manajer mengambil nilai yang terkait dengan objek yang diberikan. Misalnya, sebuah objek dapat didefinisikan yang menghitung jumlah bingkai yang dibuang perangkat karena checksum bingkai salah. Perangkat harus dirancang untuk meningkatkan penghitung setiap kali kesalahan checksum terdeteksi. Manajer dapat menggunakan SNMP untuk mengambil nilai yang terkait dengan penghitung untuk menentukan apakah terjadi kesalahan checksum. Menggunakan paradigma fetch-store untuk mengontrol perangkat mungkin tidak terlihat jelas; operasi kontrol didefinisikan sebagai efek samping dari penyimpanan ke dalam suatu objek. Misalnya, SNMP tidak menyertakan perintah terpisah untuk mengatur ulang penghitung kesalahan checksum atau untuk mem-boot ulang perangkat. Dalam kasus penghitung kesalahan checksum, menyimpan nol ke dalam objek adalah intuitif karena itu mengatur ulang penghitung ke nol. Untuk operasi seperti reboot, bagaimanapun, agen SNMP harus diprogram untuk menafsirkan permintaan penyimpanan dan untuk menjalankan urutan operasi yang benar untuk mencapai efek yang diinginkan. Dengan demikian, perangkat lunak SNMP mungkin mendefinisikan objek reboot, dan menentukan bahwa menyimpan nol ke dalam objek akan menyebabkan sistem melakukan boot ulang. Tentu saja, objek SNMP adalah virtual dalam arti bahwa perangkat yang mendasarinya tidak mengimplementasikannya secara langsung. Sebagai gantinya, agen menerima permintaan dan melakukan tindakan yang sesuai dengan setiap operasi pengambilan atau penyimpanan. Untuk meringkas: SNMP menggunakan paradigma fetch-store untuk interaksi antara manajer dan agen. Manajer mengambil nilai untuk menentukan status perangkat; operasi yang mengontrol perangkat didefinisikan sebagai efek samping dari penyimpanan ke dalam objek.

12.8 SNMP MIB dan Nama Objek

Setiap objek yang memiliki akses SNMP harus didefinisikan dan diberi nama yang unik. Lebih lanjut, program manajer dan agen harus menyetujui nama dan arti dari operasi pengambilan dan penyimpanan. Secara kolektif, kumpulan semua objek yang dapat diakses SNMP dikenal sebagai Management Information Base (MIB). Faktanya, definisi MIB tidak terkait langsung dengan SNMP. Sebaliknya, standar SNMP hanya menentukan format pesan dan menjelaskan bagaimana pesan dikodekan; standar terpisah menentukan variabel MIB bersama dengan arti operasi pengambilan dan penyimpanan pada setiap variabel. Bahkan, dokumen standar terpisah menentukan variabel MIB untuk setiap jenis perangkat.

Objek dalam MIB didefinisikan dengan skema penamaan ASN1, yang memberikan setiap objek awalan panjang yang menjamin nama akan unik. Misalnya, bilangan bulat yang menghitung jumlah datagram IP yang diterima perangkat diberi nama:

iso.org.dod.internet.mgmt.mib.ip.ipInReceives

Selanjutnya, ketika nama objek direpresentasikan dalam pesan SNMP, setiap bagian dari nama tersebut diberi bilangan bulat. Jadi, dalam pesan SNMP, nama ipInReceives adalah:

1.3.6.1.2.1.4.3

12.9 Variasi Variabel MIB

Karena SNMP tidak menentukan satu set variabel MIB, desainnya fleksibel. Variabel MIB baru dapat didefinisikan dan distandarisasi sesuai kebutuhan, tanpa mengubah protokol dasar. Lebih penting lagi, pemisahan protokol komunikasi dari definisi objek memungkinkan setiap grup untuk mendefinisikan variabel MIB, sesuai kebutuhan. Misalnya, ketika protokol baru dirancang, grup yang membuat protokol dapat menentukan variabel MIB yang digunakan untuk memantau dan mengontrol perangkat lunak protokol. Demikian pula, ketika grup membuat perangkat keras baru, grup dapat menentukan variabel MIB yang digunakan untuk memantau dan mengontrol perangkat.

Seperti yang dimaksudkan oleh perancang asli, banyak set variabel MIB telah dibuat. Misalnya, ada variabel MIB yang sesuai dengan protokol seperti UDP, TCP, IP, dan ARP, serta variabel MIB untuk perangkat keras jaringan seperti Ethernet. Selain itu, grup telah menetapkan MIB untuk perangkat keras seperti router, sakelar, modem, dan printer.

12.10 Variabel MIB yang Sesuai dengan Array

Selain variabel sederhana seperti bilangan bulat yang sesuai dengan penghitung, MIB dapat menyertakan variabel yang sesuai dengan tabel atau larik. Definisi tersebut berguna karena sesuai dengan implementasi informasi dalam sistem komputer. Misalnya, pertimbangkan tabel penerusan IP. Dalam sebagian besar implementasi, tabel penerusan dapat dilihat sebagai larik entri, di mana setiap entri berisi alamat tujuan dan hop berikutnya yang digunakan untuk mencapai alamat tersebut.

Tidak seperti bahasa pemrograman konvensional, ASN.1 tidak menyertakan operasi indeks. Sebagai gantinya, referensi yang diindeks bersifat implisit — pengirim harus tahu bahwa objek yang direferensikan adalah tabel, dan harus menambahkan informasi pengindeksan ke nama objek. Misalnya, variabel MIB:

standard MIB prefix.ip.ipRoutingTable

sesuai dengan tabel penerusan IP, setiap entri berisi beberapa bidang. Secara konseptual, tabel diindeks oleh alamat IP tujuan. Untuk mendapatkan nilai bidang tertentu dalam entri, manajer menentukan nama formulir:

standard MIB prefix.ip.ipRoutingTable.ipRouteEntry.field.IPdestaddr

di mana bidang sesuai dengan salah satu bidang entri yang valid, dan IPdestaddr adalah alamat IP 4 oktet yang digunakan sebagai indeks. Misalnya, bidang ipRouteNextHop sesuai dengan hop berikutnya dalam sebuah entri. Ketika dikonversi ke representasi integer, permintaan untuk hop berikutnya menjadi:

1.3.6.1.2.1.4.21.1.7.destination

di mana 1.3.6.1.2.1 adalah awalan MIB standar, 4 adalah kode untuk ip, 21 adalah kode untuk ipRoutingTable, 1 adalah kode untuk ipRouteEntry, 7 adalah kode untuk bidang ipRouteNextHop, dan tujuan adalah nilai numerik untuk Alamat IP suatu tujuan. Untuk meringkas: Meskipun ASN.1 tidak menyediakan mekanisme untuk pengindeksan, variabel MIB dapat berhubungan dengan tabel atau array. Untuk meniru tabel atau larik dengan variabel ASN1, indeks untuk entri dikodekan dengan menambahkannya ke nama variabel; ketika perangkat lunak agen menemukan nama yang sesuai dengan tabel, perangkat lunak mengekstrak dan menggunakan informasi indeks untuk memilih entri tabel yang benar.

12.11 Ringkasan

Manajer jaringan adalah orang yang memantau dan mengontrol sistem perangkat keras dan perangkat lunak yang membentuk intranet. Model FCAPS mendefinisikan lima aspek dasar manajemen jaringan menjadi deteksi kesalahan, konfigurasi, akuntansi, analisis kinerja, dan keamanan. Berbagai alat ada untuk membantu manajer dalam melakukan fungsi manajemen. Karena sebagian besar alat hanya menyediakan manajemen elemen, seorang manajer harus menangani tugas yang melintasi perangkat secara manual. Karena perangkat lunak manajemen jaringan menggunakan model client-server, perangkat lunak memerlukan dua komponen. Komponen yang berjalan di komputer manajer dan bertindak sebagai klien disebut manajer; komponen yang berjalan pada perangkat dalam jaringan dan bertindak sebagai server disebut agen.

Simple Network Management Protocol (SNMP) adalah protokol manajemen jaringan standar yang digunakan di Internet. SNMP mendefinisikan format dan makna pesan yang dipertukarkan oleh manajer dan agen. Alih-alih mendefinisikan banyak operasi, SNMP menggunakan paradigma fetch-store di mana seorang manajer mengirimkan permintaan untuk mengambil nilai dari atau menyimpan nilai ke dalam variabel. Semua operasi didefinisikan sebagai efek samping dari operasi toko. SNMP tidak mendefinisikan kumpulan variabel yang dapat digunakan. Sebaliknya, variabel dan artinya didefinisikan dalam standar yang terpisah, sehingga memungkinkan kelompok untuk mendefinisikan serangkaian variabel MIB yang berbeda untuk setiap perangkat keras atau protokol. Nama-nama variabel MIB diberi nama menggunakan standar ASN.1; semua variabel MIB memiliki nama ASN.1 yang panjang dan hierarkis, yang diterjemahkan ke representasi numerik yang lebih ringkas untuk transmisi. ASN.1 tidak menyertakan tipe data agregat seperti tabel atau larik, juga tidak menyertakan operator subskrip.

Sebagai gantinya, untuk membuat variabel MIB meniru tabel atau larik, ASN.1 memperluas nama variabel dengan menambahkan informasi indeks.

Latihan

1. Berikan contoh mekanisme protokol yang menyembunyikan kesalahan.
2. Jika pengguna mengeluh bahwa mereka tidak dapat mengakses layanan tertentu, aspek FCAPS mana yang berpotensi terlibat dalam keluhan tersebut?
3. Jika firewall tidak berfungsi, aspek FCAPS mana yang termasuk dalam situasi tersebut? Mengapa?
4. Temukan dua contoh elemen yang dapat dikelola selain yang tercantum dalam Gambar 12.2.
5. Jelaskan pengertian penganalisa protokol?
6. Apa alat analisis aliran membantu manajer memahami?
7. Istilah apa yang digunakan perangkat lunak manajemen jaringan alih-alih klien dan server?
8. ASN.1 mendefinisikan format yang tepat dari bilangan bulat. Mengapa standar ASN.1 tidak hanya menyatakan bahwa setiap bilangan bulat adalah nilai 32-bit?
9. Telah dikemukakan bahwa seseorang tidak boleh menggunakan jaringan untuk men-debug masalah dalam jaringan. Mengapa SNMP menggunakan jaringan yang sama dengan yang sedang di-debug?
10. Tulis sebuah program yang membaca bilangan bulat besar sembarang dalam desimal, mengkodekan bilangan bulat ke dalam format yang diilustrasikan pada Gambar 12.3, dan mencetak hasilnya.
11. Apa dua operasi dasar yang digunakan SNMP?
12. Unduh perangkat lunak pengelola SNMP gratis, dan coba hubungi perangkat seperti printer.
13. Apakah SNMP menentukan nama untuk setiap kemungkinan variabel MIB? Menjelaskan.
14. Apa keuntungan utama dari menambahkan informasi indeks ke nama daripada menggunakan array konvensional yang diindeks oleh bilangan bulat?
15. Baca tentang bagaimana ASN.1 mengkodekan nama dan nilai. Tulis program komputer untuk menyandikan dan mendekode nama ASN.1 seperti nama yang ditetapkan untuk ipInReceives.

Bab 13 Tren Teknologi dan Penggunaan Jaringan

Bab ini akan membahas tentang:

- Tren dalam teknologi jaringan, aplikasi, dan layanan
- Perkembangan terakhir teknologi internet serta penelitian jangka panjang

13.1 Kebutuhan Akan Layanan Internet yang Dapat Diskalakan

Dalam arti sempit, model komunikasi client-server berarti bahwa satu aplikasi (server) dimulai terlebih dahulu dan menunggu kontak dari aplikasi lain (klien). Dalam arti yang lebih luas, industri jaringan menggunakan istilah client-server untuk mengkarakterisasi arsitektur di mana banyak klien potensial terhubung ke satu server terpusat. Misalnya, perusahaan yang menjalankan server web dapat mengharapkan kontak dari pengguna yang sewenang-wenang. Kerugian dari server terpusat muncul dari kinerja yang dihasilkan: dengan meningkatnya jumlah klien, server (atau jaringan akses yang mengarah ke server) dengan cepat menjadi hambatan, terutama jika setiap klien mengunduh banyak byte konten.

Masalah bottleneck server dianggap sebagai salah satu batasan terpenting pada layanan Internet. Akibatnya, baik komunitas riset jaringan dan industri jaringan telah menyelidiki cara untuk menyediakan arsitektur dan teknologi yang memungkinkan layanan Internet untuk mengukur dan menggabungkan tren baru; berbagai pendekatan sedang digunakan. Bagian selanjutnya menjelaskan beberapa.

Poin Penting

Berbagai teknologi telah dirancang untuk memungkinkan layanan Internet untuk skala; meskipun pendekatannya sangat berbeda, masing-masing berguna dalam beberapa kasus.

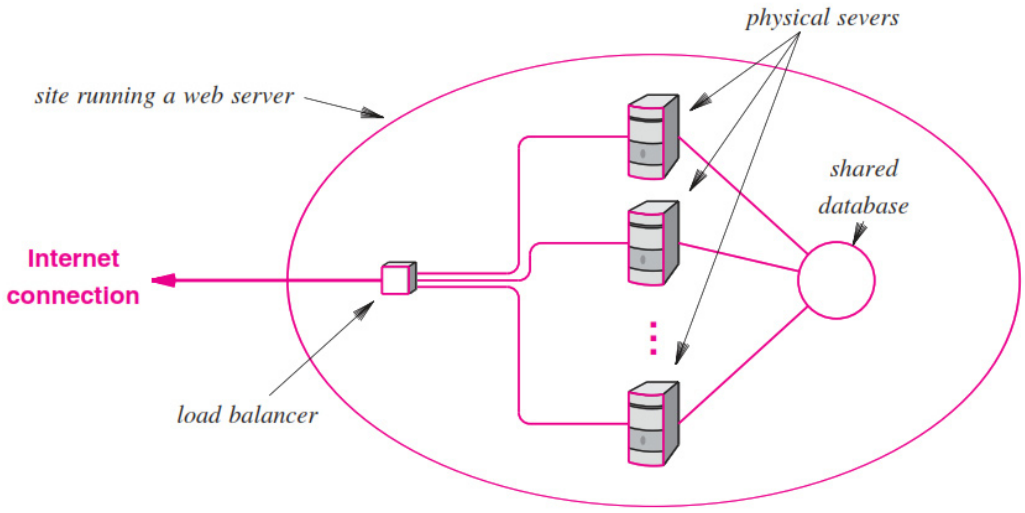
13.2 Penyimpanan Konten (Akamai)

Salah satu teknologi penskalaan pertama yang berfokus pada caching konten web. Misalnya, ISP sering memiliki cache yang menyimpan salinan setiap halaman web statis (yaitu, halaman yang kontennya tidak berubah dengan cepat). Jika N pengguna ISP mengambil halaman yang sama, hanya satu permintaan yang perlu dikirim ke server asal; N-1 permintaan dapat dipenuhi dari cache. Perusahaan seperti Akamai telah memperluas ide caching dengan menawarkan layanan caching terdistribusi. Akamai memiliki satu set server yang terletak di seluruh Internet, dan organisasi dapat membuat kontrak dengan Akamai untuk memuat cache Akamai dengan konten terlebih dahulu. Untuk memastikan bahwa cache tetap terkini, pelanggan organisasi dapat memperbarui cache Akamai secara berkala. Pengunjung situs web organisasi memperoleh banyak konten dari cache Akamai terdekat daripada dari server pusat organisasi. Akibatnya, beban di server pusat berkurang.

13.3 Penyeimbang Beban Web

Karena pemanfaatannya tinggi dan banyak bisnis ritel bergantung pada Web untuk penjualan langsung ke pelanggan, pengoptimalan server web telah mendapat banyak perhatian. Salah satu mekanisme menarik yang digunakan untuk membangun situs web besar dikenal sebagai penyeimbang beban. Penyeimbang beban memungkinkan situs memiliki beberapa komputer yang masing-masing menjalankan server web yang identik, dan mendistribusikan permintaan masuk di antara server fisik. Gambar 13.1 mengilustrasikan arsitekturnya.

Penyeimbang beban memeriksa setiap permintaan HTTP yang masuk dan mengirimkan permintaan ke salah satu server. Penyeimbang beban mengingat permintaan terbaru, dan mengarahkan semua permintaan dari sumber tertentu ke server fisik yang sama. Untuk memastikan bahwa semua server mengembalikan jawaban yang sama untuk sebuah permintaan, server menggunakan sistem database bersama yang umum. Jadi, jika pelanggan memesan, semua salinan server web akan dapat mengakses pesanan.



Gambar 13.1 Ilustrasi penyeimbang beban yang digunakan untuk situs web skala besar.

13.4 Virtualisasi Server

Sentuhan lain pada skalabilitas muncul dari virtualisasi server. Motivasi dimulai dengan pengamatan: banyak situs menjalankan beberapa server (misalnya, server email, server web, dan server database). Dalam arsitektur konvensional, setiap server harus ditempatkan pada komputer fisik. Masalah kinerja dapat terjadi karena server yang berjalan di komputer A semuanya sibuk, tetapi server yang berjalan di komputer B menganggur.

Virtualisasi server memecahkan masalah dengan memungkinkan manajer untuk memindahkan server dari satu komputer ke komputer lain kapan saja. Tentu banyak detail teknis yang harus ditangani, termasuk perubahan forwarding. Namun, idenya sederhana: jalankan server di bawah sistem Mesin Virtual (VM) yang mendukung migrasi proses. Jika komputer fisik tertentu menjadi kewalahan, seorang manajer dapat memindahkan satu atau lebih proses ke komputer lain.

13.5 Komunikasi Peer-To-Peer

Pada 1990-an, beberapa kelompok bereksperimen dengan teknik umum untuk meningkatkan kecepatan pengunduhan file. Alih-alih mengambil file lengkap dari server pusat, klien mengambil potongan file individual. Selanjutnya, potongan file ditempatkan di server di seluruh Internet. Setiap kali klien membutuhkan sepotong file, klien memilih untuk mengambil salinan dari server yang terdekat. Untuk menambah jumlah lokasi di mana sepotong dapat ditemukan, setiap klien yang memperoleh sepotong file setuju untuk bertindak sebagai server yang memungkinkan klien lain untuk mendapatkan potongan tersebut. Pendekatan ini dikenal sebagai arsitektur peer-to-peer (p2p).

Beberapa sistem p2p yang paling terkenal telah dibuat untuk memungkinkan berbagi file musik. Misalnya, Napster dan Kazaa sama-sama mengikuti pendekatan p2p, dan masing-masing populer di kalangan remaja. Tentu saja, pengguna biasa tidak peduli dengan teknologi yang mendasarinya — mereka hanya peduli bahwa sistem memungkinkan mereka untuk mendapatkan salinan file musik. Banyak pengguna tidak menyadari bahwa ketika mereka menggunakan sistem p2p, komputer mereka setuju untuk menyebarkan file ke orang lain.

13.6 Pusat Data Terdistribusi dan Replikasi

Meskipun memuat cache konten, penyeimbang beban, virtualisasi server, dan arsitektur p2p masing-masing dapat meningkatkan skalabilitas server, beberapa situs memiliki begitu banyak lalu lintas sehingga diperlukan solusi lain: replikasi seluruh situs. Kami menggunakan istilah pusat data terdistribusi untuk mengkarakterisasi pendekatan. Sebagai contoh, pertimbangkan mesin pencari Google. Google menerima miliaran

kontak setiap hari. Untuk menangani beban tersebut, Google telah membuat beberapa pusat data, ditempatkan di berbagai lokasi geografis. Saat pengguna memasukkan nama domain www.google.com, pengguna diarahkan ke pusat data Google terdekat; pendekatan ini dapat dianggap sebagai bentuk penyeimbangan beban antar situs. Tentu saja, untuk memberikan layanan yang konsisten, Google harus memastikan bahwa pusat data tertentu mengembalikan hasil pencarian yang sama persis dengan pusat data lainnya.

13.7 Representasi Universal (XML)

Salah satu tren paling menarik dalam jaringan muncul dari adopsi luas Extensible Markup Language (XML). Awalnya, XML dirancang untuk menggabungkan struktur ke dalam dokumen web

sehingga dokumen dapat dipahami oleh banyak aplikasi. Alih-alih memperbaiki tag, XML memungkinkan pemrogram untuk memilih tag arbitrer, sehingga memungkinkan untuk memberi setiap bidang nama yang intuitif. Misalnya, seseorang dapat menganggap dokumen yang berisi tag <nama>, <jalan>, <kota>, <negara>, <kode_pos> menyertakan catatan alamat seseorang. Salah satu ide kunci di balik XML adalah kemampuannya untuk mengkodekan dokumen yang mendeskripsikan diri sendiri. Artinya, dokumen menyertakan lembar gaya yang menentukan struktur dokumen yang sah.

XML telah menjadi standar de facto untuk representasi, dan digunakan dalam berbagai cara baru yang tidak terduga dalam desain awal. Misalnya, XML digunakan pada antarmuka antara server web dan database, dan beberapa penyeimbang beban telah dibuat yang dapat mengurai XML. Selain itu, XML digunakan untuk mengontrol unduhan di perangkat seluler dan untuk mewakili spesifikasi yang digunakan oleh sistem manajemen jaringan.

13.8 Jejaring Sosial

Pada awal 2000-an, penggunaan Internet bergeser dari model konsumen ke salah satu interaksi sosial di antara rekan-rekan. Awalnya, sebagian besar informasi di Internet disediakan oleh produsen, organisasi seperti perusahaan media. Seorang pengguna individu mengkonsumsi informasi, tetapi tidak memproduksinya. Pada tahun 2000-an, situs-situs seperti Facebook, Myspace, dan YouTube muncul yang memungkinkan setiap pengguna membuat konten, yang berarti bahwa pengguna biasa mengunggah lebih banyak data.

Pergeseran dalam interaksi paling terlihat di antara pengguna yang lebih muda. Banyak remaja telah membuat blog atau berlangganan salah satu situs yang disebutkan di atas. Di AS, persentase yang tidak sepele dari pasangan yang baru menikah bertemu pasangan mereka melalui layanan online. Selain itu, penggunaan obrolan online dan bentuk komunikasi orang ke orang lainnya telah meningkat.

13.9 Mobilitas dan Jaringan Nirkabel

Komunikasi seluler adalah salah satu tren yang paling signifikan, dan pengguna berharap untuk terus terhubung ke Internet. Sebagian besar hotel menawarkan koneksi Internet kepada tamu mereka, dan maskapai penerbangan menawarkan layanan Internet di pesawat. Penulis baru-baru ini melakukan pelayaran, dan senang menemukan bahwa koneksi Internet di atas kapal bekerja dengan sangat baik sehingga dapat digunakan untuk panggilan telepon VoIP.

Permintaan untuk komunikasi seluler telah memicu minat pada teknologi nirkabel, dan banyak standar nirkabel telah dibuat. Teknologi 802.11n memberikan throughput yang lebih tinggi dari pendahulunya, 802.11b. Namun, perubahan paling signifikan telah terjadi di industri telepon seluler: telepon seluler akan segera diubah dari protokol lain ke IP. Secara khusus, begitu operator seluler mulai menggunakan WiMAX, seluruh sistem akan menjadi IP, yang berarti bahwa layanan seluler dan Internet telah menyatu. Ironisnya, sementara industri seluler telah mengadopsi IP sebagai strategi jangka panjang, teknologi yang dikenal sebagai IP seluler belum diadopsi oleh industri jaringan. Sebaliknya, sebagian besar pengguna seluler mengandalkan Wi-Fi sebagai teknologi akses lokal dan menggunakan perangkat lunak VPN untuk terhubung ke bisnis mereka.

13.10 Video Digital

Penyedia kabel menggantikan fasilitas transmisi analog dengan digital, dan akan segera mengirimkan konten dalam bentuk digital melalui jaringan paket. Faktanya, banyak penyedia menggunakan

IP sebagai protokol paket, dan istilah IPTV digunakan untuk teknologi tersebut. Menggunakan IP untuk video menciptakan peluang menarik. Pertama, televisi dan internet bertemu, sehingga mudah untuk menonton program televisi di komputer atau menggunakan televisi digital sebagai tampilan komputer. Selain itu, IP mempermudah penerapan video sesuai permintaan, di mana pengguna dapat mengakses konten saat diinginkan, mengontrol pemutaran dengan fungsi jeda dan mundur, dan merekam konten langsung untuk dilihat nanti.

13.11 Pengiriman Multicast

Meskipun multicasting di seluruh Internet belum menikmati banyak keberhasilan, perpindahan ke IPTV telah merangsang minat multicast. Motivasi muncul dari keinginan untuk mengoptimalkan penyampaian. Meskipun penyedia mungkin menawarkan ratusan saluran konten, pelanggan tertentu biasanya hanya memiliki beberapa televisi yang menampilkan konten pada waktu tertentu. Selain itu, beberapa saluran biasanya menarik sebagian besar pemirsa. IP multicast memungkinkan pelanggan untuk mendaftarkan minat dalam suatu program dengan bergabung dengan grup multicast untuk program tersebut. Pelanggan di lingkungan terhubung ke segmen LAN logis. Setelah pelanggan bergabung dengan grup, penyedia kabel mulai melakukan multicasting salinan program pada segmen LAN. Multicasting berlanjut selama salah satu pelanggan di segmen tersebut menonton program. Intinya adalah: Dengan multicasting IP, hanya satu salinan program televisi yang perlu dikirim melalui segmen LAN logis; multicasting suatu program berhenti setelah tidak ada lagi pelanggan yang menonton program tersebut.

13.12 Akses dan Peralihan Berkecepatan Lebih Tinggi

Di ujung teknologi akses Internet seperti DSL dan modem kabel memberikan kecepatan data beberapa megabit per detik, dua kali lipat lebih banyak throughput daripada koneksi telepon dialup. Di beberapa wilayah AS, penyedia layanan menawarkan Fiber To The Home (FTTH), yang meningkatkan potensi kecepatan data hingga gigabit per detik, tiga kali lipat melebihi DSL dan modem kabel. Sakelar Ethernet yang digunakan di pusat data perusahaan menyediakan 1 Gbps ke desktop. Tautan berkapasitas lebih tinggi beroperasi pada 10 Gbps, dan tampaknya kecepatannya akan meningkat hingga 40 Gbps. Kecepatan data tersebut cukup untuk mendukung video definisi tinggi.

13.13 Pengalihan Optik

Inti dari Internet, pertanyaan besarnya adalah: bagaimana kita dapat menggabungkan teknologi optik dan elektronik? Perangkat optik memungkinkan penyedia untuk membuat jalur cahaya ujung ke ujung yang beroperasi pada 10 Gbps, sering disebut lambda. Meskipun sebagian besar teknologi saat ini membutuhkan waktu yang lama (beberapa detik) untuk mengatur jalur cahaya tunggal, teknologi optik yang muncul menjanjikan untuk mengurangi waktu. Akibatnya, dimungkinkan untuk mengatur jalur cahaya dalam waktu kurang dari satu milidetik. Jika jalur cahaya dapat dibuat dengan cepat, bagaimana cara menggunakannya? Haruskah ISP menggunakan jalur cahaya untuk menghubungkan router dan kemudian menggunakan teknologi paket untuk akses? Haruskah ISP menyiapkan jalur cahaya setiap kali pengguna membentuk koneksi TCP? Pertanyaan-pertanyaan tersebut merupakan dasar untuk area penelitian yang penting; sebagian besar ISP besar yakin bahwa peralihan optik akan menjadi semakin penting.

13.14 Penggunaan Jaringan dalam Bisnis

Sebagian besar perusahaan besar mengandalkan jaringan komputer untuk semua aspek bisnis. Namun, jaringan mengubah bisnis dalam tiga cara. Pertama, ketersediaan teknologi RFID mengubah produksi, pengiriman, dan inventaris. Kedua, ketersediaan sakelar Layer 2 berkecepatan tinggi dan teknologi paket untuk suara dan video memungkinkan untuk menggantikan perjalanan dengan sistem telekonferensi video berkualitas tinggi. Ketiga, banyak bisnis beralih dari budaya perintah-dan-kontrol yang ketat ke gaya manajemen yang lebih kolaboratif di mana sebuah tim bekerja sama untuk membuat keputusan. Ketersediaan alat dan infrastruktur jaringan yang mendukung interaksi kelompok, seperti wiki, memungkinkan untuk berkolaborasi melalui jaringan.

13.15 Sensor Skala Besar dan Rumahan

Jaringan kabel dan nirkabel berbiaya rendah dan perangkat sensor berdaya rendah telah memungkinkan untuk membangun jaringan sensor besar dan menghubungkan jaringan tersebut ke Internet. Sensor digunakan untuk mengukur lingkungan (misalnya, memantau kualitas udara dan air atau mengumpulkan informasi cuaca), melacak pergerakan hewan liar, membantu petani memantau tanaman, memantau orang di gedung perkantoran, dan menilai lalu lintas di jalan raya. Salah satu penggunaan sensor yang sangat menarik melibatkan penggunaannya di bangunan tempat tinggal. Sudah dimungkinkan untuk memasang sensor yang mengukur suhu dan kelembaban, atau memantau rumah dari bahaya seperti asap dan karbon monoksida. Jaringan sensor rumah dapat dihubungkan ke Internet, memungkinkan pemilik untuk memantau rumah mereka saat bepergian†. Akan segera mungkin untuk mendapatkan perangkat sensor murah seperti sensor di setiap bola lampu atau sensor di setiap alat.

13.16 Jaringan Ad Hoc

Sejak hari-hari awal jaringan paket, militer AS telah mendanai penelitian tentang jaringan ad hoc yang mengatur diri sendiri. Yaitu, satu set stasiun nirkabel menemukan tetangga, memilih topologi, dan menetapkan perutean yang memungkinkan setiap stasiun menjangkau stasiun lainnya. Motivasi militer muncul dari operasi yang dibayangkan di mana tentara masing-masing membawa stasiun jaringan nirkabel, dan stasiun membentuk sistem komunikasi secara otomatis. Jaringan ad hoc menjadi penting di dunia sipil juga, terutama di daerah pedesaan dan negara berkembang. Di AS, petani menggunakan teknologi ad hoc untuk menghubungkan pertanian pedesaan ke Internet. Setiap petani mendirikan stasiun nirkabel (biasanya di gedung tinggi, seperti silo), dan stasiun setuju untuk meneruskan paket, sesuai kebutuhan. Di negara berkembang, jaringan ad hoc digunakan sebagai cara murah untuk menyediakan akses Internet ke seluruh desa.

13.18 CPU Multi-Core Dan Prosesor Jaringan

Kecepatan data yang tinggi menimbulkan masalah bagi produsen peralatan jaringan: bagaimana membangun sistem yang dapat memproses paket dengan cepat. Router kelas atas harus menangani paket yang tiba melalui antarmuka dengan kecepatan 10 Gbps. Chip tujuan khusus (ASIC) dapat digunakan, tetapi chip tersebut mahal dan membutuhkan waktu berbulan-bulan untuk merancang atau merevisinya. Prosesor konvensional cukup untuk perangkat jaringan kelas bawah seperti router nirkabel yang digunakan di rumah, tetapi tidak memiliki daya komputasi yang cukup untuk kecepatan data yang lebih tinggi. Vendor chip menawarkan dua solusi. Pertama, vendor chip menawarkan CPU

multi-core yang masing-masing berisi beberapa prosesor. Satu pendekatan mendistribusikan paket yang masuk di antara N core, yang berarti bahwa satu core hanya menangani 1/N paket. Kedua, vendor chip menawarkan prosesor jaringan. Kita dapat menganggap prosesor jaringan sebagai CPU cepat yang mencakup banyak inti ditambah instruksi khusus untuk menangani tugas pemrosesan paket umum dengan kecepatan tinggi. Intinya adalah bahwa vendor peralatan menggunakan lebih banyak prosesor yang dapat diprogram dalam peralatan mereka.

13.18 IPv6

Tidak ada daftar tren jaringan yang lengkap tanpa menyebutkan IPv6. Pekerjaan aslinya dimulai pada tahun 1993, dan desainnya telah ada selama bertahun-tahun. Awalnya, para pendukung mengklaim bahwa IPv6 diperlukan karena IPv4 tidak dapat menangani audio atau video, tidak aman, dan akan kehabisan alamat. Setiap tahun sejak penciptaan IPv6, berbagai kalangan dari akademisi dan industri telah memprediksi kehancuran IPv4 dan kebangkitan IPv6. Sementara itu, IPv4 telah beradaptasi, menjalankan aplikasi multimedia, dan memiliki keamanan sebanyak IPv6. Pengalamatan NAT dan CIDR telah memperluas kemampuan pengalamatan IPv4. IPv4 berlanjut sebagai protokol dasar Internet. Beberapa operator seluler, terutama di Asia, melihat IPv6 sebagai cara untuk mengizinkan pengalamatan IP pada ponsel, tetapi operator juga memiliki opsi untuk merancang skema pengalamatan lapisan 2. Pada titik ini, tidak ada alasan teknis untuk mengadopsi IPv6. Faktanya, karena pemrosesan paket IPv6 menimbulkan lebih banyak overhead, pindah ke IPv6 dapat membatasi kecepatan pengiriman paket. Dengan demikian, motivasi untuk IPv6 menjadi tradeoff ekonomi: adalah mungkin untuk menghapus NAT dari Internet dan memiliki pengalamatan ujung ke ujung, tetapi melakukannya berarti mengganti semua peralatan jaringan dan perangkat lunak. Sulit untuk mengatakan kapan pelanggan akan memutuskan bahwa biaya tinggi membenarkan perubahan.

13.19 Ringkasan

Internet terus berkembang. Aplikasi dan teknologi baru diciptakan terus-menerus. Tren saat ini mencakup teknologi untuk kecepatan yang lebih tinggi, peningkatan mobilitas, dan skalabilitas. Dalam hal aplikasi Internet, trennya mengarah ke jejaring sosial. Selain itu, teknologi baru telah memungkinkan pengguna rata-rata untuk menghasilkan konten. Bisnis menggunakan alat yang mendukung manajemen kolaboratif, dan menggunakan sistem telekonferensi kelas atas untuk menggantikan perjalanan.

Latihan

1. Jelaskan bagaimana cache konten memungkinkan Internet untuk diskalakan.
2. Di mana penyeimbang beban digunakan?
3. Situs web dengan N server fisik mungkin tidak dapat memproses N kali lebih banyak permintaan per detik karena sumber daya bersama dapat menimbulkan hambatan. Sebutkan dua sumber daya yang digunakan bersama.
4. Selain mengizinkan penskalaan, virtualisasi server juga memungkinkan situs menghemat energi pada saat beban rendah (misalnya, pada akhir pekan). Jelaskan bagaimana.
5. Dengan penggunaan umum apa komputasi peer-to-peer sering dikaitkan?
6. Apakah pendekatan pusat data terdistribusi masuk akal untuk bisnis di mana setiap permintaan web memerlukan akses ke database pusat? Mengapa atau mengapa tidak?

7. Sebutkan tiga contoh aplikasi jejaring sosial.
8. Bagaimana Internet dan sistem telepon seluler berkumpul?
9. Apa yang ditawarkan video digital kepada pengguna?

Daftar Pustaka

A. Kershenbaum, Telecommunications Network Design Algorithms, McGraw-Hill, 1993.

Andi. Windows Server 2003. Enterprise Edition, Andi Offset, Yogjakarta. 2006.

Arifin, Zainal. 2008 . Langkah Mudah Membangun Jaringan Komputer, Andi

Irawan, Budhi. Jaringan Komputer. Yogyakarta, Graha Ilmu, 2005

D. Bertsekas and R. Gallager, Data Networks, 2nd Edition, Prentice Hall, 1992.

D.E. McDysan and D.L. Spohn, ATM Theory and Application, McGraw-Hill, 1995

Daryanto. 2003. Pengetahuan Dasar Ilmu Komputer. Rama Widya. Bandung.

Daryanto. 2004. Konsep Jaringan Komputer dan Pengembangan. Salemba. Infotek. Jakarta.

J. Kurose and K. Ross, Computer Networking: A Top Down Approach Using the Internet, Addison-Wesley Computer Science, 6th Edition, 2013.

Kurniawan, Wiharso. 2007. Computer Starter Guide : Jaringan Komputer Yogyakarta : Penerbit Andi.

Kustanto dan Saputro, D. T. 2010. Membangun Server Internet dengan Mikrotik OS. Jakarta. Gaya Media.

Nugroho, Endro. 2009. Buku Pintar Jaringan Komputer. Modeoms. Yogjakarta.

Madcoms. 2009, Membangun Sistem Jaringan Komputer, Andi Offset, Yogyakarta.

Odlyzko, A. “Privacy, Economics and Price Discrimination on the Internet.” Unpublished white paper. http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf

Parker, D., and Nycum, S. “Computer Crime.” Comm of the ACM, v27 n4, Apr 1984, p313–321.

Rafiudin, Rahmat. Menguasai Security Unix. Jakarta, Elex Media Komputindo, 2007

Rubin, A. “Security Considerations for Remote Electronic Voting over the Internet.” *Proc Internet Policy Institute Workshop on Internet Voting*, Oct 2000.

Simarmata, Janner. Pengamanan Sistem Komputer. Yogyakarta, Andi, 2006.

Sopandi, Dede. Instalasi dan Konfigurasi Jaringan Komputer. Bandung, Informatika, 2006

Statowski, Mariusz..”The Principles of Network Security Design”. 2007

Stoll, Clifford. 1988. "Stalking the Wily Hacker," Communications of the ACM, Vol. 31, No. 5, May, pp. 484–497.

Supandi, Dede. 2006. Instalasi dan konfigurasi jaringan Komputer. Informatika. Bandung, 2006

Sutabri, Tata. 2003. Sistem Informasi Manajemen. Andi Offset. Jogjakarta.

Sutedjo Dharma Oetomo, Budi. Konsep dan Perancangan Jaringan Komputer. Yogyakarta, Andi, 2003

U.S. Air Force. “Operational Risk Management.” Air Force Policy Directive, 90-9, 1 Apr 2000

Wagito, 2007, Jaringan Komputer : Teori dan Implementasi Berbasis Linux, Gava Media, Yogyakarta.

Wahidin, 2007. Jaringan Komputer untuk orang Awam. Maxicom. Palembang.

Weippl, Edgar R. (2005). Security in E-Learning-An Abstraction Based Approach. United States of America: Springer

Winarno Sugeng, 2006. Jaringan Komputer dengan TCP/IP. Bandung : Penerbit Informatika.

U. Black, ATM: Foundation for Broadband Networks, Prentice Hall, 1995.

Yani, Ahmad. 2008. Panduan Membangun Jaringan Komputer. Jakarta: Kawan Pustaka

Yudho, Satrio. 2013. Pengantar Sistem Operasi Komputer, Graha Ilmu