

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
TRUNG TÂM ĐÀO TẠO BƯU CHÍNH VIỄN THÔNG 2

TÀI LIỆU THAM KHẢO

TCP/IP

CĂN BẢN

*(dành cho Học viên khóa học “TCP/IP căn bản”
bằng hình thức đào tạo e-Learning)*

GIẢNG VIÊN:

Th.S Nguyễn Xuân Khánh

(Lưu hành nội bộ)

TP. HCM, tháng 11/2004

Lời nói đầu

Theo xu hướng phát triển mạng viễn thông lên NGN dựa trên nền tảng IP thì việc phổ cập cho cán bộ công nhân viên của Tổng công ty Bưu chính Viễn thông Việt Nam những kiến thức cơ bản về bộ giao thức TCP/IP trở thành một nhu cầu rất cần thiết.

Tài liệu tham khảo “TCP/IP căn bản” giới thiệu các nội dung căn bản của bộ giao thức TCP/IP. Bố cục của tài liệu được trình bày theo mô hình tham khảo TCP/IP. Mặc dù không được phân định rõ ràng nhưng người đọc có thể thấy qua từng chương các phân lớp của mô hình tham khảo này. Chương 1 giới thiệu về TCP/IP, chương 2 – lớp truy cập mạng, chương 3, 4, 6, 7 – lớp Internet, chương 5 – lớp vận chuyển. Và từ chương 8 trở đi trình bày các giao thức ở lớp ứng dụng.

Tài liệu này được trình bày theo một trình tự thống nhất cho tất cả các chương như sau: phần đầu sẽ nêu tóm tắt các **nội dung chính** sẽ được trình bày trong chương, tiếp theo là **mục tiêu** mà tác giả muốn truyền đạt tới người đọc, cuối cùng là phần **tóm tắt** và **thực hành (nếu có)**. Ngoài ra, còn có phần **thông tin thêm** cung cấp những thông tin bổ sung khác có liên quan đến bài học.

Đây là tài liệu *lưu hành nội bộ*, dùng riêng cho học viên của khóa học “**TCP/IP căn bản**” – khóa học thử nghiệm hình thức đào tạo e-Learning đầu tiên do Trung tâm Đào tạo Bưu chính Viễn thông 2 phối hợp với Trung tâm Đào tạo Bưu chính Viễn thông 1 tổ chức. Tài liệu này được dịch và biên soạn lại dựa trên nội dung cuốn sách nguyên bản tiếng Anh:

“Teach Yourself TCP/IP in 24 Hours”, Third Edition

Tác giả: Joe Casad

Nhà xuất bản: Sams PublishingPub

Ngày: 03/09/2003

Số ISBN: 0-672-32565-9

Số trang: 450

Trong quá trình dịch thuật và biên soạn, nhóm tác giả đã có nhiều cố gắng để đảm bảo về mặt chất lượng nội dung cũng như hình thức trình bày của tài liệu, nhưng chắc chắn còn rất nhiều điều thiếu sót, bất cập. Chúng tôi rất mong nhận được những ý kiến đóng góp xây dựng về cuốn tài liệu này qua địa chỉ:

pttc2_elearning@yahoo.com

Xin chân thành cảm ơn.

TP. HCM, tháng 10/2004

Nhóm tác giả

CHỦ BIÊN:

Th.S Nguyễn Xuân Khánh – Trường khoa Viễn thông 2

Học viện Công nghệ Bưu chính Viễn thông.

Các cộng tác viên:

T.T. Nguyễn Quang Trung

Trương Hoàng Khanh

Nguyễn Sỹ Hoàng Anh

Lê Thị Mỹ Linh

Nguyễn Ngọc Trâm Anh

Nguyễn Ngọc Chân

Võ Ngọc Quang

Nguyễn Đức Thắng

MỤC LỤC

Trang

Chương 1	TCP/IP làm việc như thế nào	1
1.1	Hệ thống giao thức TCP/IP	2
1.2	TCP/IP và mô hình OSI	4
1.3	Các gói dữ liệu	6
1.4	Xem qua hoạt động mạng TCP/IP	7
Chương 2	Lớp truy cập mạng	10
2.1	Các giao thức và phần cứng	11
2.2	Lớp truy cập mạng và mô hình OSI	12
2.3	Kiến trúc mạng	13
2.4	Đánh địa chỉ vật lý	14
2.5	Cấu trúc khung	15
2.6	Các công nghệ LAN	16
2.6.1	Ethernet	17
2.6.2	Token Ring	19
2.6.3	FDDI	20
2.7	Các kỹ thuật truy cập mạng khác	20
Chương 3	Lớp Internet	21
3.1	Đánh địa chỉ và phân phối	22
3.2	Giao thức Internet (IP)	24
3.2.1	Các trường tiêu đề IP	26
3.2.2	Đánh địa chỉ IP	28
3.2.3	Chuyển một địa chỉ nhị phân 32 bit sang dạng chấm thập phân	30
3.2.4	Chuyển một số thập phân sang một octet nhị phân	32
3.2.5	Các lớp D và E	34
3.2.6	Các địa chỉ IP đặc biệt	34
3.3	Giao thức phân giải địa chỉ (ARP)	35
3.4	Giao thức phân giải địa chỉ ngược (RARP)	36
3.5	Giao thức thông điệp điều khiển Internet (ICMP)	37
Chương 4	Phân mạng con	39
4.1	Các mạng con trong TCP/IP	40
4.2	Chuyển đổi một Subnet Mask sang dạng chấm thập phân	43
4.3	Làm việc với các mạng con	45
4.4	Định tuyến tên miền Internet không phân lớp	50
Chương 5	Lớp vận chuyển	51
5.1	Giới thiệu về lớp vận chuyển	52
5.2	Các khái niệm lớp vận chuyển	53
5.2.1	Giao thức hướng kết nối và không kết nối	53

5.2.2	Cổng và socket	55
5.2.3	Đa hợp/ Giải đa hợp.....	59
5.3	TCP và UDP.....	60
5.3.1	TCP: Giao thức truyền tải hướng kết nối	61
5.3.2	UDP: Giao thức truyền tải không kết nối	67
5.4	Một lưu ý về tường lửa (firewall)	69
Chương 6 Phần cứng mạng		71
6.1	Mạng được chia nhỏ	72
6.1.1	Bridge.....	73
6.1.2	Hub	74
6.1.3	Switch	75
6.1.4	Router	77
6.2	Định tuyến trong TCP/IP	78
6.2.1	Thế nào là một bộ định tuyến?	78
6.2.2	Giới thiệu về định tuyến	80
6.2.3	Bảng định tuyến.....	82
6.3	Chuyển đổi địa chỉ mạng (NAT).....	83
Chương 7 Định tuyến		85
7.1	Giới thiệu về định tuyến trong TCP/IP	86
7.2	Trở lại vấn đề router.....	86
7.2.1	Vài nét về chuyển tiếp IP (IP forwarding)	87
7.2.2	Định tuyến trực tiếp và gián tiếp.....	88
7.2.3	Các thuật toán định tuyến động.....	90
7.3	Định tuyến trong những mạng phức tạp	94
7.4	Khảo sát các router nội	96
7.4.1	Giao thức thông tin định tuyến (RIP)	97
7.4.2	Giao thức ưu tiên đường đi ngắn nhất (OSPF)	98
7.5	Định tuyến không phân lớp (classless)	98
Chương 8 Phân giải tên		100
8.1	Thế nào là phân giải tên?	101
8.2	Phân giải tên miền sử dụng các tập tin host	102
8.3	Phân giải tên DNS	104
8.4	Đăng ký một miền	109
8.5	Quản lý DNS	110
8.5.1	Cấu hình máy chủ DNS	111
8.5.2	Tập tin Zone	111
8.5.3	Tập tin Zone truy vấn ngược	113
8.5.4	Những tiện ích cho DNS.....	114
8.5.5	Kiểm tra phân giải địa chỉ với Ping	114
8.5.6	Kiểm tra phân giải địa chỉ với NSLookup	115
8.6	DNS động	116
8.7	Phân giải tên NetBIOS	117
8.8	Các phương pháp phân giải địa chỉ NetBIOS.....	118

8.8.1	Phương pháp phân giải dựa trên Broadcast	118
8.8.2	Phân giải tên dùng các tập tin LMHosts	119
8.8.3	Phân giải tên: Dịch vụ phân giải tên Internet trên Windows (WINS)	121
8.9	Kiểm tra phân giải tên NetBIOS.....	123
8.10	Những dịch vụ phân giải tên khác	124
Chương 9 Giao thức cấu hình host động -DHCP		125
9.1	Trường hợp server cung cấp địa chỉ IP cho server	126
9.2	Thế nào là DHCP?.....	126
9.3	Cơ chế làm việc của DHCP	127
9.3.1	Trạm chuyển tiếp.....	128
9.3.2	Trường thời gian DHCP	129
9.4	Cấu hình DHCP	129
9.4.1	Cấu hình DHCP Server trên Windows	130
9.4.2	Cấu hình DHCP Server trên Linux.....	134
Chương 10 Truyền tập tin và các tiện ích truy cập.....		136
10.1	Giao thức truyền tập tin (FTP)	137
10.2	Giao thức truyền tập tin bình thường (TFTP).....	140
10.3	Sao chép từ xa (Remote Copy).....	141
10.4	Tích hợp truy cập tập tin mạng.....	142
10.5	Khối thông điệp server (SMB)	143
Chương 11 Các tiện ích truy cập từ xa		146
11.1	Telnet.....	147
11.2	Tiện ích Berkeley.....	149
11.3	Các hướng mới trong việc truy cập từ xa.....	153
Chương 12 HTTP, HTML, và World Wide Web.....		155
12.1	World Wide Web là gì?	156
12.2	Khảo sát kỹ hơn về URL	159
12.3	HTML.....	161
12.4	HTTP	166
12.5	Các kỹ thuật HTML tiên tiến	168
12.5.1	Kỹ thuật HTML phía Server.....	168
12.5.2	Kỹ thuật HTML phía Client.....	171
12.6	XML	171
12.7	Các công nghệ Web mới	173
12.7.1	Web đa phương tiện	173
12.7.2	Các giao dịch Web	174
12.7.3	Peer-to-Peer	177
Chương 13 Email		179
13.1	Thư điện tử là gì?	180
13.2	Thư điện tử có dạng như thế nào?	180

13.3	Thư điện tử hoạt động như thế nào?	182
13.4	Giao thức chuyển thư đơn giản SMTP	185
13.5	Quá trình lấy thư	187
13.5.1	POP3	188
13.5.2	IMAP4.....	189
13.6	Các bộ đọc thư điện tử.....	189
13.6.1	Pine.....	190
13.6.2	Eudora.....	191
13.6.3	Các ứng dụng thư điện tử tích hợp	192
13.7	Thư điện tử trên Web.....	193
13.8	Spam	194
Chương 14 Các giao thức quản lý mạng		197
14.1	Giao thức quản lý mạng đơn giản SNMP	198
14.2	Không gian địa chỉ SNMP.....	199
14.3	Các lệnh SNMP	201
14.4	Giám sát từ xa (RMON).....	203

DANH SÁCH CÁC HÌNH

	Trang
Hình 1-1 Các lớp giao thức của mô hình TCP/IP	3
Hình 1-2 Mô hình OSI 7 lớp.....	5
Hình 1-3 Ở mỗi lớp, dữ liệu được đóng gói lại với phần tiêu đề của lớp đó	6
Hình 1-4 Xem qua hệ thống hoạt động mạng TCP/IP cơ bản	8
Hình 2-1 OSI và lớp Truy cập mạng	13
Hình 2-2 Lớp Truy cập mạng định dạng dữ liệu cho mạng vật lý	15
Hình 2-3 Một mạng ethernet đồng trục 10BASE-2	18
Hình 2-4 Một mạng ethernet dựa trên hub 10BASE-T.....	18
Hình 2-5 Một Token Ring	19
Hình 3-1 Gateway nhận các datagram được đánh địa chỉ đến các mạng khác	23
Hình 3-2 Bạn có thể nói ra mạng của thiết bị bằng cách nhìn vào địa chỉ	25
Hình 3-3 Trường tiêu đề IP	26
Hình 3-4 Hệ thống số thập phân	30
Hình 3-5 Hệ thống số nhị phân	31
Hình 3-6 ARP ánh xạ các địa chỉ IP vào các địa chỉ vật lý.....	36
Hình 4-1 Phân phối dữ liệu đến một mạng lớp A.....	40
Hình 4-2 Tổ chức mạng để phân phối hiệu quả	41
Hình 4-3 Một cặp địa chỉ IP/subnet mask	42
Hình 4-4 Phân phối các bit địa chỉ trong một mạng phân mạng con so với mạng không phân mạng con	42
Hình 4-5 Các datagram đang đến trên một mạng phân mạng con.....	43
Hình 4-6 Một mạng lớp B được phân mạng con	46
Hình 4-7 Một mạng lớp C được phân mạng con	47
Hình 5-1 Một giao thức hướng kết nối.....	54
Hình 5-2 Một giao thức không kết nối.....	54
Hình 5-3 Một địa chỉ cổng đưa dữ liệu tới một ứng dụng cụ thể	55
Hình 5-4 Trao đổi số hiệu socket nguồn và đích	56
Hình 5-5 Đa hợp và giải đa hợp	59
Hình 5-6 Địa chỉ socket nhận dạng duy nhất một ứng dụng trên một máy chủ cụ thể...	60
Hình 5-7 Các router chuyển tiếp chứ không xử lý dữ liệu lớp vận chuyển	62
Hình 5-8 Định dạng dữ liệu đoạn TCP (segment)	63
Hình 5-9 Tiêu đề và trường dữ liệu của datagram UDP	68
Hình 5-10 Minh họa một tường lửa điển hình	70
Hình 6-1 Một thiết bị lọc.....	72
Hình 6-2 Một mạng ethernet sử dụng hub	74

Hình 6-3 Một switch liên kết mỗi port với một địa chỉ vật lý	75
Hình 6-4 Một switch tách biệt mỗi máy tính để giảm lưu lượng.....	76
Hình 6-5 Một máy tính đa kết nối hoạt động như một router.....	78
Hình 6-6 Định tuyến trong một mạng phức tạp.....	79
Hình 6-7 Tiến trình định tuyến	81
Hình 6-8 Bảng định tuyến.....	82
Hình 6-9 Một thiết bị chuyển đổi địa chỉ mạng	83
 Hình 7-1 Tiến trình chuyển tiếp IP	88
Hình 7-2 Một router kết nối 2 phân đoạn mạng có thể định tuyến trực tiếp tới mỗi phân đoạn	89
Hình 7-3 Một router phải thực hiện định tuyến gián tiếp nếu nó phải chuyển tiếp các datagram sang những mạng không kết nối trực tiếp với nó	89
Hình 7-4 Sự cập nhật trong định tuyến vector khoảng cách	93
Hình 7-5 Kiến trúc router trên internet	95
 Hình 8-1 Phân giải tên host	102
Hình 8-2 Một máy chủ DNS cung cấp dịch vụ phân giải tên miền cho mạng	105
Hình 8-3 Trong các mạng lớn hơn, máy chủ DNS liên lạc với nhau để cung cấp dịch vụ phân giải địa chỉ	105
Hình 8-4 Không gian tên miền DNS.....	106
Hình 8-5 Sơ đồ gần đúng của DNS.....	107
Hình 8-6 Tiến trình phân giải địa chỉ	108
Hình 8-7 Đáp ứng NSLookup.....	116
Hình 8-8 Cập nhật DNS động	117
Hình 8-9 Nội dung của tập tin LMHosts.....	121
Hình 8-10 Phân giải tên NetBIOS-WINS.....	122
 Hình 9-1 Hộp thoại DHCP Manager's Create Scope	131
Hình 9-2 Hộp thoại Options DHCP: Scope	132
Hình 9-3 Hộp thoại DHCP Options: Global	133
Hình 9-4 Hộp thoại IP Address Array Editor.....	134
Hình 9-5 Phạm vi	134
 Hình 10-1 Bắt đầu một phiên làm việc FTP.....	138
Hình 10-2 Lệnh <code>ls</code>	139
Hình 10-3 SMB và chồng giao thức TCP/IP.....	144
 Hình 11-1 Telnet server và client.....	148
Hình 11-2 Vào và ra mạng với Telnet	148
Hình 11-3 Tiến trình truy cập tin cậy trên Unix	150
 Hình 12-1 Một Web site là một hệ thống hợp nhất giữa trang và các liên kết.....	157
Hình 12-2 Nhập URL trong hộp địa chỉ của trình duyệt window	158

Hình 12-3 Các URLtương đối tạo khả năng di động cho Website	161
Hình 12-4 Một ví dụ về trang Web đơn giản.....	164
Hình 12-5 Mở rộng ví dụ easy!	165
Hình 12-6 Một mô hình server-side scripting	169
Hình 12-7 Một mô hình giao dịch Web đặc trưng	176
Hình 12-8 Một máy tính đăng ký dịch vụ peer-to-peer với địa chỉ và danh sách tài nguyên của nó. Các máy tính khác truy cập các tài nguyên này thông qua một kết nối trực tiếp	178
 Hình 13-1 Tiến trình phân phối email	 183
Hình 13-2 Các server chuyển tiếp thường tăng hiệu suất của tiến trình phân phối thư	184
Hình 13-3 Dịch vụ SMTP và dịch vụ lấy thư phải được sắp xếp để được truy cập vào hộp thư.....	188
Hình 13-4 Cửa sổ chính của Eudora Light.....	191
Hình 13-5 Cấu hình các tùy chọn trong Eudora Light.....	192
Hình 13-6 Một virus thư điện tử.....	193
Hình 13-7 Các Spammer có thể dùng server không bị nghi ngờ và không được bảo vệ để gửi các thông điệp của họ	195
Hình 13-8 Đặt server SMTP đằng sau bức tường lửa và ngăn cấm các yêu cầu SMTP, bảo vệ server khỏi sự lợi dụng của spammer.....	196
 Hình 14-1 Một cộng SNMP gồm có một hoặc nhiều các thiết bị giám sát và tập hợp các node.....	 198
Hình 14-2 Một chương trình tác nhân đang chạy tại các node ở xa gửi thông tin tới thiết bị giám sát mạng và nhận các yêu cầu thay đổi các thiết lập cấu hình.....	199
Hình 14-3 Một phần nhỏ của MIB.....	200

DANH SÁCH CÁC BẢNG

	Trang
Bảng 2-1 Công nghệ môi trường truyền dẫn Ethernet.....	18
Bảng 3-1 Các giới hạn địa chỉ cho các mạng lớp A, B và C.....	29
Bảng 3-2 Chuyển một địa chỉ nhị phân sang dạng chấm thập phân	32
Bảng 4-1 Subnet Mask dạng dấu chấm thập phân và dạng nhị phân.....	48
Bảng 5-1 Các cổng TCP phổ biến	56
Bảng 5-2 Các cổng UDP phổ biến	58
Bảng 12-1 Lược đồ URL.....	159
Bảng 12-2 Một vài thẻ HTML quan trọng.....	162
Bảng 12-3 Các thuộc tính thẻ	165
Bảng 12-4 Các ví dụ về các vùng tiêu đề HTTP	167
Bảng 13-1 Một số vùng quan trọng trong tiêu đề thư điện tử.....	181
Bảng 13-2 Các lệnh SMTP Client.....	185
Bảng 13-3 Một số hỏi đáp của SMTP Server	185

CHƯƠNG TCP/IP LÀM VIỆC

1 NHƯ THẾ NÀO

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Các lớp giao thức TCP/IP**
- **Mô hình OSI**
- **Các giao thức TCP/IP tương tác như thế nào**

TCP/IP là một hệ thống (hay hệ) các giao thức, và một giao thức là một hệ thống các luật và các thủ tục. Phần lớn phần cứng và phần mềm của các máy tính truyền thông với nhau theo các luật truyền thông TCP/IP mà người dùng không cần quan tâm một cách chi tiết. Tuy nhiên, sự hiểu biết về cách thức làm việc của TCP/IP là cần thiết nếu bạn muốn thông suốt về việc cấu hình và các vấn đề gỡ rối mà bạn sẽ gặp phải với các mạng TCP/IP.

Chương này mô tả hệ thống giao thức TCP/IP và cho thấy các thành phần của TCP/IP làm việc với nhau như thế nào để truyền và nhận dữ liệu qua mạng.

Kết thúc chương này bạn sẽ có thể :

- Mô tả các lớp của hệ thống giao thức TCP/IP và nhiệm vụ của các lớp.
- Mô tả các lớp của mô hình giao thức OSI và giải thích mối quan hệ giữa các lớp OSI và TCP/IP như thế nào.
- Giải thích các tiêu đề (header) của giao thức TCP/IP và dữ liệu được đóng gói với phần thông tin tiêu đề ở mỗi lớp của chồng giao thức như thế nào.
- Tên của gói dữ liệu ở mỗi lớp của chồng TCP/IP.
- Thảo luận về các giao thức TCP, UDP, IP và chúng làm việc với nhau như thế nào để thực hiện các chức năng TCP/IP.

1.1 Hệ thống giao thức TCP/IP

Trước khi xem xét các thành phần của TCP/IP, chúng ta điểm lại các chức năng của một hệ thống giao thức.

Một hệ thống giao thức, chẳng hạn như TCP/IP đảm nhiệm các chức năng sau :

- Chia các thông điệp (message) thành các đoạn dữ liệu để có thể quản lý và truyền qua môi trường truyền một cách hiệu quả.
- Giao tiếp với phần cứng tương thích mạng.
- Đánh địa chỉ: Máy tính truyền phải có khả năng đưa dữ liệu đến đúng máy tính nhận. Và máy tính nhận cũng phải có khả năng nhận ra một thông điệp là truyền cho nó.
- Định tuyến dữ liệu đến mạng con của máy tính đích, cho dù mạng con của máy tính nguồn và máy tính đích không thuộc cùng một loại mạng vật lý.
- Thực hiện kiểm soát lỗi, điều khiển luồng và báo nhận: Đối với truyền thông tin cậy, các máy tính truyền và nhận phải có khả năng nhận dạng, sửa lỗi và điều khiển luồng dữ liệu.
- Nhận dữ liệu từ một ứng dụng và truyền nó vào mạng.
- Và ngược lại, nhận dữ liệu từ mạng và truyền nó đến một ứng dụng.

Để thực hiện các chức năng trên, TCP/IP được xây dựng dựa trên thiết kế module. Hệ thống giao thức TCP/IP được chia thành các thành phần riêng biệt độc lập chức năng với nhau về mặt lý thuyết. Mỗi thành phần đảm nhận một phần của tiến trình truyền thông.

Ưu điểm của thiết kế module là giúp cho nhà cung cấp dễ dàng tích hợp phần mềm giao thức với phần cứng cụ thể và các hệ điều hành. Ví dụ, lớp Truy cập mạng - Network Access layer (như bạn sẽ học trong **chương 2, “Lớp truy cập mạng”**) gồm các chức năng liên quan đến kiến trúc LAN cụ thể, như Token Ring hay Ethernet. Dựa vào thiết kế module của TCP/IP, một nhà cung cấp như Microsoft không phải xây dựng một gói phần mềm khác hẳn hoàn toàn giữa các mạng TCP/IP Token Ring và TCP/IP Ethernet. Các lớp trên không bị ảnh hưởng; chỉ có lớp Truy Cập Mạng là phải thay đổi.

Hệ thống giao thức TCP/IP được phân ra thành các thành phần theo lớp, mỗi phần thực hiện các nhiệm vụ riêng biệt (xem **hình 1-1**). Mô hình này, hay chồng giao thức này, có từ những ngày đầu xây dựng TCP/IP, và đôi lúc nó được gọi là mô hình TCP/IP. Các lớp TCP/IP chính thức và các chức năng của nó được mô tả trong hình sau :

Hình 1-1 Các lớp giao thức của mô hình TCP/IP

Lớp ứng dụng
Lớp vận chuyển
Lớp Internet
Lớp truy cập mạng

So sánh các chức năng trong danh sách với các nhiệm vụ được liệt kê phía trên trong chương này, bạn sẽ thấy các nhiệm vụ của hệ thống giao thức được phân bổ vào các lớp như thế nào.

Thông tin thêm

Mô hình bốn lớp được thể hiện trong **hình 1-1** là một mô hình chung cho việc mô tả hoạt động mạng TCP/IP, nhưng nó không phải là một mô hình duy nhất. Ví dụ, mô hình ARPANet (RFC 871) mô tả ba lớp : *lớp Giao tiếp mạng (Network Interface layer)*, *lớp Host-to-Host*, *lớp Mức xử lý/ Các ứng dụng (Process-Level/ Applications layer)*. Các mô tả khác của TCP/IP là mô hình năm lớp, với các lớp Vật lý (Physical) và Liên kết dữ liệu (Data Link) tương ứng với lớp Truy cập mạng (để phù hợp với mô hình OSI). Vẫn có một số mô hình khác không có lớp Truy cập mạng (Access Network layer) hay lớp Ứng dụng (Application layer), vì các lớp này hay thay đổi và khó định nghĩa hơn các lớp trung gian.

Tên của các lớp cũng có thể thay đổi. Các tên lớp ARPANet vẫn xuất hiện trong một số cuộc thảo luận về TCP/IP, và lớp Internet đôi khi được gọi là *lớp Liên mạng (Internetwork layer)* hay *lớp Mạng (Network layer)*.

Cuốn sách này sử dụng mô hình bốn lớp, với các tên lớp được thể hiện trong **hình 1-1**.

- **Lớp Truy cập mạng (Network Access layer)** – Cung cấp một giao tiếp với mạng vật lý. Các định dạng dữ liệu cho môi trường truyền và các địa chỉ dữ liệu cho mạng con (subnet) được dựa trên các địa chỉ phần cứng vật lý. Cung cấp kiểm soát lỗi cho dữ liệu phân bố trên mạng vật lý.
- **Lớp Internet (Internet layer)** – Cung cấp chức năng đánh địa chỉ luận lý, độc lập phần cứng mà nhờ đó dữ liệu có thể di chuyển giữa các mạng con có các kiến trúc vật lý khác nhau. Cung cấp chức năng định tuyến để giảm lưu lượng và hỗ trợ phân bố dọc theo Liên mạng (internetwork). (Thuật ngữ *Liên mạng* nói đến một mạng lớn hơn, liên kết giữa các LAN). Liên kết các địa chỉ vật lý (sử dụng ở lớp Truy cập mạng) với các địa chỉ luận lý.

- **Lớp Vận chuyển (Transport layer)** – Cung cấp chức năng điều khiển luồng, kiểm soát lỗi và các dịch vụ báo nhận cho liên mạng. Hoạt động như là một giao tiếp cho các ứng dụng mạng.
- **Lớp Ứng dụng (Application layer)** – Cung cấp các ứng dụng cho việc xử lý sự cố mạng, truyền tập tin, điều khiển từ xa, và các hoạt động Internet. Lớp này cũng hỗ trợ cho Các giao tiếp lập trình ứng dụng (Application Programming Interfaces - APIs) cho phép các chương trình viết trên một môi trường điều hành cụ thể để truy cập mạng.

Các chương sau sẽ mô tả chi tiết hơn các hoạt động ở mỗi lớp của giao thức TCP/IP này.

Khi phần mềm giao thức TCP/IP chuẩn bị một đoạn dữ liệu để truyền qua mạng, mỗi lớp của máy phát sẽ thêm thông tin điều khiển liên quan với lớp tương ứng trên máy nhận. Ví dụ, lớp Internet của máy tính gửi sẽ thêm một phần tiêu đề với một số thông tin có ý nghĩa liên quan đến lớp Internet của máy tính sẽ nhận thông điệp. Tiến trình này thường được xem là quá trình đóng gói (*encapsulation*). Ở đầu nhận, các phần tiêu đề này sẽ được loại bỏ khi dữ liệu được đưa lên các lớp bên trên.

Thông tin thêm

Thuật ngữ "**lớp**" (**layer**) được sử dụng trong toàn ngành công nghệ máy tính cho các mức thành phần giao thức như được thể hiện trong **hình 1-1**. Thông tin tiêu đề trong các lớp được gắn vào dữ liệu khi nó đi qua các thành phần của chồng giao thức. (Bạn sẽ hiểu rõ hơn về điều này ở phần cuối của chương này). Dù thế nào thì thuật ngữ "lớp" cũng chỉ là một điều gì đó mang tính ẩn dụ.

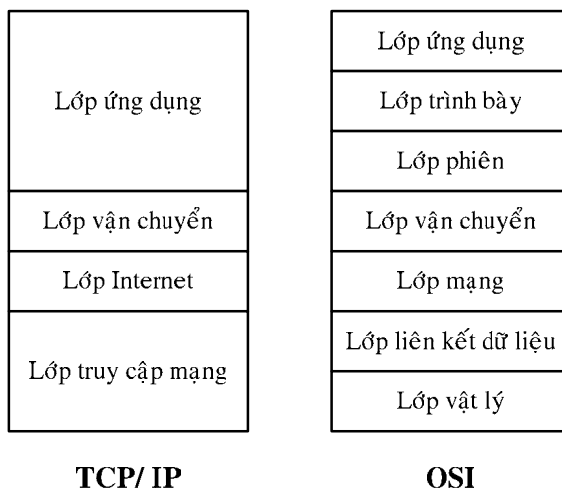
1.2 TCP/IP và mô hình OSI

Công nghệ kết nối mạng có một mô hình 7 lớp chuẩn cho kiến trúc giao thức mạng được gọi là *mô hình Liên kết các hệ thống mở (Open Systems Interconnection - OSI)*. Mô hình OSI là một nỗ lực của tổ chức tiêu chuẩn thế giới ISO (International Standards Organization), một tổ chức tiêu chuẩn quốc tế, nhằm tiêu chuẩn hóa thiết kế các hệ thống giao thức mạng để làm tăng tính liên kết và truy cập mở đến các chuẩn giao thức cho các nhà phát triển phần mềm.

Vì TCP/IP ra đời và phát triển trước khi có kiến trúc chuẩn OSI nên TCP/IP hoàn toàn không tuân theo mô hình OSI. Tuy nhiên, hai mô hình đã có những mục tiêu tương tự nhau, và có sự ảnh hưởng lẫn nhau giữa các nhà thiết kế các tiêu chuẩn này nên chúng được đưa ra với tính tương thích nào đó. Mô hình OSI rất có ảnh hưởng trong sự phát triển của các giao thức, và hiện nay thuật ngữ OSI áp dụng cho TCP/IP là khá phổ biến. **Hình 1-2** cho thấy mối quan hệ giữa 4 lớp chuẩn TCP/IP và mô hình OSI 7 lớp. Chú ý rằng mô hình OSI chia các nhiệm vụ của lớp Ứng dụng thành 3 lớp :

lớp Ứng dụng (Application), lớp Trình bày (Presentation) và lớp Phiên (Session). OSI tách các hoạt động của lớp Giao tiếp mạng (Network Interface) thành một lớp Liên kết dữ liệu (Data Link) và một lớp Vật lý (Physical). Việc chia lớp nhỏ hơn này làm tăng sự phức tạp, nhưng cũng làm tăng tính linh hoạt cho các nhà phát triển bằng việc đưa các lớp giao thức đến nhiều dịch vụ cụ thể hơn.

Hình 1-2 Mô hình OSI 7 lớp



Bảy lớp của mô hình OSI bao gồm các lớp sau :

- **Lớp Vật lý (Physical layer)** - Chuyển đổi dữ liệu thành chuỗi các xung điện hay tương tự sẽ thực sự truyền qua môi trường truyền và quan sát việc truyền dữ liệu.
- **Lớp Liên kết dữ liệu (Data Link layer)** – Cung cấp một giao tiếp với bộ tương thích mạng (network adapter), duy trì các liên kết luận lý cho mạng con.
- **Lớp Mạng (Network layer)** - Hỗ trợ việc đánh địa chỉ luận lý và định tuyến.
- **Lớp Vận chuyển (Transport layer)** – Cho phép kiểm soát lỗi và điều khiển luồng trong liên mạng.
- **Lớp Phiên (Session layer)** - Thiết lập các phiên làm việc giữa các ứng dụng truyền thông trên các máy tính truyền thông.
- **Lớp Trình bày (Presentation layer)** – Chuyển đổi dữ liệu sang định dạng chuẩn; quản lý việc mã hóa và nén dữ liệu.
- **Lớp Ứng dụng (Application layer)** – Cung cấp một giao tiếp mạng cho các ứng dụng; hỗ trợ các ứng dụng mạng cho việc truyền tập tin, truyền thông

Điều quan trọng cần phải nhớ là mô hình TCP/IP và mô hình OSI là các tiêu chuẩn để dựa trên đó mà thực hiện. Thực tế thì TCP/IP thường không tương ứng hoàn

toàn với các mô hình trong **hình 1-1** và **hình 1-2**, sự tương ứng hoàn hảo trong **hình 1-2** cũng là một vấn đề trong các cuộc thảo luận trong công nghệ.

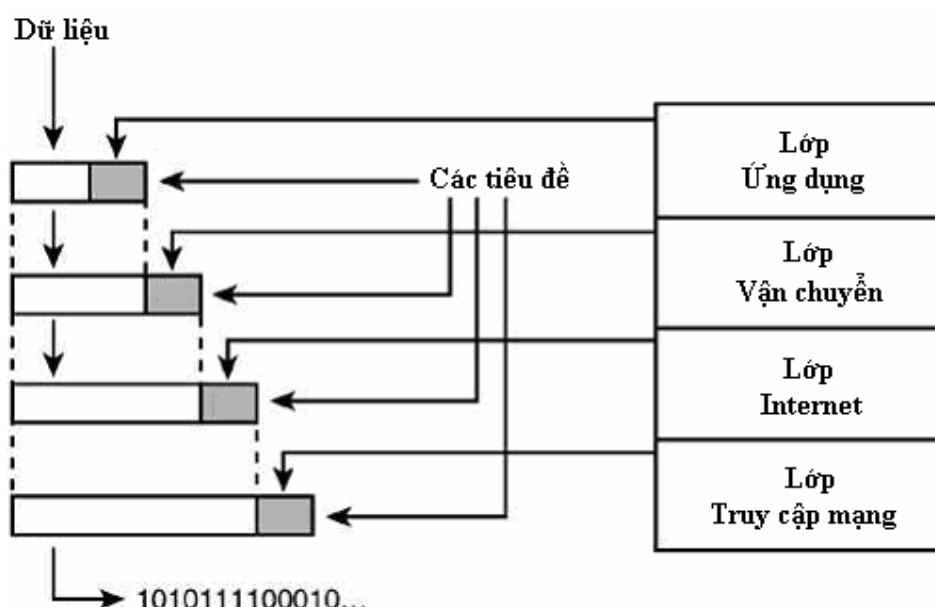
Chú ý rằng các mô hình OSI và TCP/IP hầu như tương tự nhau ở các lớp quan trọng là lớp Vận chuyển và lớp Internet (được gọi là lớp mạng trong mô hình OSI). Các lớp này chứa các thành phần phân biệt và có thể nhận dạng được của hệ thống giao thức, và không phải ngẫu nhiên mà các hệ thống giao thức đôi khi được đặt tên là các giao thức lớp Vận chuyển và lớp Mạng của chúng. Như bạn sẽ thấy ở các chương sau của tài liệu này, bộ giao thức TCP/IP gồm TCP, một giao thức lớp Vận chuyển, và IP, một giao thức lớp Internet/ Mạng.

1.3 Các gói dữ liệu

Điều quan trọng cần nhớ về chồng giao thức TCP/IP là mỗi lớp đóng một vai trò trong toàn bộ quá trình truyền thông. Mỗi lớp đòi hỏi các dịch vụ cần thiết để thực hiện vai trò của nó. Khi truyền, dữ liệu đi xuyên qua từng lớp của chồng giao thức từ trên xuống dưới, mỗi lớp sẽ có một số thông tin thích hợp gọi là *tiêu đề (header)* gắn vào dữ liệu, tạo thành *Đơn vị dữ liệu giao thức PDU (Protocol Data Unit)* của lớp tương ứng. Khi PDU được đưa xuống các lớp thấp hơn, nó lại trở thành dữ liệu đối với lớp này và lại được đóng gói cùng với phần tiêu đề của lớp này.

Tiến trình này được thể hiện trong **hình 1-3**. Khi gói dữ liệu đến máy nhận thì tại đây sẽ có một tiến trình ngược lại. Khi dữ liệu đi lên qua từng lớp của chồng giao thức thì các lớp sẽ bỏ phần tiêu đề tương ứng và sử dụng phần dữ liệu.

Hình 1-3 Ở mỗi lớp, dữ liệu được đóng gói lại với phần tiêu đề của lớp đó



Lớp Internet trên máy nhận sẽ sử dụng thông tin trong phần tiêu đề lớp Internet. Lớp Vận chuyển sẽ sử dụng thông tin trong phần tiêu đề lớp Vận chuyển. Ở mỗi lớp, gói dữ liệu ở dưới dạng thích hợp sẽ cung cấp thông tin cần thiết cho lớp tương ứng trên máy nhận. Bởi vì mỗi lớp đảm nhận những chức năng khác nhau nên định dạng của gói dữ liệu cơ bản thì rất khác nhau ở mỗi lớp.

Thông tin thêm

Gói dữ liệu ở mỗi lớp có dạng khác nhau, và ở mỗi lớp nó có một tên khác nhau. Các tên của các gói dữ liệu được tạo ra ở mỗi lớp như sau :

- Gói dữ liệu được tạo ra ở lớp Ứng dụng được gọi là thông điệp (message).
 - Gói dữ liệu được tạo ra ở lớp Vận chuyển do sự đóng gói thông điệp lớp Ứng dụng, được gọi là một đoạn (segment) nếu là giao thức TCP của lớp Vận chuyển. Nếu gói dữ liệu đến từ giao thức UDP của lớp Vận chuyển, nó được gọi là **datagram**.
 - Gói dữ liệu ở lớp Internet, đóng gói đoạn của lớp Vận chuyển, được gọi là một **datagram**.
 - Gói dữ liệu ở lớp Truy cập mạng được gọi là **khung (frame)**, nó đóng gói một datagram của lớp Internet và có thể chia nhỏ một datagram thành nhiều khung. Khung này sau đó được chuyển thành luồng các bit ở lớp con thấp nhất của lớp Truy cập mạng.
-

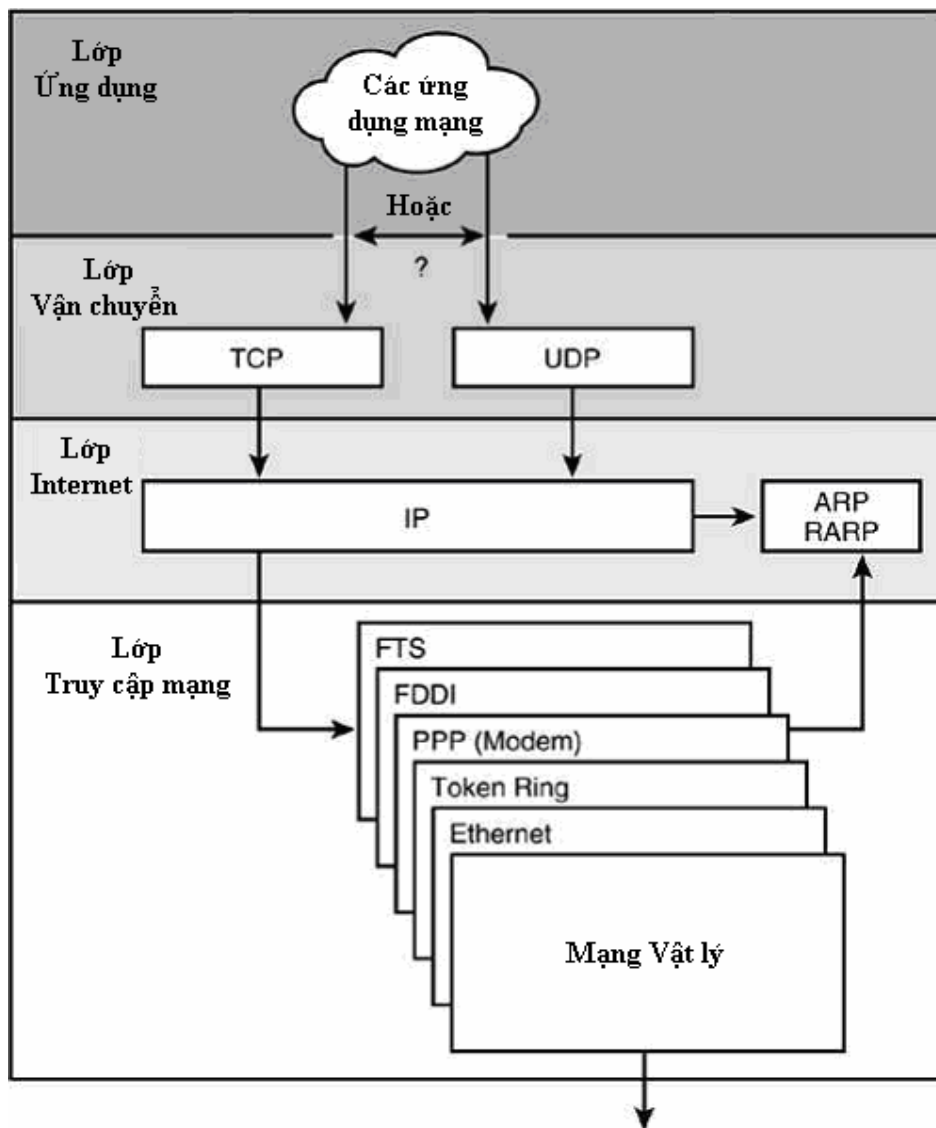
1.4 Xem qua hoạt động mạng TCP/IP

Thói quen mô tả các hệ thống giao thức dưới dạng các lớp của chúng nói chung là phổ biến. Hệ thống phân lớp cho phép ta hiểu biết sâu sắc hệ thống giao thức, và không thể mô tả TCP/IP mà không giới thiệu kiến trúc phân lớp của nó trước. Tuy nhiên, việc chỉ tập trung vào các lớp giao thức cũng chỉ là những mô phỏng.

Trước hết, việc nói về các lớp giao thức hơn là chính các giao thức đưa ra thêm các khái niệm trừu tượng cho một vấn đề mà bản thân nó đã rất trừu tượng. Thứ hai, việc ghi thành từng khoản các giao thức khác nhau giống như các tiêu đề trong các chủ đề lớn hơn của một lớp giao thức có thể gây nên suy nghĩ sai lầm là tất cả các giao thức đều có tầm quan trọng như nhau. Trên thực tế, mặc dù mỗi giao thức đóng một vai trò, nhưng hầu hết các tính năng của bộ TCP/IP có thể chỉ được mô tả dưới dạng một số các giao thức quan trọng nhất của nó. Việc xem xét cận cảnh các giao thức quan trọng này đôi khi có ích hơn là mô tả hệ thống phân lớp ở phần trước của chương này.

Hình 1-4 mô tả hoạt động của hệ thống mạng giao thức TCP/IP cơ bản. Dĩ nhiên trong gói giao thức hoàn chỉnh sẽ có thêm các giao thức và các dịch vụ bổ sung.

Hình 1-4 Xem qua hệ thống hoạt động mạng TCP/IP cơ bản



Kịch bản cơ bản như sau :

1. Dữ liệu truyền từ một ứng dụng TCP/IP, hay từ một giao tiếp chương trình ứng dụng mạng, qua một cổng TCP hay UDP đến một trong hai giao thức lớp Vận chuyển (TCP hay UDP). Các chương trình có thể truy cập mạng qua TCP hay UDP, phụ thuộc vào các yêu cầu của chương trình.
 - TCP/IP là một giao thức hướng kết nối. Như bạn sẽ học trong **chương 5, “Lớp Vận chuyển”** các giao thức hướng kết nối cung cấp cho ta khả năng điều khiển luồng và kiểm soát lỗi tinh xảo hơn các giao thức không kết nối. TCP thực hiện với một nỗ lực hết sức lớn để bảo đảm việc truyền dữ liệu trên mạng. TCP tin cậy hơn UDP, nhưng việc bổ sung kiểm tra lỗi và điều khiển luồng có nghĩa là TCP chậm hơn UDP.

- UDP là một giao thức không kết nối. Nó nhanh hơn TCP, nhưng không tin cậy. Đối với UDP, các chức năng kiểm tra lỗi được chuyển cho các ứng dụng thực hiện.
2. Đoạn dữ liệu được chuyển xuống lớp Internet, ở đó giao thức IP cung cấp thông tin đánh địa chỉ luận lý và đóng gói dữ liệu vào một datagram.
 3. Datagram IP vào lớp Truy cập mạng, tại đây nó đi qua các thành phần phần mềm được thiết kế để giao tiếp với mạng vật lý. Lớp Truy cập mạng tạo một hay nhiều khung dữ liệu sau đó đưa vào mạng vật lý. Trong trường hợp của một hệ thống mạng LAN như là ethernet, khung có thể chứa thông tin địa chỉ vật lý có được từ các bảng tìm kiếm và các bảng này được duy trì nhờ các giao thức ARP và RARP lớp Internet. (**ARP**, giao thức phân giải địa chỉ - Address Resolution Protocol, chuyển đổi các địa chỉ IP thành các địa chỉ vật lý. **RARP**, giao thức phân giải địa chỉ ngược - Reverse Address Resolution Protocol, chuyển đổi các địa chỉ vật lý thành các địa chỉ IP).
 4. Khung dữ liệu được chuyển thành một luồng các bit để truyền trên môi trường mạng.

Dĩ nhiên, có vô số các chi tiết mô tả làm thế nào mỗi giao thức thực hiện các nhiệm vụ của nó. Ví dụ, TCP cung cấp khả năng điều khiển luồng như thế nào, ARP và RARP ánh xạ các địa chỉ vật lý sang các địa chỉ IP như thế nào, và IP làm thế nào biết được phải gửi datagram tới đâu để đến một mạng con khác? Các câu hỏi này đã được sáng tỏ ở các chương sau của tài liệu. Bạn cũng sẽ học nhiều hơn về các giao thức TCP/IP và về các tiến trình được mô tả trong chương này ở các chương sau.

Tóm tắt

Trong chương này, bạn đã học về các lớp của chồng giao thức TCP/IP và các lớp này có quan hệ với nhau như thế nào. Bạn cũng đã học mô hình TCP/IP kinh điển quan hệ với mô hình hoạt động mạng OSI 7 lớp như thế nào. Ở mỗi lớp trong chồng giao thức, dữ liệu được đóng gói dưới dạng hữu dụng nhất cho lớp tương ứng ở phía nhận. Chương này thảo luận tiến trình của việc đóng gói thông tin tiêu đề ở mỗi lớp giao thức và phác thảo các dạng thuật ngữ được sử dụng ở mỗi lớp để mô tả gói dữ liệu. Cuối cùng, bạn đã xem qua các hoạt động hệ thống giao thức TCP/IP như thế nào từ việc xem xét một số các giao thức quan trọng nhất : TCP, UDP, IP, ARP và RARP.

CHƯƠNG LỚP

2 TRUY CẬP MẠNG

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Địa chỉ vật lý**
- **Khung Ethernet**
- **Các công nghệ LAN**

Ở phần nền của chồng giao thức TCP/IP là lớp Truy cập mạng, nó là tập hợp các dịch vụ và các đặc tả cung cấp và quản lý truy cập đến phần cứng mạng. Trong chương này bạn sẽ học về các nhiệm vụ của lớp Truy cập mạng và lớp Truy cập mạng quan hệ với mô hình OSI như thế nào. Chương này cũng xem xét một số công nghệ mạng vật lý thông dụng trong lớp Truy cập mạng.

Kết thúc chương này bạn sẽ có thể :

- Giải nghĩa lớp Truy cập mạng
- Thảo luận về mối quan hệ giữa lớp Truy cập mạng của TCP/IP và mô hình hoạt động mạng OSI
- Giải thích một kiến trúc mạng
- Liệt kê các nội dung của một khung Ethernet
- Nhận dạng các phương thức mà Ethernet, Token Ring, và FDDI sử dụng cho việc điều khiển truy cập đến môi trường truyền.

2.1 Các giao thức và phần cứng

Lớp Truy cập mạng là lớp khó giải thích nhất và đa dạng nhất trong các lớp của TCP/IP. Lớp Truy cập mạng quản lý tất cả các dịch vụ và các chức năng cần thiết để chuẩn bị dữ liệu cho mạng vật lý. Các nhiệm vụ này bao gồm :

- Giao tiếp với bộ tương thích mạng (card mạng) của máy tính.
- Phối hợp việc truyền dữ liệu với các quy ước của phương thức truy cập thích hợp. Bạn sẽ biết rõ hơn về các phương thức truy cập trong phần sau của chương này.
- Định dạng dữ liệu vào một đơn vị được gọi là một khung và chuyển đổi khung đó thành luồng các xung điện hoặc tương tự để đi qua môi trường truyền.
- Kiểm tra lỗi trong các khung đến.
- Thêm thông tin kiểm tra lỗi vào các khung đi để máy tính nhận có thể kiểm tra các lỗi của khung.
- Báo nhận các khung dữ liệu và truyền lại các khung nếu không nhận được báo nhận.

Dĩ nhiên, ở phía nhận cũng phải thực hiện việc định dạng các khung nhận được bởi máy tính mà nó được đánh địa chỉ.

Lớp Truy cập mạng định nghĩa các thủ tục để giao tiếp với phần cứng mạng và truy cập môi trường truyền. Trong lớp Truy cập mạng của TCP/IP, bạn có thể thấy sự tác động qua lại phức tạp giữa phần cứng, phần mềm và các chi tiết kỹ thuật môi trường truyền. Không may, có nhiều loại mạng vật lý khác nhau mà đều có những quy ước riêng của chúng, và bất kỳ mạng vật lý nào cũng có thể tạo thành nền tảng cho lớp Truy cập mạng. Bạn sẽ học về các loại mạng vật lý này sau trong chương này. Một số ví dụ bao gồm :

- Ethernet
- Token ring
- FDDI
- PPP (Point-to-Point Protocol, thông qua modem)
- Wireless networks

Thông tin thêm

Không phải mọi máy tính hoạt động mạng đều trên một LAN. Phần mềm truy cập mạng cũng có thể hỗ trợ cho những thứ khác với bộ thích hợp mạng chuẩn và cáp LAN. Một trong những giải pháp thông dụng là một kết nối modem đến một mạng ở xa, như là kết nối bạn thiết lập khi bạn quay số vào một nhà cung cấp dịch vụ Internet (ISP). Các chuẩn giao thức

modem như là Serial Line Internet Protocol (SLIP) và Point-to-Point Protocol (PPP) cung cấp truy cập mạng cho chồng giao thức TCP/IP thông qua một kết nối modem.

Điều đáng mừng là lớp Truy cập mạng hầu như hoàn toàn vô hình đối với người sử dụng. Bộ phận điều khiển bộ tương thích mạng, kết hợp với các thành phần mức thấp quan trọng của hệ điều hành và phần mềm giao thức, quản lý hầu hết các thao tác được giao cho lớp Truy cập mạng, và người dùng chỉ cần thực hiện một số bước cấu hình đơn giản. Các bước thao tác này đang ngày càng trở nên đơn giản do các tính năng plug-and-play của các hệ điều hành ngày càng được nâng cao.

Khi bạn đọc hết chương này, nhớ rằng việc đánh địa chỉ IP được thảo luận trong các **chương 1, 3 và 4** là hoàn toàn bằng phần mềm. Hệ thống giao thức yêu cầu các dịch vụ bổ sung để phân phối dữ liệu qua một hệ thống LAN cụ thể và đi ngược lên qua bộ tương thích mạng của một máy tính đích. Các dịch vụ này hoạt động trong phạm vi của lớp Truy cập mạng.

Thông tin thêm

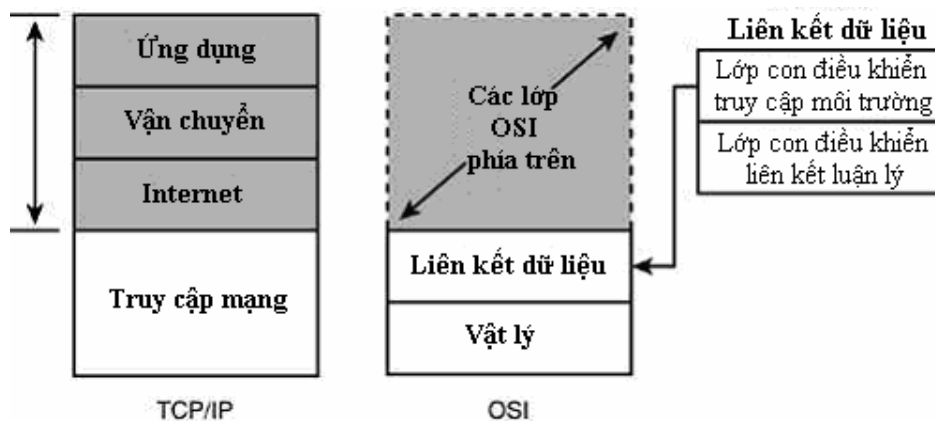
Điều đáng quan tâm là do tính đa dạng, tính phức tạp, và tính vô hình của lớp Truy cập mạng mà một số tác giả loại nó ra khỏi các cuộc thảo luận của TCP/IP. Thay vào đó chỉ đề cập các driver LAN thuộc về lớp Truy cập mạng là các phần của chồng giao thức dưới lớp Internet. Quan điểm này cũng đúng, tuy nhiên lớp Truy cập mạng thực sự là một bộ phận của chồng giao thức TCP/IP, và khi thảo luận về các tiến trình truyền thông mạng thì không thể không đề cập đến nó.

2.2 Lớp truy cập mạng và mô hình OSI

Như ở **chương 1, “TCP/IP làm việc như thế nào”** đã đề cập, TCP/IP độc lập với mô hình hoạt động mạng 7 lớp OSI, nhưng mô hình OSI thường được sử dụng như là một khuôn mẫu cho việc tìm hiểu về các hệ thống giao thức. Thuật ngữ OSI và các khái niệm đặc biệt phổ biến trong các cuộc thảo luận của lớp Truy cập mạng vì mô hình OSI cung cấp các quá trình phân nhỏ hơn cho phạm trù rộng của truy cập mạng. Các quá trình phân nhỏ này tạo ra thêm một vài hoạt động bên trong lớp này. Mô hình OSI đã có ảnh hưởng với các nhà cung cấp mạng máy tính, và xu hướng hiện nay hướng về các chuẩn đa giao thức như là NDIS và ODI (được thảo luận ở phần sau) đã làm nổi bật nhu cầu thuật ngữ thông dụng mà mô hình OSI cung cấp.

Như **hình 2-1** cho thấy, lớp Truy cập mạng TCP/IP rất phù hợp với các lớp Vật lý và Liên kết dữ liệu OSI. Lớp Vật lý OSI đảm nhiệm việc chuyển khung dữ liệu thành luồng các bit phù hợp với môi trường truyền. Nghĩa là, lớp Vật lý OSI quản lý và đồng bộ các xung điện và xung tương tự tạo thành truyền thông thực sự. Ở đầu nhận, lớp Vật lý tập hợp các xung này lại thành một khung dữ liệu.

Hình 2-1 OSI và lớp Truy cập mạng



Lớp Liên kết dữ liệu OSI thực hiện hai chức năng riêng biệt và được phân nhỏ vào hai lớp tương ứng sau :

- **Điều khiển truy cập môi trường truyền - Media Access Control (MAC)** - Lớp con này cung cấp một giao tiếp với bộ tương thích mạng. Bộ điều khiển bộ tương thích mạng, trên thực tế thường được gọi là bộ điều khiển MAC, và địa chỉ phần cứng được ghi vào tấm thẻ ở xưởng sản xuất thường được xem là địa chỉ MAC.
- **Điều khiển liên kết luận lý - Logical Link Control (LLC)** - Lớp con này thực hiện các chức năng kiểm tra lỗi cho các khung được phân phối trên mạng con và quản lý các liên kết giữa các thiết bị đang giao tiếp trên mạng con.

Thông tin thêm

Trong các thực thi giao thức mạng thực, sự khác biệt giữa các lớp của các hệ thống TCP/IP và OSI trở nên rắc rối hơn bởi sự phát triển của Đặc tả giao tiếp bộ điều khiển mạng (Network Driver Interface Specification_NDIS) và đặc tả Giao tiếp liên kết dữ liệu mở (Open Data-Link Interface_ODI). NDIS (được phát triển bởi Microsoft và 3Com Corp.) và ODI (được phát triển bởi Apple và Novell) được thiết kế để cho một chồng giao thức đơn (như TCP/IP) sử dụng nhiều bộ tương thích mạng và để cho một bộ tương thích mạng sử dụng nhiều giao thức lớp trên. Điều này thực sự làm cho các giao thức lớp trên có thể không lệ thuộc hệ thống truy cập mạng, tăng cường thêm chức năng cho mạng nhưng đồng thời cũng tạo ra thêm sự phức tạp trong việc thảo luận một cách có hệ thống các thành phần của phần mềm quan hệ với nhau ở các lớp thấp hơn.

2.3 Kiến trúc mạng

Trong thực tế, khi nói đến khái niệm mạng cục bộ thì người ta thường quan tâm kiến trúc LAN hay kiến trúc mạng chứ không phải các lớp giao thức. (Đôi khi một kiến trúc mạng được xem như là một loại LAN hay một cấu trúc liên kết (topology) LAN). Một kiến trúc mạng, như ethernet, cung cấp một gói các đặc tả chi phối truy cập môi

trường, đánh địa chỉ vật lý, và sự tương tác của các máy tính với môi trường truyền thông. Khi bạn quyết định chọn một kiến trúc mạng, bạn đang quyết định về một phác thảo cho lớp truy cập mạng.

Một kiến trúc mạng là một thiết kế cho mạng vật lý và một tập hợp các đặc tả định nghĩa các truyền thông trên mạng vật lý đó. Các chi tiết truyền thông phụ thuộc vào các chi tiết vật lý, vì thế các đặc tả thường đi cùng với nhau thành một gói hoàn chỉnh. Các đặc tả này bao gồm các vấn đề như sau :

- **Phương thức truy cập** - Một phương thức truy cập là một tập các luật định nghĩa các máy tính sẽ chia sẻ môi trường truyền thông như thế nào. Để tránh các đụng độ dữ liệu (data collision), các máy tính phải tuân theo các luật này khi truyền dữ liệu.
- **Định dạng khung dữ liệu – Datagram** - mức IP từ lớp Internet được đóng gói trong một khung dữ liệu với một định dạng được định nghĩa trước. Dữ liệu trong phần tiêu đề phải cung cấp thông tin cần thiết để phân phối dữ liệu trên mạng vật lý. Bạn sẽ học nhiều hơn về các khung dữ liệu trong phần sau của chương này.
- **Loại cáp (cable)** - Loại cáp sử dụng cho một mạng có ảnh hưởng trên các thông số thiết kế nào đó như là các đặc tính điện của luồng bit được truyền bởi bộ tương thích.
- **Các luật đi cáp** – Các giao thức, loại cáp, và các đặc tính điện truyền dẫn có ảnh hưởng đến chiều dài tối đa và tối thiểu của cáp và các chi tiết kỹ thuật kết nối cáp.

Các chi tiết như là loại cáp và loại bộ nối không phải là nhiệm vụ trực tiếp của lớp Truy cập mạng, nhưng để thiết kế các thành phần phần mềm của lớp Truy cập mạng, các nhà phát triển phải thừa nhận một tập cụ thể các đặc điểm của mạng vật lý. Do đó, phần mềm truy cập mạng phải đi cùng với thiết kế phần cứng cụ thể.

2.4 Đánh địa chỉ vật lý

Như bạn đã học trong chương trước về các khái niệm TCP/IP cơ bản, lớp Truy cập mạng cần phải gắn liền với địa chỉ IP luận lý được cấu hình thông qua phần mềm giao thức với địa chỉ vật lý cố định thực sự của bộ tương thích mạng. Địa chỉ vật lý được ghi vào card mạng ở xí nghiệp sản xuất. Các khung dữ liệu truyền qua LAN phải sử dụng địa chỉ vật lý này để xác định các bộ tương thích nguồn và đích, nhưng địa chỉ vật lý dài dòng (48 bit trong trường hợp sử dụng ethernet) không được thân thiện với con người. Ngoài ra, việc mã hóa địa chỉ vật lý ở các mức giao thức cao hơn làm ảnh

hướng đến kiến trúc module linh hoạt của TCP/IP, nó đòi hỏi các lớp trên duy trì các chi tiết vật lý liên quan.

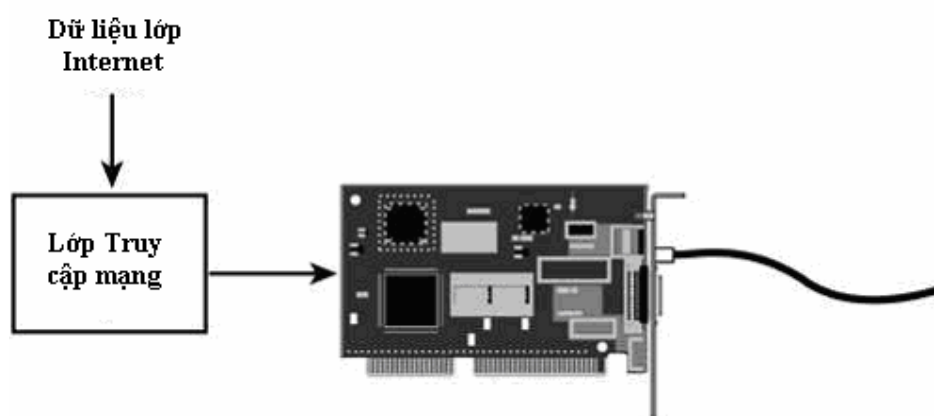
TCP/IP sử dụng Giao thức phân giải địa chỉ (Address Resolution Protocol_ARP) và Giao thức phân giải địa chỉ ngược (Reverse Address Resolution Protocol_RARP) để liên kết các địa chỉ IP với các địa chỉ vật lý của các bộ tương thích mạng trên mạng cục bộ. ARP và RARP cung cấp một liên kết giữa các địa chỉ IP luận lý mà người dùng nhìn thấy và các địa chỉ phần cứng (thực sự không thể trông thấy được) được dùng trên LAN.

Bạn sẽ học về ARP và RARP trong *Chương 3, “Lớp Internet”*.

2.5 Cấu trúc khung

Phần mềm lớp Truy cập mạng nhận một datagram từ lớp Internet và chuyển đổi dữ liệu đó đến dạng phù hợp với các đặc tả của mạng vật lý (xem *hình 2-2*). Vì có nhiều dạng mạng vật lý nên có nhiều định dạng cho dữ liệu ở lớp Truy cập mạng, và không dễ dàng để mô tả chi tiết tất cả các định dạng này.

Hình 2-2 Lớp Truy cập mạng định dạng dữ liệu cho mạng vật lý



Chúng ta lấy ví dụ trong trường hợp sử dụng ethernet (kiến trúc thông dụng nhất trong các kiến trúc LAN) để minh họa những gì xảy ra ở lớp Truy cập mạng. Khi phần mềm ethernet nhận một datagram từ lớp Internet, nó thực hiện các bước sau :

1. Chia dữ liệu lớp IP thành các đoạn nhỏ, nếu cần, để chuyển chúng vào các vùng dữ liệu của các khung ethernet. Kích thước tổng cộng của một khung ethernet phải từ 64 byte đến 1.518 byte (không bao gồm phần mở đầu).
2. Gói các đoạn dữ liệu vào các khung. Mỗi khung bao gồm dữ liệu cũng như thông tin khác mà các bộ tương thích mạng trên ethernet cần để xử lý khung. Một khung ethernet IEEE 802.3 bao gồm các phần sau :

Phần mở đầu (Preamble): Một chuỗi tuần tự các bit dùng để đánh dấu bắt đầu của khung (8 byte, byte cuối là byte 1 định ra điểm bắt đầu khung).

Địa chỉ nhận (Recipient address): Địa chỉ vật lý 6 byte (48 bit) của bộ tương thích mạng sẽ nhận khung.

Địa chỉ nguồn (Source address): Địa chỉ vật lý 6 byte (48 bit) của bộ tương thích mạng gửi khung đi.

Chiều dài (Length): Một trường 2 byte (16 bit) cho biết kích thước của trường dữ liệu.

Dữ liệu (Data): Dữ liệu được truyền cùng với khung.

Kiểm tra chuỗi khung (Frame Check Sequence - FCS): Một giá trị kiểm tra tổng 4 byte (32 bit) cho khung. FCS thường dùng để kiểm tra truyền thông dữ liệu, máy tính gởi tính toán một giá trị Kiểm tra dư vòng (Cyclical Redundancy Check - CRC) cho khung và mã hóa giá trị CRC trong khung. Máy tính nhận sau đó sẽ tính toán lại CRC và kiểm tra trường FCS để xem các giá trị có tương ứng hay không. Nếu các giá trị không tương ứng, một vài dữ liệu đã mất hay bị thay đổi trong quá trình truyền thông, trong trường hợp đó khung sẽ được truyền lại.

3. Truyền khung dữ liệu đến các thành phần mức thấp hơn tương ứng với lớp Vật lý của OSI để chuyển khung thành luồng bit và gởi nó trên môi trường truyền.

Các bộ tương thích mạng khác nhận khung và kiểm tra địa chỉ đích. Nếu địa chỉ đích tương ứng với địa chỉ của bộ tương thích mạng, phần mềm bộ tương thích xử lý khung đến và chuyển dữ liệu đến các lớp cao hơn của chồng giao thức.

Thông tin thêm

IEEE 802.3 không phải là tiêu chuẩn ethernet duy nhất. Tiêu chuẩn Ethernet II, được sử dụng bởi một số nhà cung cấp, có một định dạng khung hơi khác.

2.6 Các công nghệ LAN

Các kiến trúc mạng thông dụng nhất :

- Ethernet
- Token Ring

Thông tin thêm

IEEE (Institute of Electrical and Electronic Engineers) đã đưa ra một tập các tiêu chuẩn cho các kiến trúc LAN. Mặc dù Token Ring và Ethernet đều được phát minh trước các tiêu chuẩn IEEE, các đặc tả IEEE cho IEEE 802.3 (ethernet) và IEEE 802.5 (Token Ring) hiện nay cung cấp các chuẩn độc lập với nhà sản xuất các công nghệ LAN quan trọng này.

Các phần sau sẽ khảo sát ethernet và token ring chi tiết hơn, cùng với kỹ thuật LAN khác là FDDI.

2.6.1 Ethernet

Ethernet và những người anh em mới hơn của nó Fast Ethernet và Gigabit Ethernet là các công nghệ LAN thông dụng nhất được sử dụng hiện nay. Ethernet đã trở nên phổ biến vì giá cả phải chăng của nó; cáp Ethernet không đắt và dễ cài đặt. Các bộ tương thích mạng Ethernet và các thành phần phần cứng Ethernet cũng tương đối rẻ.

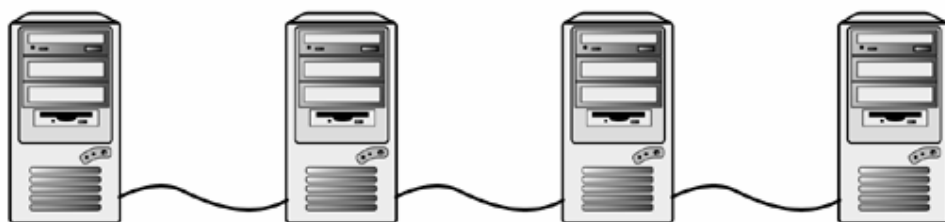
Trên các mạng ethernet, tất cả các máy tính chia sẻ một môi trường truyền thông chung. Ethernet sử dụng một phương thức truy cập được gọi là Đa truy cập cảm nhận sóng mang (Carrier Sense Multiple Access) với Dò tìm đụng độ (Collision Detect) - CSMA/CD để quyết định khi nào một máy tính có thể truyền dữ liệu trên môi trường truy cập. Sử dụng CSMA/CD, tất cả các máy tính quan sát môi trường truyền thông và chờ đến khi tuyến truyền thông sẵn sàng thì mới truyền. Nếu hai máy tính cố gắng truyền cùng một lúc thì sẽ xảy ra đụng độ. Các máy tính sẽ dừng lại, chờ một khoảng thời gian ngẫu nhiên, và thử truyền lại.

CSMA/CD có thể được so sánh với giao thức hoạt động trong một phòng họp gồm những người lịch sự. Một người nào đó muốn nói trước hết anh ta lắng nghe để xác định xem có người nào khác hiện đang nói không (đây là cảm nhận sóng mang - Carrier Sense). Nếu hai người bắt đầu nói cùng lúc, cả hai sẽ phát hiện ra vấn đề, ngừng nói, và chờ trước khi nói tiếp (đây là Dò tìm đụng độ - Collision Detect).

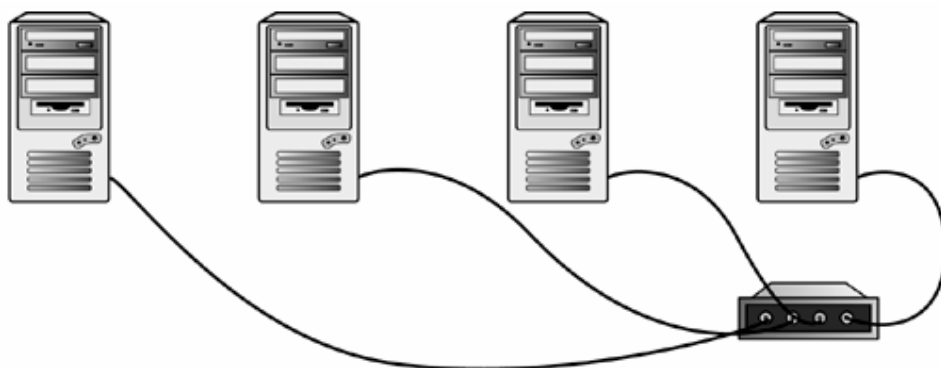
Ethernet truyền thông làm việc tốt trong trường hợp tải bình thường nhưng tỉ lệ đụng độ sẽ cao khi mức độ sử dụng tăng. Một số biến thể mới của ethernet, có thể bao gồm các hub thông minh hoặc switch, hỗ trợ cho các mức lưu lượng cao hơn. Bạn sẽ học nhiều hơn về các hub và switch trong **Chương 6, "Phần cứng mạng"**.

Ethernet có khả năng hoạt động trong nhiều loại môi trường khác nhau. Các mạng Ethernet tiêu biểu hoạt động ở các tốc độ băng tần cơ sở 10Mbps hay 100Mbps. Các hệ thống Ethernet 1000Mbps (Gigabit) hiện nay đã sẵn sàng và có thể sớm trở nên phổ biến. **Bảng 2-1** liệt kê các thuật ngữ được sử dụng để xác định môi trường cáp, các tốc độ và các khoảng cách tối đa. Ethernet không dây cũng đang trở nên phổ biến. Các mạng ethernet đồng trục 10BASE-2 và 10BASE-5 đã từng rất phổ biến. **Hình 2-3** cho thấy một mạng 10BASE-2 đồng trục. Chú ý rằng các máy tính được gắn vào một cáp đơn hoạt động như môi trường truyền thông chia sẻ. Trong những năm gần đây, các biến thể ethernet khác nhau dựa trên hub như là 10BASE-T (xem **hình 2.4**) đã và đang trở nên rất phổ biến. Trên một mạng 10BASE-T, các máy tính được gắn vào một hub trung tâm. 10BASE-2 và 10BASE-T xem ra có thể khác nhau, nhưng bên trong chúng đều là ethernet.

Hình 2-3 Một mạng ethernet đồng trục 10BASE-2



Hình 2-4 Một mạng ethernet dựa trên hub 10BASE-T



Bảng 2-1 Công nghệ môi trường truyền dẫn Ethernet

Tên công nghệ	Môi trường truyền dẫn	Tốc độ hoạt động	Khoảng cách tối đa
10BASE-2	Đồng trục mảnh	10 megabits	185 m
10BASE-5	Đồng trục dày	10 megabits	500 m
10BASE-T	CAT3 hoặc CAT5 UTP	10 megabits	100 m
10BASE-F	Cáp quang	10 megabits	2,000 m
100BASE-TX	CAT 5 UTP hoặc STP	100 megabits	100 m
100BASE-FX	Cáp quang	100 megabits	2,000 m

Kiến trúc ethernet linh hoạt thậm chí thích hợp với hoạt động mạng không dây. Ethernet không dây đang trở nên phổ biến, và sẽ trở nên phổ biến hơn nữa trong những năm sắp tới khi phần cứng mạng phát triển hỗ trợ cho cuộc cách mạng không dây. Bạn có thể tự hỏi làm thế nào một kiến trúc quá tập trung trong việc đặc tả các loại, chiều dài, và cấu hình cáp của Ethernet lại có thể hoạt động trong môi trường không dây.

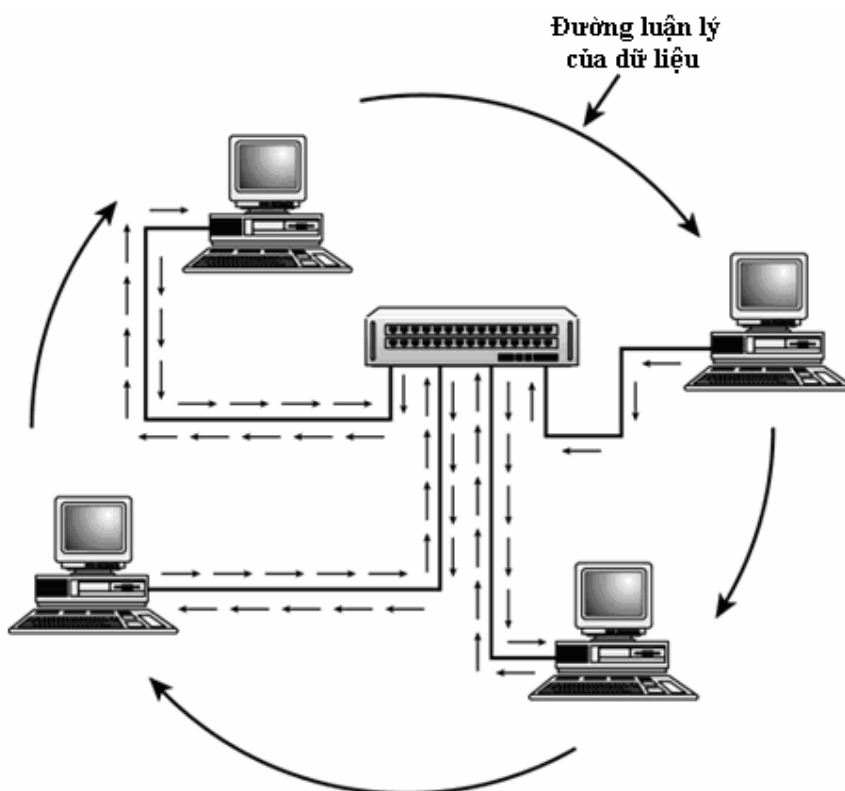
Khi nghĩ về Ethernet thì ta thấy bản chất thông tin quảng bá khá tương thích với hệ thống không dây có đặc tính là truyền dẫn tự do và lưu động.

2.6.2 Token Ring

Kỹ thuật Token Ring sử dụng một khái niệm hoàn toàn khác hẳn với Ethernet trong quy trình truy cập môi trường. Phương thức truy cập này được gọi là chuyển token.

Với phương thức truy cập chuyển token, các máy tính trên LAN được kết nối với nhau sao cho dữ liệu được truyền vòng quanh mạng trong một vòng luân lý (xem **hình 2-5**). Việc cấu hình token ring đòi hỏi các máy tính phải được nối vào một hub trung tâm được gọi là MAU hay MSAU. **Hình 2-5** có thể trông không giống một vòng, nhưng MSAU được nối sao cho dữ liệu truyền từ một máy tính đến máy kế theo cách thức di chuyển vòng quanh. Các máy tính truyền một gói điều khiển đặc biệt được gọi là một token vòng quanh mạng. Chỉ máy tính giữ token mới có thể truyền một thông điệp lên vòng.

Hình 2-5 Một Token Ring



Token ring về kỹ thuật thì phức tạp hơn ethernet, và nó bao gồm một số các chẩn đoán và sửa lỗi được thiết lập sẵn bên trong và có thể hỗ trợ cho việc khắc phục sự cố mạng. Ngoài ra, vì dữ liệu được truyền có thứ tự hơn, trong token ring không xảy ra trường hợp tải nặng. Hầu như mọi thứ liên quan đến token ring đều đắt tiền hơn

ethernet khi so sánh giữa chúng – cáp, các card mạng, và các thành phần khác cũng vậy.

Token ring điển hình hoạt động ở tốc độ 4Mbps hoặc 16Mbps. Nó cũng có thể hoạt động ở tốc độ 100Mbps.

Token ring đã không còn phổ biến trong những năm gần đây, mặc dù vậy cấu trúc liên kết dạng vòng trong Token Ring vẫn được sử dụng trong các kỹ thuật đỉnh cao như FDDI, mà bạn sẽ học trong phần sau.

2.6.3 FDDI

Fiber Distributed Data Interface (FDDI) là một kỹ thuật LAN đắt tiền dùng hai vòng cáp quang. Một vòng được xem như là vòng chính và vòng thứ hai để thay thế vòng chính nếu xảy ra sự cố. FDDI sử dụng một phương thức truy cập chuyển token tương tự như token ring.

Giống như token ring, FDDI cũng có khả năng dò tìm và sửa lỗi. Trong một vòng FDDI hoạt động thông thường, token luôn truyền bởi mỗi máy. Nếu không thấy token trong thời gian tối đa luân chuyển quanh một vòng, thì có nghĩa là đã xảy ra một vấn đề gì đó, chẳng hạn như đứt cáp.

Cáp sợi quang được sử dụng với FDDI có thể cho phép tải một lượng dữ liệu rất lớn trên các khoảng cách lớn.

2.7 Các kỹ thuật truy cập mạng khác

Các kỹ thuật LAN cũng như là ethernet rất phổ biến, nhưng có nhiều cách khác để kết nối các máy tính. Bất kỳ kỹ thuật hoạt động mạng nào cũng phải có một số cách thức để chuẩn bị dữ liệu cho mạng vật lý, và do đó bất kỳ kỹ thuật TCP/IP nào cũng phải có một lớp Truy cập mạng. Như đã đề cập trước đây, một modem là một cách thức khác hỗ trợ cho một kết nối mạng. Các kỹ thuật WAN (Wide area network) hỗ trợ các kết nối hoạt động trên các khoảng cách lớn hơn nhưng thường ở tốc độ truyền thông thấp hơn. Các kết nối WAN đòi hỏi phần cứng riêng, và ta có thể đoán được, nó cũng đòi hỏi phần mềm riêng biệt ở lớp Truy cập mạng. Bạn sẽ học nhiều hơn về các kỹ thuật WAN trong *Chương 6, “Phần cứng mạng”*.

Tóm tắt

Trong chương này, bạn đã học về lớp Truy cập mạng, là lớp đa dạng nhất và có thể cho là phức tạp nhất trong chồng giao thức TCP/IP. Lớp Truy cập mạng định nghĩa các thủ tục để giao tiếp với phần cứng mạng và truy cập môi trường truyền. Có nhiều loại kiến trúc LAN và do đó có nhiều dạng lớp Truy cập mạng. Chương này cũng mô tả các nội dung của khung ethernet và nói ngắn gọn về ethernet, token ring, và FDDI.

CHƯƠNG

3

LỚP

INTERNET

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Địa chỉ IP**
- **Tiêu đề IP**
- **ARP**
- **ICMP**

Như bạn đã học trong phần trước, các máy tính trên một đoạn mạng đơn như một ethernet LAN có thể thông tin với nhau sử dụng các địa chỉ vật lý sẵn có ở lớp Truy cập mạng. Sau đó, làm thế nào một thông điệp email từ Carolina đến California và đến chính xác đích của nó? Như bạn sẽ học trong chương này, các giao thức ở lớp Internet cung cấp việc phân phối vượt ra ngoài mạng con. Chương này thảo luận các giao thức lớp Internet quan trọng như IP, ARP và ICMP.

Kết thúc chương này bạn sẽ có thể :

- Giải thích mục đích của IP, ARP và ICMP
- Giải thích một network ID và một host ID là gì
- Giải thích một octet là gì
- Chuyển một địa chỉ dạng dấu chấm thập phân sang dạng nhị phân tương ứng của nó
- Chuyển một địa chỉ IP nhị phân 32 bit sang dạng dấu chấm thập phân
- Mô tả các nội dung của một tiêu đề IP
- Giải thích mục đích của địa chỉ IP
- Xác định các trường network ID và host ID của các địa chỉ lớp A, B và C.

3.1 Đánh địa chỉ và phân phối

Như bạn đã học trong **Chương 2, “Lớp Truy cập mạng”**, một máy tính thông tin với mạng thông qua một thiết bị giao tiếp mạng như một card tương thích mạng. Thiết bị giao tiếp mạng có một địa chỉ vật lý duy nhất và được thiết kế để nhận dữ liệu gửi đến địa chỉ vật lý đó. Địa chỉ vật lý này được ghi vào card mạng khi nó được chế tạo. Một thiết bị như một card ethernet không biết bất kỳ chi tiết nào của các lớp giao thức bên trên. Nó không biết địa chỉ IP của nó và cũng không biết một khung đến được gửi đến Telnet hay là FTP. Nó chỉ lắng nghe các khung đang tới, chờ một khung có địa chỉ là địa chỉ vật lý của chính nó, và chuyển khung đó ngược lên trên chồng giao thức.

Sự phối hợp địa chỉ vật lý này làm việc rất tốt trên một đoạn LAN riêng biệt. Một mạng chỉ bao gồm một ít máy tính trên một môi trường liên tục có thể hoạt động mà không cần gì khác ngoài các địa chỉ vật lý. Dữ liệu có thể chuyển trực tiếp từ bộ tương thích mạng này đến bộ tương thích mạng kia mà chỉ cần sử dụng các giao thức mức thấp liên quan với lớp Truy cập mạng. (Giao thức NetBEUI không thể định tuyến là một giao thức cũ hoạt động trong kết nối mạng đơn giản này).

Không may, trên một mạng định tuyến không thể phân phối dữ liệu bằng địa chỉ vật lý. Các thủ tục tìm ra đích đến dùng cho việc phân phối bằng địa chỉ vật lý lại, không hoạt động được thông qua giao tiếp router. Cho dù chúng có thực hiện được thì việc phân phối bằng địa chỉ vật lý sẽ công kênh vì địa chỉ vật lý cố định ghi vào trong thẻ mạng không cho phép bạn áp đặt một cấu trúc luận lý trên không gian địa chỉ.

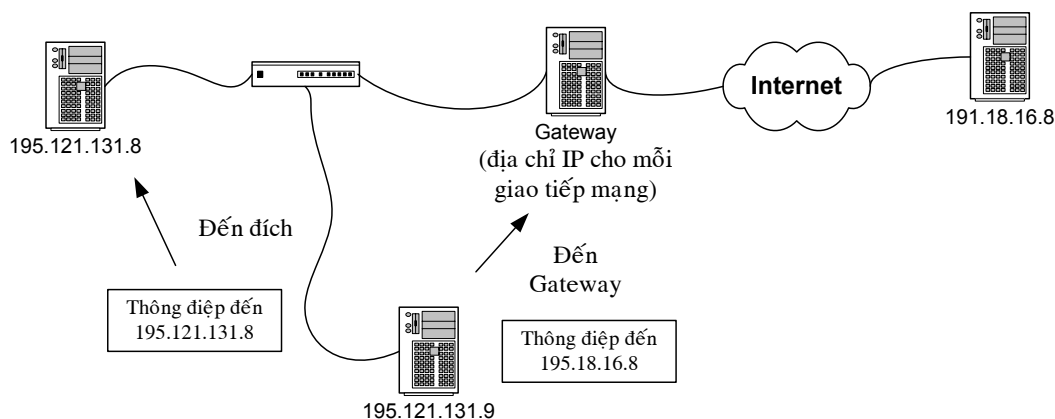
Vì thế TCP/IP sẽ làm cho địa chỉ vật lý trở nên vô hình và thay vào đó nó tổ chức mạng theo một sơ đồ đánh địa chỉ phân cấp và luận lý. Sơ đồ đánh địa chỉ luận lý được duy trì bởi giao thức IP ở lớp Internet. Địa chỉ luận lý được gọi là địa chỉ IP. Một giao thức lớp Internet khác được gọi là Giao thức phân giải địa chỉ (Address Resolution Protocol - ARP) hình thành tập hợp một bảng ánh xạ các địa chỉ IP vào các địa chỉ vật lý. Bảng ARP này là liên kết giữa địa chỉ IP và địa chỉ vật lý.

Trên một mạng định tuyến (xem **hình 3-1**), phần mềm TCP/IP sử dụng chiến lược sau để gửi dữ liệu trên mạng :

1. Nếu địa chỉ đích trên cùng một đoạn mạng như máy tính nguồn, máy tính nguồn gửi gói trực tiếp đến đích. Địa chỉ IP được phân giải sang một địa chỉ vật lý sử dụng ARP và dữ liệu được hướng tới bộ tương thích mạng đích.
2. Nếu địa chỉ đích trên một đoạn mạng khác với máy tính nguồn, các tiến trình sau bắt đầu :

- a. Datagram được đưa tới gateway. Gateway là một thiết bị trên đoạn mạng cục bộ mà có thể chuyển tiếp một datagram đến các đoạn mạng khác. (Như bạn sẽ học trong **chương 6, “Phần cứng mạng”**, và **chương 7, “Định tuyến”**, một gateway cơ bản là một router). Địa chỉ gateway được phân giải sang địa chỉ vật lý sử dụng ARP, và dữ liệu được gửi đến bộ tương thích mạng của gateway.
- b. Datagram được định tuyến qua gateway đến một đoạn mạng mức cao hơn (xem **hình 3-1**) ở đó tiến trình được lặp lại. Nếu địa chỉ đích nằm trên đoạn mạng mới này, dữ liệu được chuyển đến đích của nó. Nếu không, datagram được gửi đến một gateway khác.
- c. Datagram đi qua chuỗi các gateway đến đoạn mạng đích, ở đó địa chỉ IP đích được ánh xạ đến một địa chỉ vật lý sử dụng ARP và dữ liệu được hướng đến bộ tương thích mạng đích.

Hình 3-1 Gateway nhận các datagram được đánh địa chỉ đến các mạng khác



Do đó, phân phối dữ liệu trên một mạng định tuyến phức tạp, các giao thức lớp Internet do đó phải có thể :

- Xác định được bất kỳ máy tính nào trên mạng.
- Cung cấp một phương tiện để xác định khi nào một thông điệp phải được truyền qua một gateway.
- Cung cấp một phương tiện xác định đoạn mạng đích độc lập sao cho datagram sẽ đi qua các router đến đúng đoạn mạng một cách hiệu quả.
- Cung cấp một phương tiện để chuyển đổi địa chỉ IP luận lý của máy tính đích sang một địa chỉ vật lý để dữ liệu có thể được phân phối đến bộ tương thích mạng của máy tính đích.

Trong chương này bạn sẽ học về hệ thống đánh địa chỉ IP quan trọng, và bạn sẽ sẽ biết làm thế nào mà TCP/IP phân phối các datagram trên một mạng phức tạp với các giao thức IP và ARP của lớp Internet. Bạn cũng sẽ học về giao thức ICMP của lớp Internet, là giao thức cung cấp chức năng dò lỗi và xử lý sự cố.

3.2 Giao thức Internet (IP)

Giao thức Internet – Internet Protocol (IP) cung cấp một hệ thống đánh địa chỉ có phân cấp, độc lập phần cứng và đưa ra các dịch vụ cần thiết cho việc phân phối dữ liệu trên một mạng định tuyến phức tạp. Mỗi bộ tương thích mạng trên một mạng TCP/IP có một địa chỉ IP duy nhất.

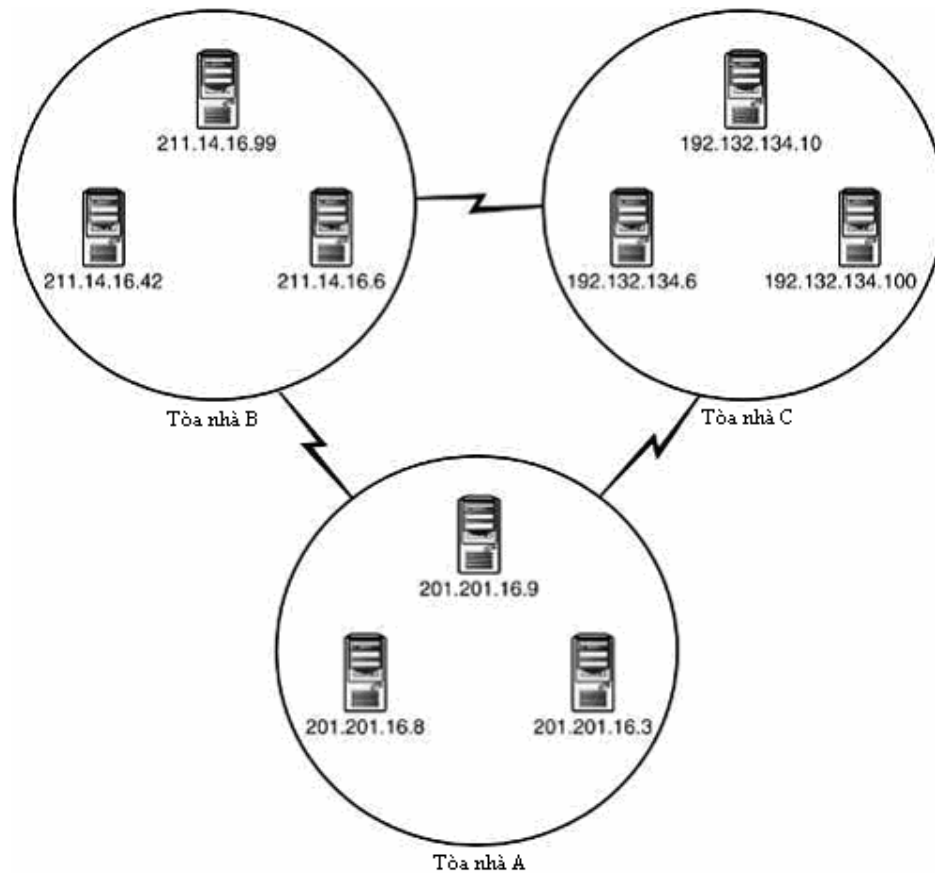
Thông tin thêm

Các mô tả của TCP/IP thường nói về một máy tính có một địa chỉ IP. Một máy tính đôi khi được xem là có một địa chỉ IP bởi vì hầu hết các máy tính chỉ có một bộ tương thích mạng. Tuy nhiên, các máy tính với nhiều bộ tương thích mạng cũng phổ biến. Ví dụ, một máy tính hoạt động như một router hay một máy chủ proxy, phải có nhiều hơn một bộ tương thích mạng và do đó có nhiều hơn một địa chỉ IP. Thuật ngữ host thường được sử dụng cho thiết bị mạng kết hợp với một địa chỉ IP.

Với nhiều hệ điều hành, nó cũng có thể ấn định nhiều hơn một địa chỉ IP vào một bộ tương thích mạng đơn.

Các địa chỉ IP trên mạng được tổ chức sao cho bạn có thể chỉ ra được vị trí của host - mạng hay mạng con nơi host cư trú - bằng cách nhìn vào địa chỉ (xem hình 3-2). Nói cách khác, một bộ phận của địa chỉ hơi giống một mã ZIP, và một bộ phận địa chỉ hơi giống địa chỉ đường chỉ ra vị trí chính xác bên trong vùng đó.

Hình 3-2 Bạn có thể nói ra mạng của thiết bị bằng cách nhìn vào địa chỉ



Ta có thể dễ dàng nhìn vào **hình 3-2** và nói, ”Mọi địa chỉ bắt đầu với 192.132.134 phải ở trong toà nhà C”. Tuy nhiên, một máy tính đòi hỏi có sự phân biệt với các máy khác. Địa chỉ IP do đó được chia thành hai phần :

- Định danh mạng (network ID).
- Định danh host (host ID).

Người sở hữu mạng cũng có thể đặt ra thêm một mức phân cấp địa chỉ bằng cách gán một định danh mạng con (subnet ID). Bạn sẽ học nhiều hơn về các mạng con và các định danh mạng con trong **Chương 4, “Phân mạng con”**.

Thông tin thêm

Học chương này và **chương 4**, bạn sẽ không thực sự thành thạo về kỹ thuật đánh địa chỉ IP cho đến khi bạn học về các định danh mạng con.

Khi bạn học phần sau của chương này, phần module IP của phần mềm giao thức có thể xác định từ địa chỉ chính nó, phần nào là định danh mạng và phần nào là định danh host.

3.2.1 Các trường tiêu đề IP

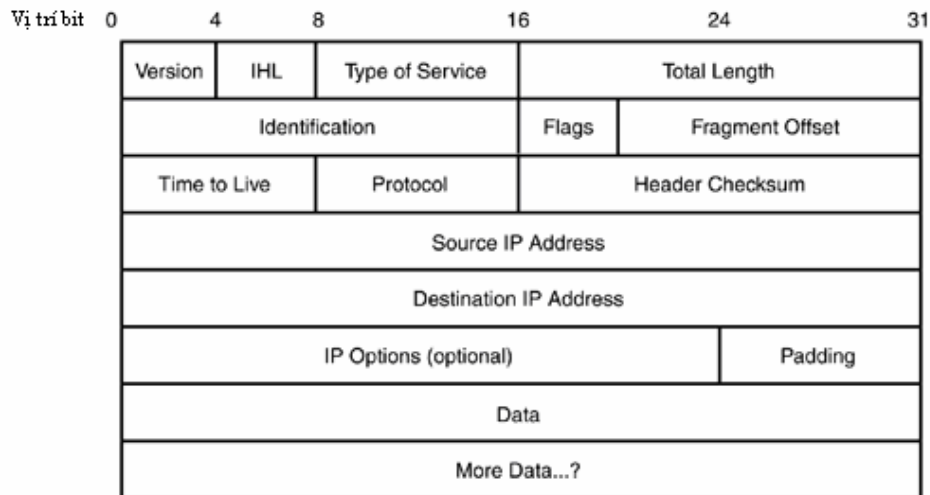
Mọi datagram IP bắt đầu với một tiêu đề IP. Phần mềm TCP/IP trên máy tính nguồn tạo ra tiêu đề IP. Phần mềm TCP/IP ở đích sử dụng thông tin được gói trong phần tiêu đề IP để xử lý datagram. Tiêu đề IP chứa một lượng thông tin lớn, bao gồm các địa chỉ IP của các máy tính nguồn và đích, chiều dài của datagram, số phiên bản IP, và các chỉ dẫn đặc biệt cho các router.

Thông tin thêm

Để có thêm thông tin về các tiêu đề IP, xem RFC 791.

Kích thước tối thiểu của một tiêu đề IP là 20 byte. **Hình 3.3** cho thấy các nội dung trên tiêu đề IP.

Hình 3-3 Trường tiêu đề IP



Các trường tiêu đề trong **hình 3-3** như sau :

Phiên bản (Version) - Trường 4 bit này xác định phiên bản của IP đang được sử dụng. Phiên bản hiện hành của IP là 4. Kiểu giá trị nhị phân cho 4 là 0100.

IHL (Internet Header Length - chiều dài tiêu đề Internet) - Trường 4 bit này cho biết chiều dài của tiêu đề IP tính theo các số 32 bit. Chiều dài tiêu đề nhỏ nhất là 5 từ 32 bit. Mẫu giá trị nhị phân của 5 là 0101.

Loại dịch vụ (Type of Service) - IP nguồn có thể chỉ định thông tin định tuyến đặc biệt. Một số router bỏ qua trường Loại dịch vụ này. Mặc dù hiện nay với sự xuất hiện của các công nghệ chất lượng dịch vụ QoS – Quality of Service, trường này đã được quan tâm nhiều hơn. Mục đích chính của vùng 8 bit này là để phân cấp độ ưu tiên của các datagram khi đi qua các router. Hiện nay trường này thường chỉ được gán toàn giá trị 0.

Chiều dài tổng cộng (Total length) - Trường 16 bit này xác định chiều dài của datagram IP tính bằng octet. Chiều dài này bao gồm tiêu đề IP và vùng tải tin.

Nhận dạng (Identification) - Trường 16 bit này là một số tuần tự tăng được gắn vào các thông điệp được gửi từ IP nguồn. Khi một thông điệp được gửi đến lớp IP và nó quá lớn so với một datagram, IP phân đoạn thông điệp thành nhiều datagram, đặt vào các datagram cùng một số nhận dạng. Số này được sử dụng ở đầu nhận để tập hợp các datagram này lại thành thông điệp ban đầu.

Các cờ (Flags) - Trường Flags xác định các khả năng phân đoạn có thể. Bit đầu tiên không được sử dụng và luôn có giá trị là 0. Bit tiếp theo được gọi là cờ DF (Don't Fragment). Cờ DF báo hiệu có cho phân đoạn (giá trị = 0) hay không (giá trị = 1). Bit tiếp theo là cờ MF (More Fragments), nói với đầu nhận là còn nhiều phân đoạn nữa đang đến. Khi MF được gán bằng 0, không còn phân đoạn nào cần truyền hay datagram chưa bao giờ bị phân đoạn.

Độ dời của phân đoạn (Fragment Offset) - Trường 13 bit này là một giá trị số được gán cho mỗi phân đoạn liên tiếp nhau. IP ở đích sử dụng fragment offset để tái hợp lại các phân đoạn theo thứ tự thích hợp. Giá trị offset tìm thấy ở đây biểu diễn giá trị độ dời là một số các đơn vị 8 byte.

Thời gian sống (Time to Live) - Trường bit này xác định lượng thời gian tính theo giây hay số chặng router hop mà datagram có thể tồn tại hoặc đi qua trước khi bị hủy. Mỗi router khảo sát và làm giảm trường này ít nhất là 1, hoặc số giây mà datagram bị trì hoãn bên trong router. Datagram bị hủy khi trường này đạt giá trị 0.

Một chặng (hop) hay một chặng router (router hop) tương quan với một router mà một datagram đi qua trên đường đến đích của nó. Nếu một datagram đi qua 5 router trước khi đến đích của nó được coi là cách 5 chặng (hop) hay 5 chặng router (router hop).

Giao thức (Protocol) - Trường giao thức 8 bit xác định giao thức sẽ nhận phần tải tin của datagram. Ví dụ một datagram với nhận dạng giao thức là 6 (00000110) được chuyển ngược lên chồng giao thức đến module TCP. Sau đây là một số giá trị giao thức thông dụng :

Tên giao thức	Nhận dạng giao thức
ICMP	1
TCP	6
UDP	17

Kiểm tra lỗi tiêu đề (Header Checksum) - Trường này giữ một giá trị 16 bit được tính toán để kiểm tra tính hợp lệ của riêng phần tiêu đề. Trường này được tính toán lại ở mỗi router khi giảm trường TTL.

Địa chỉ IP nguồn (Source IP Address) - Trường 32 bit này giữ địa chỉ của nguồn của datagram.

Địa chỉ IP đích (Destination IP Address) - Trường 32 bit này giữ địa chỉ đích của datagram và được IP đích sử dụng bởi để kiểm tra sự phân phối chính xác.

Các tùy chọn IP (IP Options) - Trường này hỗ trợ một số thiết đặt tiêu đề tùy ý sử dụng cho việc kiểm tra, gỡ rối vào an toàn. Các tùy chọn bao gồm Strict Source Route (một đường đi riêng qua một số router nhất định mà datagram phải theo), Internet Timestamp (một mẫu tin các nhãn thời gian ở mỗi router) và các giới hạn an toàn.

Đệm (Padding) - Trường các tùy chọn IP có chiều dài biến đổi. Trường Padding cung cấp các bit 0 bổ sung để chiều dài tổng cộng của phần tiêu đề là bội số chính xác của 32 bit. (Phần tiêu đề phải kết thúc sau một từ 32 bit bởi vì trường IHL đo chiều dài phần tiêu đề theo các từ 32 bit).

IP Data Payload - Trường này chứa dữ liệu dự định giao đến TCP hoặc UDP (trong lớp Vận chuyển), ICMP hay IGMP. Lượng dữ liệu có thể biến thiên đến hàng ngàn byte.

3.2.2 Đánh địa chỉ IP

Một địa chỉ IP là một địa chỉ nhị phân 32 bit. Địa chỉ 32 bit này được phân chia thành 4 đoạn 8 bit được gọi là các octet. Con người không thoải mái khi làm việc với các địa chỉ nhị phân 32 bit hay ngay cả các octet nhị phân 8 bit, vì thế địa chỉ IP hầu như luôn biểu diễn dưới dạng chấm thập phân. Dưới dạng chấm thập phân, mỗi octet được gán một số thập phân tương ứng. 4 giá trị thập phân ($4 \times 8 = 32$ bit) sau đó được phân biệt bằng các dấu chấm. 8 bit nhị phân có thể đại diện cho bất kỳ số nguyên nào từ 0 đến 255, vì thế các đoạn của một địa chỉ chấm thập phân là các số thập phân từ 0 đến 255. Có lẽ bạn đã thấy các ví dụ về các địa chỉ IP chấm thập phân trên máy của bạn, trong tài liệu này, hoặc trong các tài liệu TCP/IP khác. Một địa chỉ IP chấm thập phân trông như sau : 209.121.131.14.

Một phần của địa chỉ IP được sử dụng cho định danh mạng, và một phần của địa chỉ được sử dụng cho định danh host. Sự phức tạp của địa chỉ IP là phần định danh mạng biến đổi. Hầu hết các địa chỉ rơi vào các lớp địa chỉ sau :

- Các địa chỉ lớp A – 8 bit đầu tiên của địa chỉ IP được sử dụng cho định danh mạng. 24 bit cuối cùng được sử dụng cho định danh host.
- Các địa chỉ lớp B – 16 bit đầu tiên của địa chỉ IP được sử dụng cho định danh mạng. 16 bit cuối cùng được sử dụng cho định danh host.

- Các địa chỉ lớp C – 24 bit đầu tiên của địa chỉ IP được sử dụng cho định danh mạng. 8 bit cuối cùng được sử dụng cho định danh host.

Càng nhiều bit thì số tổ hợp bit sẽ lớn hơn. Ta có thể thấy, định dạng lớp A cung cấp một số nhỏ các định danh mạng và một số lớn các định danh host cho mỗi mạng. Một mạng lớp A có thể hỗ trợ khoảng 2^{24} , hay 16.777.216 host. Ngược lại, một mạng lớp C chỉ có thể cung cấp số định dạng host hay số lượng host ít (khoảng 2^8 , hay 256), nhưng nhiều định dạng mạng hơn.

Bạn có thể ngạc nhiên làm thế nào một máy tính hay một router biết một địa chỉ IP là địa chỉ lớp A, lớp B hay lớp C. Các nhà thiết kế TCP/IP đã đưa ra các luật địa chỉ sao cho có thể nhận biết được lớp của một địa chỉ của nó. Một vài bit đầu của địa chỉ nhị phân sẽ cho biết địa chỉ này là một địa chỉ lớp A, lớp B hay lớp C (xem **bảng 3-1**). Các luật để nhận dạng lớp địa chỉ như sau :

- Nếu địa chỉ nhị phân 32 bit bắt đầu với 1 bit 0, địa chỉ là một địa chỉ lớp A.
- Nếu địa chỉ nhị phân 32 bit bắt đầu với các bit 10, địa chỉ là một địa chỉ lớp B.
- Nếu địa chỉ nhị phân 32 bit bắt đầu với các bit 110, địa chỉ là một địa chỉ lớp C.

Sơ đồ địa chỉ này dễ dàng chuyển sang ký hiệu chấm thập phân bởi vì các luật này có ảnh hưởng đến giới hạn dãy các giá trị địa chỉ cho số hạng đầu tiên trong định dạng dấu chấm thập phân. Ví dụ, vì một địa chỉ lớp A phải có một bit 0 ở tận cùng bên trái trong octet đầu tiên, số hạng đầu tiên trong một địa chỉ chấm thập phân lớp A không thể cao hơn 127. Bạn sẽ học nhiều hơn về việc chuyển các số nhị phân sang thập phân ở phần sau của chương này. **Bảng 3-1** cho thấy các dãy địa chỉ cho các mạng lớp A, B và C. Chú ý rằng một vài dãy địa chỉ IP được sử dụng cho các mục đích đặc biệt. Bạn sẽ học nhiều hơn về các địa chỉ IP đặc biệt trong phần sau của chương này.

Bảng 3-1 Các giới hạn địa chỉ cho các mạng lớp A, B và C

<i>Lớp địa chỉ</i>	<i>Địa chỉ nhị phân phải bắt đầu với</i>	<i>Số hạng đầu tiên của địa chỉ chấm thập phân phải là</i>	<i>Các địa chỉ loại bỏ</i>
A	0	0 đến 127	10.0.0.0 đến 10.255.255.255 127.0.0.0 đến 127.255.255.255
B	10	128 đến 191	172.16.0.0 đến 172.31.255.255
C	110	192 đến 223	192.168.0.0 đến 192.168.255.255

Thông tin thêm

Các đặc tả Internet cũng xác định các địa chỉ dành riêng lớp D và lớp E. Bạn sẽ học về các địa chỉ lớp D và lớp E trong phần sau của chương này.

Người sở hữu mạng có thể chia mạng thành các mạng con nhỏ hơn được gọi là các subnet. Việc phân mạng con về cơ bản mượn một số bit của định danh host để tạo các mạng bổ sung trong mạng. Như bạn có thể đoán, các mạng lớp A và B, với các không gian địa chỉ định danh host lớn, giúp mở rộng việc phân chia mạng con. Việc phân mạng con cũng được sử dụng trên các mạng lớp C. Bạn sẽ học nhiều hơn về việc phân mạng con trong **Chương 4, “Phân mạng con”**.

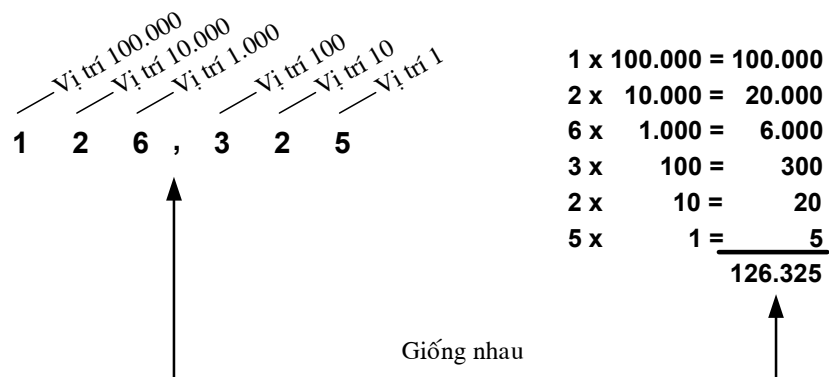
Thông tin thêm

Về mặt lý thuyết, mỗi máy tính trên Internet phải có một địa chỉ IP duy nhất. Trong thực tế, các máy tính trên mạng Internet vẫn có thể hoạt động được với các địa chỉ IP không đăng ký hoặc không duy nhất nhờ các thiết bị Chuyển đổi địa chỉ mạng (Network Address Translation - NAT). Bạn sẽ học nhiều hơn về các thiết bị NAT trong **chương 6, “Phân cứng mạng”**.

3.2.3 Chuyển một địa chỉ nhị phân 32 bit sang dạng chấm thập phân

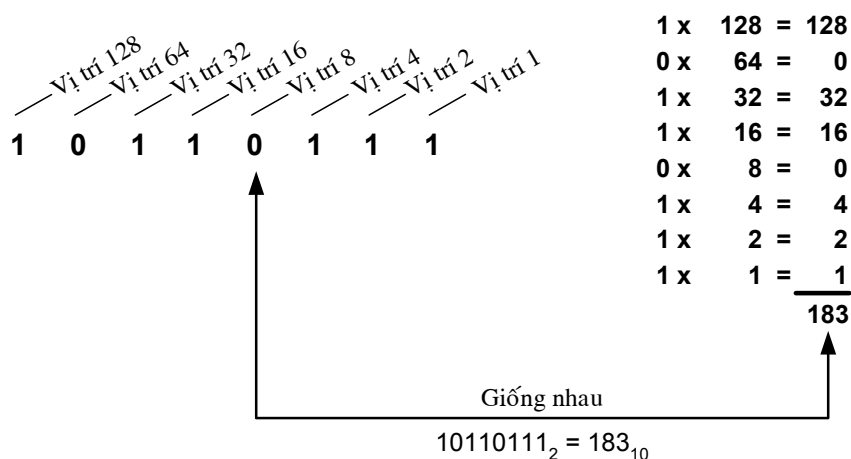
Các số nhị phân tương tự như các số thập phân, chỉ khác là thừa số nhân khi tính giá trị là 2 thay vì 10, và các chữ số cũng chỉ có hai giá trị 0 và 1, thay vì từ 0 đến 9 như số thập phân. Như **hình 3-4** cho thấy, một số nguyên thập phân bắt đầu với chữ số ở tận cùng bên phải, và mỗi chữ số kế tiếp sang trái có giá trị là bội số 10^n với n là vị trí của chữ số đó ($n=0$ đối với chữ số tận cùng bên phải). Giá trị của số thập phân là tổng của các giá trị của các vị trí thập phân. Ví dụ, giá trị của số thập phân 126.325 được xác định như sau : $(1 \times 10^5) + (2 \times 10^4) + (6 \times 10^3) + (3 \times 10^2) + (2 \times 10^1) + (5 \times 10^0) = 126.325$.

Hình 3-4 Hệ thống số thập phân



Một số nguyên nhị phân cũng bắt đầu bằng bit thấp nhất (ở tận cùng bên phải). Mỗi chữ số nhị phân kế tiếp sang trái là bội số 2^n , với n là vị trí của chữ số nhị phân đó ($n=0$ đối với chữ số tận cùng bên phải) (xem *hình 3-5*).

Hình 3-5 Hệ thống số nhị phân



Thông tin thêm

Các máy tính làm việc với các số nhị phân vì một mẫu bit 1 và 0 tương ứng dễ dàng với các trạng thái on và off sử dụng trong mạch số.

Để xác định giá trị thập phân tương ứng của một giá trị nhị phân, cộng tất cả các giá trị vị trí của bất kỳ bit nào có giá trị 1. Nhớ rằng địa chỉ IP bao gồm 4 octet mà mỗi octet phải được chuyển sang dạng thập phân một cách độc lập. Sau đây là một ví dụ cho thấy làm thế nào để chuyển một địa chỉ IP nhị phân 32 bit sang định dạng chấm thập phân.

Chuyển địa chỉ nhị phân 01011001 00011101 11001100 00011000.

1. Trước hết chia địa chỉ thành các octet 8 bit:

Octet 1: 01011001

Octet 2: 00011101

Octet 3: 11001100

Octet 4: 00011000

2. Chuyển mỗi octet thành một số thập phân. Tiến trình này được minh họa trong *bảng 3-2*.
3. Viết ra các giá trị thập phân tương ứng theo thứ tự từ trái sang phải, phân biệt các giá trị này bằng các dấu chấm.

Bảng 3-2 Chuyển một địa chỉ nhị phân sang dạng chấm thập phân

Octet	Giá trị nhị phân	Tính toán	Giá trị thập phân
1	01011001	$1+8+16+64$	89
2	00011101	$1+4+8+16$	29
3	11001100	$4+8+64+128$	204
4	00011000	$8+16$	24

Địa chỉ dạng dấu chấm thập phân là: 89.29.204.24

Bạn có thể xem thêm các ví dụ của cách chuyển đổi này trong phần **Thực hành** ở cuối chương này.

Thông tin thêm

Bạn có thể sử dụng phần mềm Calculator của hệ điều hành Windows để chuyển đổi giữa số nhị phân sang và số thập phân. Chọn mục View và chọn Scientific. Nút tùy chọn Bin chuyển máy tính sang chế độ nhị phân. Nút tùy chọn Dec chuyển số trở lại chế độ thập phân.

3.2.4 Chuyển một số thập phân sang một octet nhị phân

Tiến trình chuyển đổi một số thập phân sang nhị phân là một tiến trình ngược lại tiến trình được thể hiện trong **hình 3-5**. Nếu bạn cần chuyển một địa chỉ chấm thập phân sang địa chỉ nhị phân 32 bit, chuyển mỗi số riêng biệt trong địa chỉ sang một octet nhị phân và sau đó nối các octet này lại. Thủ tục sau cho thấy làm thế nào để chuyển đổi số thập phân 207 sang một octet nhị phân:

Thông tin thêm

Thủ tục này giả định bạn bắt đầu với một số thập phân biểu diễn một octet địa chỉ IP. Nếu số mà bạn đang chuyển cao hơn 255, bạn sẽ cần mở rộng giá trị vị trí nhị phân được thể hiện trong **hình 3-5** bằng cách thêm vào các vị trí bit cao hơn và phông theo thủ tục này với các giá trị cao hơn (256, 512, 1024 ...)

Để chuyển số thập phân 207 sang một octet nhị phân, theo các bước sau :

1. So sánh số thập phân bạn muốn chuyển (trong trường hợp này là 207) với số 128. Nếu số thập phân lớn hơn hay bằng 128, trừ 128 và ghi giá trị 1. Nếu số thập phân nhỏ hơn 128, trừ 0 và ghi giá trị 0.
 $207 > 128$
 $207 - 128 = 79$
Ghi giá trị 1 thay thế cho 128.
Kết quả là : 1

2. Lấy kết quả từ bước 1 (79 trong trường hợp này) và so sánh với giá trị 64. Nếu số thập phân lớn hơn hay bằng 64, trừ đi 64 và ghi giá trị 1. Nếu số thập phân nhỏ hơn 64, trừ 0 và ghi giá trị 0.
 $79 > 64$
 $79 - 64 = 15$
 Ghi 1 thay thế cho 64.
 Kết quả là : 11
3. Lấy kết quả từ bước 2 (ở đây là 15) và so sánh nó với số 32. Nếu số thập phân lớn hơn hay bằng 32, trừ 32 và ghi giá trị 1. Nếu số thập phân nhỏ hơn 32, trừ 0 và ghi giá trị 0.
 $15 < 32$
 $15 - 0 = 15$
 Ghi 0 thay thế cho 32
 Kết quả là : 110
4. So sánh kết quả từ bước 3 với số 16. Nếu số lớn hơn hay bằng 16, trừ 16 và ghi giá trị 1. Nếu số nhỏ hơn 16, trừ 0 và ghi giá trị 0.
 $15 < 32$
 $15 - 0 = 15$
 Ghi 0 thay thế cho 16
 Kết quả là : 1100
5. So sánh kết quả ở bước 4 với số 8. Nếu số thập phân lớn hơn hay bằng 8, trừ 8 và ghi giá trị 1. Nếu số thập phân nhỏ hơn 8, trừ 0 và ghi giá trị 0.
 $15 > 8$
 $15 - 8 = 7$
 Ghi 1 thay thế cho 8
 Kết quả là : 11001
6. So sánh kết quả của bước 5 với số 4. Nếu số thập phân lớn hơn hay bằng 4, trừ 4 và ghi giá trị 1. Nếu số thập phân nhỏ hơn 4, trừ 0 và ghi giá trị 0.
 $7 > 4$
 $7 - 4 = 3$
 Ghi 1 thay thế cho 4
 Kết quả là : 110011
7. So sánh kết quả của bước 6 với số 2. Nếu số thập phân lớn hơn hay bằng 2, trừ 2 và ghi giá trị 1. Nếu số thập phân nhỏ hơn 2, trừ 0 và ghi giá trị 0.
 $3 > 2$
 $3 - 2 = 1$
 Ghi 1 thay thế cho 2
 Kết quả là : 1100111
8. Nếu kết quả ở bước 7 là 1, ghi giá trị 1. Nếu giá trị ở bước 7 là 0, ghi giá trị 0.
 $1 = 1$
 Ghi giá trị 1
 Kết quả cuối cùng : 11001111

Bây giờ bạn đã chuyển xong số thập phân 207 sang giá trị nhị phân tương ứng của nó là 11001111.

3.2.5 Các lớp D và E

Như bạn đã học ở phần trước của chương này, các đặc tả IP cũng cung cấp các địa chỉ lớp D và lớp E.

Hầu hết các truyền thông TCP/IP đều là host-to-host (gửi từ một máy tính nguồn đến một máy tính đích) hay quảng bá (broadcast) - gửi đến tất cả các máy tính trên đoạn hay mạng. Mặt khác, các địa chỉ lớp D được sử dụng cho truyền đa hướng (multicasting). Một multicast là một thông điệp đơn gửi đến một mạng con của mạng. 4 bit đầu tiên bên trái của một địa chỉ mạng lớp D luôn bắt đầu với dạng nhị phân 1110, tương ứng với các số thập phân từ 224 đến 239.

Thông tin thêm

Giao thức quản lý nhóm Internet (The Internet Group Management Protocol _IGMP) là một giao thức lớp Internet sử dụng phương thức truyền đa hướng với địa chỉ lớp D.

Các RFC Internet đưa ra một số địa chỉ multicast cố định truyền đa hướng. Đây là nội dung nâng cao nên không được trình bày trong tài liệu này. Các mạng lớp E được xem là các mạng thử nghiệm. Thông thường chúng không được dùng trong bất kỳ môi trường sản xuất nào. 5 bit bên trái đầu tiên của một mạng lớp E luôn bắt đầu với mẫu nhị phân 11110, tương ứng với các số thập phân từ 240 đến 247.

3.2.6 Các địa chỉ IP đặc biệt

Một số địa chỉ IP có ý nghĩa đặc biệt không được gán cho các host riêng biệt. Một định danh host với tất cả các bit bằng 0 ám chỉ đến chính mạng đang xét (chuyển đến chính nó). Ví dụ, địa chỉ IP 129.152.0.0 chỉ đến mạng lớp B với định danh mạng là 129.152.

Một định danh với tất cả các bit bằng 1 biểu thị một địa chỉ quảng bá - broadcast. Một broadcast là một thông điệp gửi đến tất cả các host trên mạng. Địa chỉ IP 129.152.255.255 là địa chỉ broadcast của mạng lớp B với định danh mạng 129.152. (Chú ý rằng dạng thập phân 255 tương ứng với octet nhị phân toàn 1 (11111111)).

Địa chỉ 255.255.255.255 cũng có thể được dùng để broadcast trên mạng.

Các địa chỉ bắt đầu với 127 là các địa chỉ loopback. Một thông điệp được đánh địa chỉ loopback được gửi bởi phần mềm TCP/IP cục bộ đến chính nó. Địa chỉ loopback được dùng để kiểm tra xem phần mềm TCP/IP có hoạt động không. Địa chỉ loopback 127.0.0.1 thường được sử dụng nhất.

RFC 1597 cũng dành riêng một vài dãy địa chỉ IP cho các mạng riêng. Với giả định là các dãy địa chỉ riêng này không được kết nối vào Internet, vì thế các địa chỉ này không là duy nhất. Trên thế giới hiện nay, các dãy địa chỉ ẩn này thường được sử dụng cho mạng được bảo vệ, nằm sau các thiết bị chuyển đổi mạng :

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

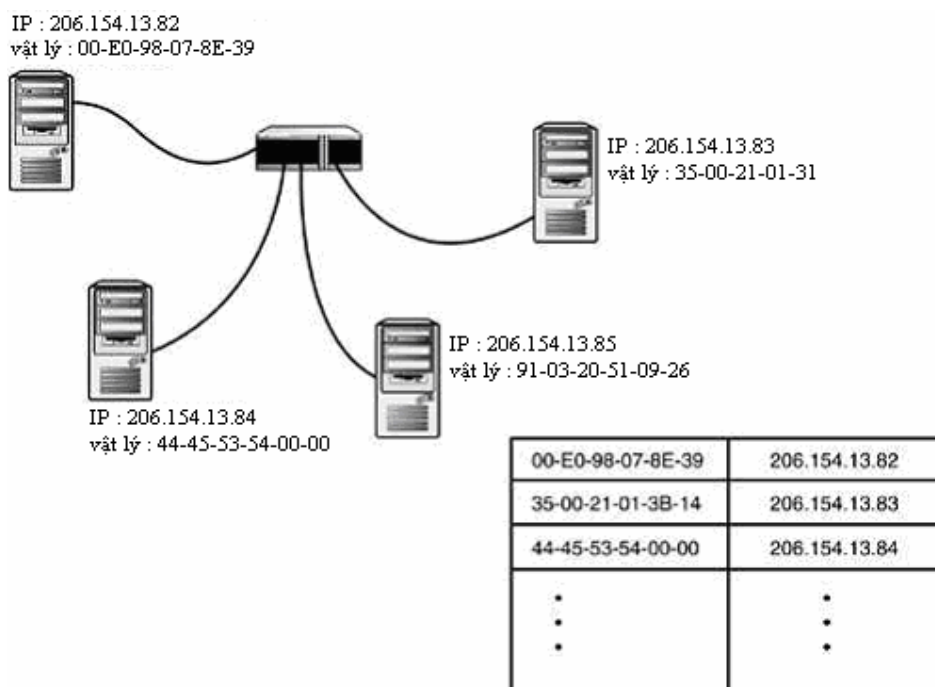
Bởi vì các dãy địa chỉ riêng này tách biệt với phần địa chỉ còn lại, toàn bộ dãy địa chỉ này có thể được sử dụng trong bất cứ mạng nào mà không sợ trùng lặp địa chỉ giữa các mạng. Một nhà quản lý mạng sử dụng các địa chỉ riêng này sẽ có nhiều không gian địa chỉ để phân chia mạng con hơn, và nhiều địa chỉ có thể gán hơn. Xem **chương 6, “Phần cứng mạng”** để biết thêm về các thiết bị chuyển đổi mạng.

3.3 Giao thức phân giải địa chỉ (ARP)

Như bạn đã học ở phần trước trong chương này, các máy tính trên một mạng cục bộ sử dụng giao thức lớp Internet được gọi là Giao thức phân giải địa chỉ - Address Resolution Protocol (ARP) để ánh xạ các địa chỉ IP vào các địa chỉ vật lý. Một host phải biết địa chỉ vật lý của bộ tương thích mạng đích để gửi bất kỳ dữ liệu nào đến nó. Vì lý do này, ARP là một giao thức rất quan trọng. Tuy nhiên, TCP/IP được thực hiện theo cách thức sao cho ARP và tất cả các chi tiết của việc chuyển đổi địa chỉ hầu như vô hình đối với người sử dụng. Bộ tương thích mạng được xác định bởi địa chỉ IP của nó. Địa chỉ IP phải được ánh xạ đến một địa chỉ vật lý để một thông điệp đến đích của nó. (Xem **chương 2, “Lớp truy cập mạng”**).

Mỗi host trên một đoạn mạng duy trì một bảng trong bộ nhớ được gọi là **bảng ARP** hay bộ nhớ nhanh ARP (*ARP cache*). ARP cache liên kết các địa chỉ IP của các host khác trên đoạn mạng với các địa chỉ vật lý (xem **hình 3-6**). Khi một host cần gửi dữ liệu đến một host khác trên đoạn, host kiểm tra bảng ARP để xác định địa chỉ vật lý của nơi nhận. Bảng ARP được hình thành một cách tự động. Nếu địa chỉ nhận dữ liệu hiện không được liệt kê trong bảng ARP, host gửi một broadcast được gọi là một khung yêu cầu ARP (xem **hình 3-6**).

Hình 3-6 ARP ánh xạ các địa chỉ IP vào các địa chỉ vật lý



Khung yêu cầu ARP chứa địa chỉ IP chưa được phân giải. Khung yêu cầu ARP cũng chứa địa chỉ IP và địa chỉ vật lý của host gửi yêu cầu. Các host khác trên đoạn mạng nhận yêu cầu ARP, và host có địa chỉ IP chưa phân giải hồi đáp bằng cách gửi địa chỉ vật lý của nó đến host gửi yêu cầu. Ánh xạ địa chỉ IP và địa chỉ vật lý được thêm vào bảng ARP của host yêu cầu.

Thông thường, các mục trong bảng ARP sẽ hết hạn sau một khoảng thời gian định trước. Khi thời gian sống của một mục ARP kết thúc, mục đó sẽ bị loại bỏ khỏi bảng. Tiến trình phân giải bắt đầu lại ở thời điểm kể khi mà host cần gửi dữ liệu đến địa chỉ IP của mục đã bị loại bỏ.

3.4 Giao thức phân giải địa chỉ ngược (RARP)

RARP là viết tắt của Reverse ARP (Giao thức phân giải địa chỉ ngược). RARP trái ngược với ARP. ARP được sử dụng khi biết địa chỉ IP nhưng không biết địa chỉ vật lý. RARP được sử dụng khi biết địa chỉ vật lý nhưng không biết địa chỉ IP. RARP thường được sử dụng kết hợp với giao thức BOOTP để khởi động các trạm làm việc không có ổ đĩa.

BOOTP (boot PROM)— Nhiều bộ tương thích mạng có một khe cắm trống để thêm một mạch tích hợp được gọi là một Rom boot. Chương trình bootPROM bắt đầu ngay khi máy tính được bật nguồn. Nó tải một hệ điều hành vào máy tính bằng cách

đọc từ một máy chủ mạng thay vì một ổ đĩa cục bộ. Hệ điều hành được tải tới thiết bị BOOTP được cấu hình trước một địa chỉ IP cụ thể.

3.5 Giao thức thông điệp điều khiển Internet (ICMP)

Dữ liệu gửi đến một máy tính ở xa thường đi qua một hay nhiều router; các router này có thể gặp phải một số vấn đề trong việc gửi thông điệp đến đích cuối cùng của nó. Các router sử dụng các thông điệp ICMP (Internet Control Message Protocol) để thông báo cho IP nguồn về các vấn đề này. ICMP cũng được dùng cho các chức năng chẩn đoán và xử lý sự cố khác.

Các thông điệp ICMP thông dụng nhất được liệt kê ở đây. Có một số ít các tình huống khác tạo ra các thông điệp ICMP nhưng tần suất xuất hiện của chúng khá thấp.

- **Echo Request và Echo Reply** - ICMP thường sử dụng trong quá trình kiểm tra. Khi một kỹ thuật viên sử dụng lệnh ping để kiểm tra kết nối với một host khác, anh ta đang sử dụng ICMP. Ping gửi một datagram đến một địa chỉ IP và yêu cầu máy tính đích đáp trả lại dữ liệu gửi trong một datagram hồi đáp. Các lệnh thực sự đang được sử dụng là ICMP Echo Request và Echo Reply.
- **Source Quench** - Nếu một máy tính đang gửi một lượng lớn dữ liệu đến một máy tính ở xa, lượng dữ liệu này có thể làm tràn ngập router. Router có thể sử dụng ICMP để gửi thông điệp Source Quench đến IP nguồn để yêu cầu nó giảm tốc độ truyền dữ liệu.
- **Destination Unreachable** - Nếu một router nhận một datagram không thể giao đến đích được, ICMP trả về một thông điệp Destination Unreachable đến IP nguồn. Một lý do mà router không thể phân phối thông điệp là mạng ngưng làm việc vì thiết bị hỏng hoặc đang được bảo trì.
- **Time Exceeded** - ICMP gửi thông điệp này đến IP nguồn nếu một datagram bị hủy do TTL = 0. Điều này cho thấy rằng đích cách khá nhiều hop so với giá trị TTL hiện tại, hoặc có các vấn đề trong bảng định tuyến làm cho datagram bị lặp liên tục qua cùng một nhóm các router.

Một vòng lặp định tuyến xảy ra khi một datagram lặp vòng liên tục qua cùng các router và không bao giờ đến đích của nó. Giả sử 3 router được đặt ở Los Angeles, San Francisco, và Denver. Router ở Los Angeles gửi các datagram đến San Francisco, router ở San Francisco gửi chúng đến Denver, và router ở Denver gửi chúng trở lại Los Angeles. Datagram bị kẹt trong vòng lặp và sẽ xoay vòng liên tục qua 3 router này cho đến khi TTL = 0. Vòng lặp định tuyến là điều không mong muốn, nhưng đôi khi nó

cũng xuất hiện, có thể do nhà quản trị mạng đặt các mục định tuyến tĩnh trong một bảng định tuyến.

- **Fragmentation Needed** - ICMP gửi thông điệp này nếu nó nhận một datagram với bit Don't Fragment được thiết lập và nếu router cần phân đoạn datagram để chuyển tiếp nó đến router kế tiếp hay đích.

Tóm tắt

Trong chương này bạn đã học về các giao thức lớp Internet là IP, ARP, RARP và ICMP. IP cung cấp một hệ thống đánh địa chỉ độc lập phần cứng để phân phối dữ liệu trên mạng. Bạn đã học về các định dạng địa chỉ IP nhị phân và chấm thập phân và về các lớp địa chỉ IP A, B, C, D và E. Bạn cũng đã học về ARP, một giao thức phân giải các địa chỉ IP sang các địa chỉ vật lý. RARP ngược với ARP, một máy tính không có ổ đĩa sẽ dùng giao thức này để truy vấn một máy chủ về địa chỉ IP của chính nó. ICMP là một giao thức sử dụng cho các chẩn đoán và kiểm tra.

Thực hành

Chuyển các octet nhị phân sau sang các số thập phân tương ứng của chúng.

00101011	Kết quả = 43
01010010	Kết quả = 82
11010110	Kết quả = 214
10110111	Kết quả = 183
01001010	Kết quả = 74
01011101	Kết quả = 93
10001101	Kết quả = 141
11011110	Kết quả = 222

Chuyển các số thập phân sau sang các octet nhị phân tương ứng của chúng.

13	Kết quả = 00001101
184	Kết quả = 10111000
238	Kết quả = 11101110
37	Kết quả = 00100101
98	Kết quả = 01100010
161	Kết quả = 10100001
243	Kết quả = 11110011
189	Kết quả = 10111101

Chuyển các địa chỉ IP 32 bit sau sang dạng chấm thập phân.

11001111 00001110 00100001 01011100	Kết quả = 207.14.33.92
00001010 00001101 01011001 01001101	Kết quả = 10.13.89.77
10111101 10010011 01010101 01100001	Kết quả = 189.147.85.97

CHƯƠNG

4

PHÂN MẠNG CON

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Phân mạng con**
- **Các mặt nạ mạng con**
- **Ký hiệu CIDR**

Việc phân mạng con là một tiến trình chia một khối các địa chỉ IP được gán cho một mạng lớp A, B hoặc C thành các khối địa chỉ nhỏ hơn. Chương này cho thấy nhu cầu và lợi ích của việc phân mạng con, cũng như các bước và các thủ tục bạn phải tuân theo để tạo ra một mặt nạ mạng con.

Kết thúc chương này, bạn sẽ có thể :

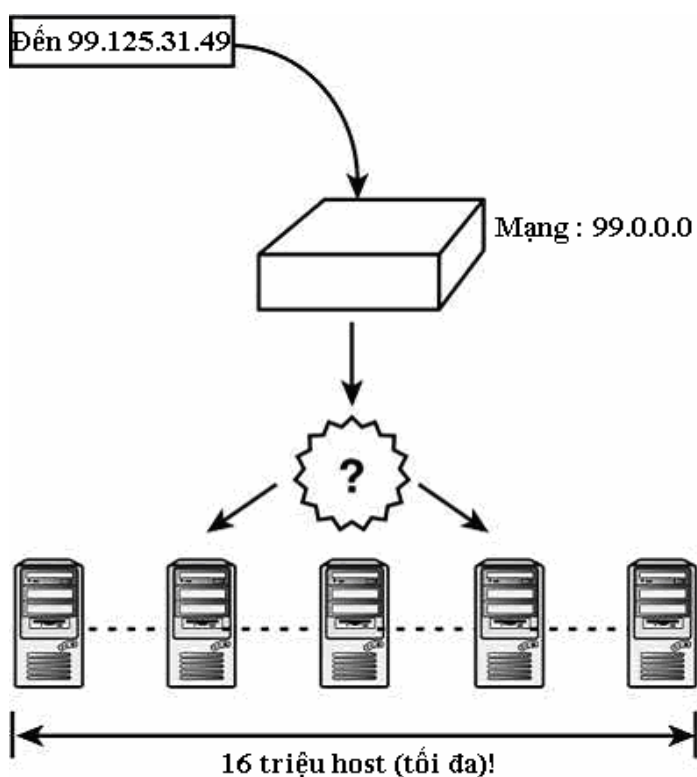
- Giải thích các mạng con và các siêu mạng được sử dụng như thế nào
- Giải thích lợi ích của việc phân mạng con
- Phát triển một mặt nạ mạng con cho nhu cầu công việc
- Mô tả siêu mạng và ký hiệu CIDR.

4.1 Các mạng con trong TCP/IP

Hệ thống lớp địa chỉ được mô tả trong **Chương 3, “Lớp Internet”**, cho phép tất cả các host có thể xác định định danh mạng trong một địa chỉ IP và gửi một datagram đến đúng mạng. Tuy nhiên, việc xác định một đoạn mạng bằng định danh mạng lớp A, B hay C của nó có một số giới hạn. Giới hạn chính của hệ thống lớp địa chỉ là nó không cung cấp bất kỳ sự phân chia luận lý nào vùng không gian địa chỉ dưới mức mạng.

Hình 4-1 cho thấy một mạng lớp A. Như đã mô tả trong chương trước, các datagram đến chính xác gateway và truyền vào không gian địa chỉ 99.0.0.0. Tuy nhiên, bức tranh của vấn đề sẽ phức tạp hơn khi bạn xem xét làm thế nào để phân phối datagram khi nó đi vào không gian địa chỉ 99.0.0.0. Một mạng lớp A có phạm vi trên 16 triệu định danh host. Mạng này có thể bao gồm hàng triệu host, đường đi – đây là một con số rất lớn trong phạm vi một mạng con đơn lẻ.

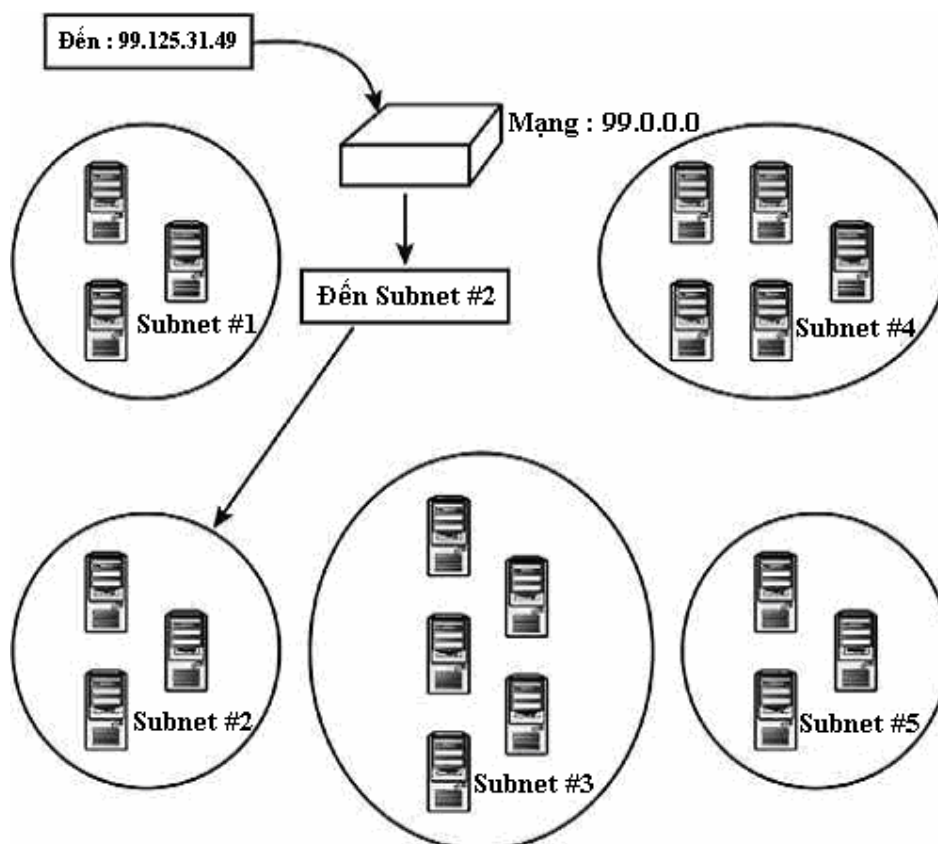
Hình 4-1 Phân phối dữ liệu đến một mạng lớp A



Để phân phối hiệu quả trên một mạng lớn, không gian địa chỉ có thể được phân nhỏ thành các đoạn mạng nhỏ hơn (xem **hình 4-2**). Việc phân đoạn thành các mạng vật lý riêng biệt làm tăng dung lượng toàn bộ của mạng và do đó làm cho mạng có thể sử dụng phần không gian địa chỉ nhiều hơn. Trong trường hợp thông thường, các router phân tách các đoạn trong không gian địa chỉ cần một số chỉ định về nơi phân phối dữ liệu. Chúng không thể dùng định danh mạng vì mỗi datagram gửi đến mạng có

cùng định danh mạng (99.0.0.0). Mặc dù có thể tổ chức không gian địa chỉ bằng định danh host, nhưng một giải pháp như vậy sẽ rất cồng kềnh, không mềm dẻo và hoàn toàn không thực tế trên một mạng với 16 triệu host. Giải pháp thực tế duy nhất là phân chia không gian địa chỉ nào đó bên dưới định danh mạng để các host và các router có thể dựa trên địa chỉ IP để biết đoạn mạng nào có thể nhận phân phối.

Hình 4-2 Tổ chức mạng để phân phối hiệu quả

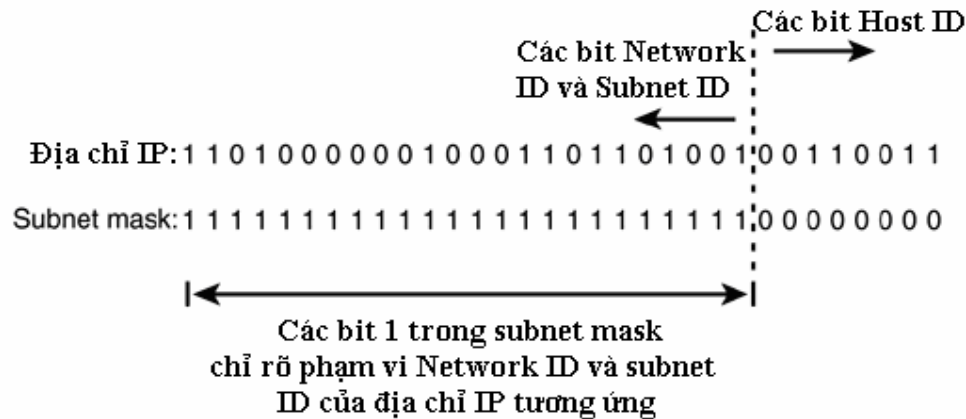


TCP/IP cung cấp một cấp tổ chức luận lý thứ hai bên dưới định danh mạng thông qua một khái niệm được gọi là subnet. Một **subnet (mạng con)** là một phân chia luận lý không gian địa chỉ mạng. Các router có thể phân phối một datagram đến một địa chỉ subnet trong mạng (thường tương ứng với một đoạn mạng), và một khi datagram đến subnet, nó có thể được phân giải thành một địa chỉ vật lý sử dụng ARP (xem **chương 3, “Lớp Internet”**).

Bạn có thể hỏi địa chỉ subnet này từ đâu, vì tất cả 32 bit của địa chỉ IP được sử dụng cho định danh mạng và định danh host. Câu trả lời là các nhà thiết kế TCP/IP cung cấp một phương tiện để mượn một số bit từ định danh host để tạo ra một địa chỉ subnet. Một thông số được gọi là mặt nạ subnet cho biết bao nhiêu địa chỉ được sử dụng cho định danh subnet và bao nhiêu còn lại cho định danh host thật sự.

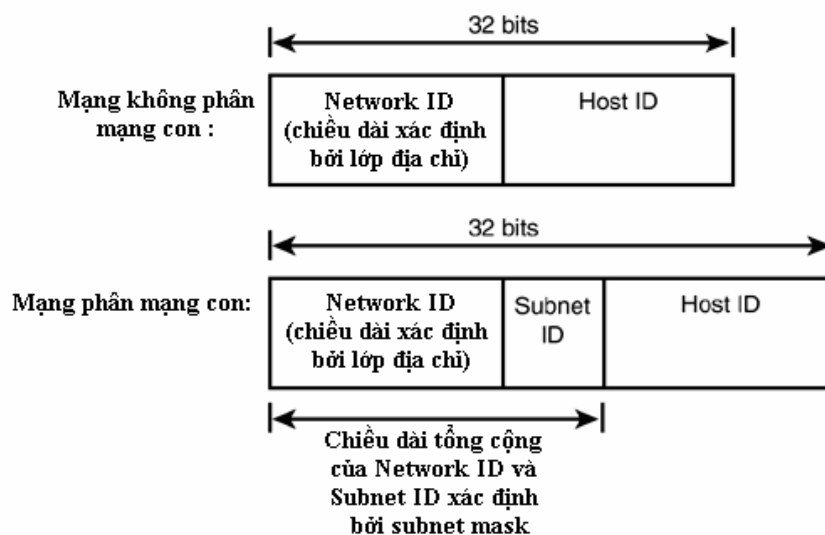
Giống một địa chỉ IP, một mặt nạ mạng con (subnet mask) là một số nhị phân 32 bit. Các bit của subnet mask được sắp xếp theo một dạng thức cho biết định dạng subnet của địa chỉ IP mà mặt nạ này kết hợp. **Hình 4-3** cho thấy một cặp địa chỉ IP/subnet mask. Mỗi vị trí bit trong subnet mask đại diện cho một vị trí bit trong địa chỉ IP.

Hình 4-3 Một cặp địa chỉ IP/subnet mask



Subnet mask sử dụng một bit 1 cho mỗi bit trong địa chỉ IP thuộc định danh mạng và định danh subnet. Subnet mask sử dụng một bit 0 để chỉ định bất kỳ bit nào trong địa chỉ IP thuộc định danh host. Bạn có thể nghĩ subnet mask như là một bản đồ sử dụng để đọc địa chỉ IP. **Hình 4.4** cho thấy sự phân phối các bit địa chỉ trong một mạng được phân mạng con so với một mạng không được phân mạng con.

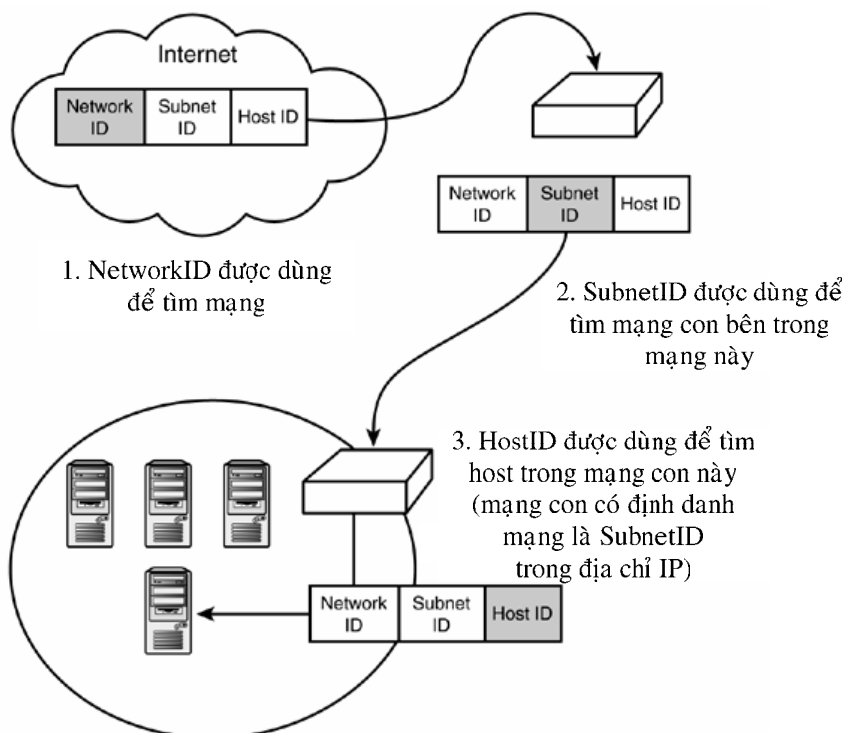
Hình 4-4 Phân phối các bit địa chỉ trong một mạng phân mạng con so với mạng không phân mạng con



Các bảng định tuyến sử dụng trong các router và các host trên một mạng phân mạng con sẽ chứa thông tin về subnet mask cùng với mỗi địa chỉ IP. (Bạn sẽ học nhiều

hơn về định tuyến trong **chương 7, "Định tuyến"**). Như **hình 4-5** cho thấy, một datagram đang tới được định tuyến đến mạng sử dụng trường định danh mạng xác định bởi lớp địa chỉ (xem **chương 3, "Lớp Internet"**). Khi datagram đến mạng này, nó được định tuyến đến phân đoạn thích hợp sử dụng định danh subnet. Sau khi đến phân đoạn, định danh host được sử dụng để phân phối datagram đến đúng máy tính.

Hình 4-5 Các datagram đang đến trên một mạng phân mạng con



4.2 Chuyển đổi một Subnet Mask sang dạng chấm thập phân

Nhà quản lý mạng thường gán một subnet mask cho mỗi host như một phần cấu hình TCP/IP. Nếu host nhận một địa chỉ IP thông qua DHCP (xem **chương 9, "Giao thức cấu hình host động - DHCP"**), DHCP server có thể gán một subnet mask cùng với địa chỉ IP.

Các subnet mask phải được tính toán cẩn thận và phải phản ánh tổ chức bên trong của mạng. Tất cả các host trong một subnet phải có cùng định danh subnet và subnet mask. Để hiệu quả cho người sử dụng, subnet mask thường được biểu diễn bằng ký hiệu chấm thập phân tương tự như ký hiệu sử dụng cho một địa chỉ IP.

Bạn hãy nhớ lại phần trước, subnet mask là một số nhị phân 32 bit. Bạn có thể chuyển subnet mask nhị phân sang một địa chỉ chấm thập phân sử dụng kỹ thuật chuyển đổi địa chỉ được mô tả trong **chương 3, "Lớp Internet"**. Một subnet mask thường dễ chuyển đổi sang dạng chấm thập phân hơn một địa chỉ IP. Các bit subnet

mask đại diện cho định danh mạng của địa chỉ IP và định danh subnet là các bit 1. Các bit đại diện cho định danh host của địa chỉ IP là các bit 0. Điều này có nghĩa là (với một số ngoại lệ hiếm có) tất cả các bit 1 đều bên trái và các bit 0 đều ở bên phải. Bất kỳ octet toàn bit 1 nào trong subnet mask sẽ mang giá trị 255 (nhị phân 11111111) trong subnet mask chấm thập phân. Bất kỳ octet toàn bit 0 nào sẽ mang giá trị 0 (nhị phân 00000000) trong subnet mask. Vì thế subnet mask thông thường có dạng sau :

111111111111111111111111100000000

được thể hiện dưới dạng ký hiệu chấm thập phân như sau 255.255.255.0. Tương tự như vậy, subnet mask

```
11111111111111110000000000000000
```

được thể hiện dưới dạng chấm thập phân là 255.255.0.0.

Như bạn có thể thấy, rất dễ xác định giá trị chấm thập phân tương ứng của subnet mask chia cắt địa chỉ theo giới hạn octet. Tuy nhiên, một số subnet mask không chia địa chỉ thành các octet. Trong trường hợp đó, bạn chỉ đơn giản xác định giá trị thập phân tương ứng của octet hỗn hợp này (octet chứa cả bit 1 và bit 0).

Để chuyển một subnet mask nhị phân sang ký hiệu chấm thập phân, theo các bước sau :

1. Chia subnet mask thành các octet bằng cách viết subnet mask nhị phân 32 bit thành các nhóm dưới dạng các octet :

11111111.11111111.11110000.00000000

2. Đối với mỗi octet toàn 1, ghi giá trị 255. Đối với mỗi octet toàn 0, ghi giá trị 0.
3. Chuyển đổi octet hỗn hợp sang thập phân sử dụng kỹ thuật chuyển đổi nhị phân đã được đề cập trong **chương 3, “Lớp Internet”**. Kết quả là tổng tất cả các giá trị vị trí bit (xem **hình 3-5**).
4. Viết địa chỉ chấm thập phân cuối cùng :

255.255.240.0

Trong hầu hết trường hợp, subnet mask chấm thập phân này là giá trị bạn sẽ nhập vào trong quá trình cấu hình TCP/IP cho máy tính.

4.3 Làm việc với các mạng con

Subnet mask xác định bao nhiêu bit sau định danh mạng sẽ được dùng cho định danh subnet. Định danh subnet có thể có chiều dài biến đổi, tùy thuộc vào giá trị mà bạn chọn cho subnet mask. Khi định danh subnet lớn hơn thì ít bit dùng cho định danh host hơn. Nói cách khác, nếu mạng của bạn có nhiều subnet, số host của bạn sẽ bị giới hạn ít hơn trên mỗi subnet. Nếu bạn có một ít subnet và chỉ đòi hỏi một số bit cho định danh subnet, bạn có thể có nhiều host trên một subnet.

Thông tin thêm

Chú ý rằng lớp địa chỉ cũng xác định bao nhiêu bit có thể dùng cho định dạng subnet. Mặt nạ

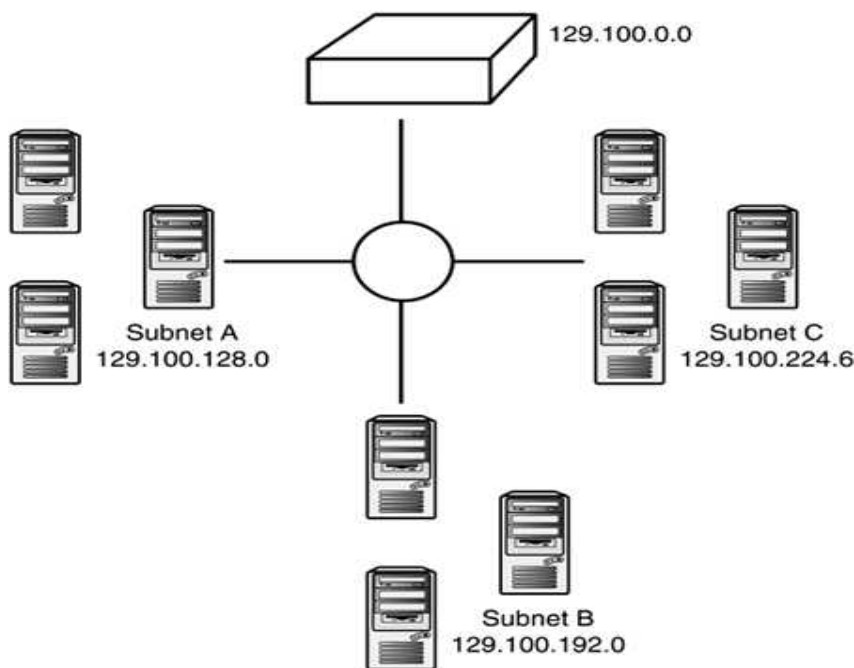
11111111111111111111000000000000

chỉ ra 19 bit cho định danh mạng và định danh subnet. Nếu mặt nạ này được sử dụng với một địa chỉ lớp B (có định danh mạng 16 bit), chỉ 3 bit có thể dùng cho việc phân chia mạng con. Với cùng mặt nạ này sử dụng với một địa chỉ lớp A (có định danh mạng 8 bit); 11 bit có thể dùng cho việc phân chia mạng con.

Việc ấn định các định danh subnet (phân định một subnet mask) dựa trên cấu hình mạng của bạn. Giải pháp tối ưu là bố trí mạng của bạn trước và xác định số và vị trí của các đoạn mạng, sau đó gán cho mỗi đoạn một định danh subnet. Bạn sẽ cần đủ số bit subnet để gán cho mỗi subnet một định danh subnet duy nhất. Nếu có thể, bạn nên để dành một số định danh subnet cho việc mở rộng mạng sau này.

Một ví dụ đơn giản của việc phân chia mạng con là một mạng lớp B mà octet thứ ba (phần thứ ba trong địa chỉ IP chấm thập phân) được dành riêng cho số subnet. Trong **hình 4-6**, mạng 129.100.0.0 được chia thành 4 mạng con. Các địa chỉ IP trên mạng có subnet mask là 255.255.255.0, cho biết định danh mạng và subnet mask gồm 3 octet của địa chỉ IP. Vì địa chỉ là một địa chỉ lớp B (xem **chương 3, “Lớp Internet”**), hai octet đầu tiên trong địa chỉ hình thành định dạng mạng. Do đó, Subnet A trong **hình 4-6** do đó có các thông số sau :

Hình 4-6 Một mạng lớp B được phân mạng con



Định danh mạng : 129.100. 0. 0

Định danh subnet : 0 . 0.128 . 0

Các định danh host không được gán các giá trị toàn 1 hoặc toàn 0. Do đó, cấu hình được hiển thị trong **hình 4.6** do đó có thể hỗ trợ 254 subnet và 254 địa chỉ cho mỗi subnet. Đây là một giải pháp rất thực tế miễn là bạn không có hơn 254 địa chỉ trên một subnet và có một địa chỉ mạng lớp B.

Thường không cần phải gán toàn bộ một octet cho định dạng subnet. Ví dụ trên một mạng lớp C, nếu bạn gán toàn bộ một octet cho định danh subnet, bạn sẽ không còn bit nào dành cho định danh host. Thậm chí trên một mạng lớp B, bạn có thể không sử dụng toàn bộ một octet cho định danh subnet, bởi vì bạn có lẽ cần nhiều địa chỉ host cho hơn 254 host trên một subnet. Các luật phân chia mạng con không đòi hỏi bạn phải đặt định danh subnet vào một octet. Khái niệm một định danh subnet không nằm trong giới hạn của một octet thì dễ hình dung trong dạng nhị phân nhưng lại trở nên hơi khó hiểu khi bạn trở về dạng chấm thập phân.

Xem xét một mạng lớp C phải được chia thành các subnet nhỏ. Các luật đánh địa chỉ lớp cho ta 8 bit sau định danh mạng để sử dụng cho định danh subnet và định danh host trong mạng lớp C. Bạn có thể chỉ định 3 trong số các bit này làm định danh subnet sử dụng subnet mask sau :

111111111111111111111111111100000

5 bit còn lại sẽ dùng cho định dạng host. 3 bit của định danh subnet cho ta 8 mẫu bit có thể. Như đã đề cập từ trước, các luật phân chia mạng con chính thức không cho phép các dạng toàn 1 và toàn 0 trong các định danh subnet (mặc dù nhiều router thực sự hỗ trợ việc gán các định danh subnet toàn 1 hay toàn 0). Trong bất cứ trường hợp nào, cấu hình này có thể cho 6 subnet nhỏ. 5 vị trí bit còn lại của định danh host cho ta 32 mẫu bit kết hợp. Loại trừ mẫu toàn 0 và toàn 1, mỗi subnet có thể có 30 host.

Để biểu diễn subnet mask này dưới dạng chấm thập phân, theo thủ tục mô tả trong phần trước :

Thêm các dấu chấm để đánh dấu biên của octet:

1. 11111111.11111111.11111111.11100000

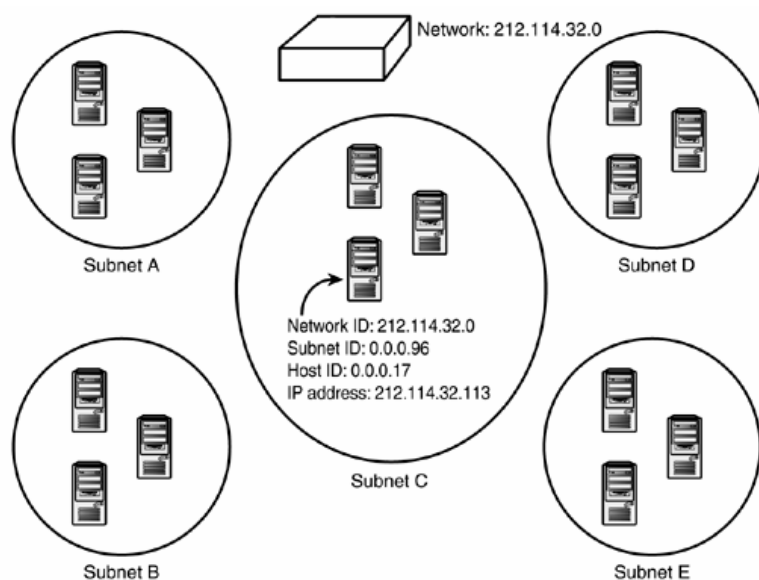
2. Viết giá trị 255 cho mỗi octet toàn 1. Chuyển đổi octet hỗn hợp sang thập phân :

$128+64+32=224$

Dạng chấm thập phân của subnet mask này là 255.255.255.224

Giả sử bạn bắt đầu đặt các host trên mạng được phân mạng con này (xem **hình 4-7**). Vì mạng này là một mạng lớp C, 3 octet đầu tiên sẽ như nhau cho tất cả các host. Để có được octet thứ tư của địa chỉ IP, chỉ đơn giản viết định danh subnet và định danh host dưới dạng nhị phân theo các bit tương ứng của chúng. Ví dụ trong **hình 4-7**, trường định danh subnet cho Subnet C có mẫu bit là 011. Vì mẫu này ở tận cùng bên trái của octet, các vị trí bit của định danh subnet thực sự là mẫu 01100000, nghĩa là số subnet là 96. Nếu định danh host là 17 (nhị phân là 10001), octet thứ tư là 01110001, được chuyển sang 113. Do đó, địa chỉ IP của host này do đó sẽ là 212.114.32.113.

Hình 4-7 Một mạng lớp C được phân mạng con



Bảng 4-1 cho thấy các giá trị tương ứng dạng nhị phân của các subnet mask. Bảng này cho thấy tất cả các mẫu subnet mask hợp lệ. Cột mô tả trong **bảng 4-1** cho biết có bao nhiêu bit 1 bổ sung theo sau các bit 1 trong mặt nạ mặc định của lớp tương ứng. Các bit mặt nạ này dành cho định danh subnet. Ví dụ, mặt nạ lớp A mặc định có 8 bit 1; hàng cho thấy hai bit mặt nạ nghĩa là 8 bit cộng thêm 2, hay tổng cộng là 10 bit 1 trong subnet mask.

Bảng 4-1 Subnet Mask dạng dấu chấm thập phân và dạng nhị phân

Mô tả	Dạng dấu chấm thập phân	Mẫu nhị phân
Lớp A		
Mặt nạ mặc định	255.0.0.0	11111111 00000000 00000000 00000000
1 bit subnet	255.128.0.0	11111111 10000000 00000000 00000000
2 bit subnet	255.192.0.0	11111111 11000000 00000000 00000000
3 bit subnet	255.224.0.0	11111111 11100000 00000000 00000000
4 bit subnet	255.240.0.0	11111111 11110000 00000000 00000000
5 bit subnet	255.248.0.0	11111111 11111000 00000000 00000000
6 bit subnet	255.252.0.0	11111111 11111100 00000000 00000000
7 bit subnet	255.254.0.0	11111111 11111110 00000000 00000000
8 bit subnet	255.255.0.0	11111111 11111111 00000000 00000000
9 bit subnet	255.255.128.0	11111111 11111111 10000000 00000000
10 bit subnet	255.255.192.0	11111111 11111111 11000000 00000000
11 bit subnet	255.255.224.0	11111111 11111111 11100000 00000000
12 bit subnet	255.255.240.0	11111111 11111111 11110000 00000000
13 bit subnet	255.255.248.0	11111111 11111111 11111000 00000000
14 bit subnet	255.255.252.0	11111111 11111111 11111100 00000000
15 bit subnet	255.255.254.0	11111111 11111111 11111110 00000000
16 bit subnet	255.255.255.0	11111111 11111111 11111111 00000000
17 bit subnet	255.255.255.128	11111111 11111111 11111111 10000000
18 bit subnet	255.255.255.192	11111111 11111111 11111111 11000000
19 bit subnet	255.255.255.224	11111111 11111111 11111111 11100000
20 bit subnet	255.255.255.240	11111111 11111111 11111111 11110000
21 bit subnet	255.255.255.248	11111111 11111111 11111111 11111000
22 bit subnet	255.255.255.252	11111111 11111111 11111111 11111100
Lớp B		

Mô tả	Dạng dấu chấm thập phân	Mẫu nhị phân
Mặt nạ mặc định	255.255.0.0	11111111 11111111 00000000 00000000
1 bit subnet	255.255.128.0	11111111 11111111 10000000 00000000
2 bit subnet	255.255.192.0	11111111 11111111 11000000 00000000
3 bit subnet	255.255.224.0	11111111 11111111 11100000 00000000
4 bit subnet	255.255.240.0	11111111 11111111 11110000 00000000
5 bit subnet	255.255.248.0	11111111 11111111 11111000 00000000
6 bit subnet	255.255.252.0	11111111 11111111 11111100 00000000
7 bit subnet	255.255.254.0	11111111 11111111 11111110 00000000
8 bit subnet	255.255.255.0	11111111 11111111 11111111 00000000
9 bit subnet	255.255.255.128	11111111 11111111 11111111 10000000
10 bit subnet	255.255.255.192	11111111 11111111 11111111 11000000
11 bit subnet	255.255.255.224	11111111 11111111 11111111 11100000
12 bit subnet	255.255.255.240	11111111 11111111 11111111 11110000
13 bit subnet	255.255.255.248	11111111 11111111 11111111 11111000
14 bit subnet	255.255.255.252	11111111 11111111 11111111 11111100
Lớp C		
Mặt nạ mặc định	255.255.255.0	11111111 11111111 11111111 00000000
1 bit subnet	255.255.255.128	11111111 11111111 11111111 10000000
2 bit subnet	255.255.255.192	11111111 11111111 11111111 11000000
3 bit subnet	255.255.255.224	11111111 11111111 11111111 11100000
4 bit subnet	255.255.255.240	11111111 11111111 11111111 11110000
5 bit subnet	255.255.255.248	11111111 11111111 11111111 11111000
6 bit subnet	255.255.255.252	11111111 11111111 11111111 11111100

Thông tin thêm

Một số mẫu trong **bảng 4.1** không thực tế lắm, và chỉ được dành cho các mục đích minh họa. Ví dụ, một mạng lớp C với 6 bit subnet chỉ có 2 bit dành để gán cho các định dạng host. Với 2 bit này, địa chỉ toàn 1 (11) được chỉ định cho broadcast, và địa chỉ toàn 0 (00) không được sử dụng. Do đó, subnet này chỉ giới hạn cho 2 host.

4.4 Định tuyến tên miền Internet không phân lớp

Các địa chỉ lớp A đã không còn, và các địa chỉ lớp B thì nhanh chóng bị cạn kiệt. Nhiều địa chỉ lớp C vẫn còn, nhưng không gian địa chỉ nhỏ của một mạng lớp C (tối đa 254 host) là một giới hạn nghiêm trọng trong cuộc chạy đua nâng cao số lượng thuê bao của các nhà cung cấp dịch vụ Internet (ISPs). Có thể cấp một dãy các địa chỉ mạng lớp C cho một mạng cần hơn 254 địa chỉ. Tuy nhiên, việc xử lý nhiều mạng lớp C này như là các thực thể riêng rẽ khi chúng cùng ở một nơi chỉ làm rối các bảng định tuyến một cách không cần thiết.

Định tuyến tên miền Internet không phân lớp (Classless Internet Domain Routing - CIDR) là một kỹ thuật cho phép một khối các định danh mạng được xem như là một thực thể đơn trong bảng định tuyến. CIDR nhóm một dãy các định danh mạng vào một mục địa chỉ đơn sử dụng một khái niệm được gọi là *supernet mask*. Bạn có thể nghĩ về một supernet mask như là một thứ gì đó ngược lại với một subnet mask. Thay vì chỉ định các bit thêm vào để nhận dạng mạng, supernet mask thực ra tách các bit khỏi định danh mạng. Do đó, các địa chỉ trong dãy được nhận dạng bởi các bit địa chỉ mạng mà các mạng trong dãy cùng có như nhau. Ví dụ, một ISP có thể được cấp tất cả các địa chỉ lớp C trong dãy

204.21.128.0 (11001100000101011000000000000000)
đến 204.21.255.255 (11001100000101011111111111111111).

Trong trường hợp này, các địa chỉ mạng giống nhau chính xác đến bit thứ 17 bắt đầu từ bên trái. Supernet mask do đó sẽ là

11111111111111111100000000000000, tương ứng với mặt nạ chấm thập phân là 255.255.128.0.

Khối địa chỉ này được nhận diện bằng cách sử dụng địa chỉ thấp nhất trong dãy theo sau bởi supernet mask. Một dạng thông thường của cặp địa chỉ/mask CIDR cho thấy số bit mặt nạ sau địa chỉ với một dấu phân cách (/) giữa địa chỉ và mặt nạ. Do đó, dãy CIDR trong ví dụ trước sẽ được viết là 204.21.128.0/17.

Dĩ nhiên, việc đánh địa chỉ CIDR chỉ có thể được sử dụng nếu các router trên mạng hỗ trợ nó.

Tóm tắt

Việc phân chia mạng con thêm một cấp trung gian cho cấu trúc đánh địa chỉ IP, cung cấp một phương tiện để nhóm các địa chỉ IP trong không gian địa chỉ dưới định danh mạng. Việc phân chia mạng con là một tính năng thông thường trên các mạng có nhiều đoạn vật lý tách biệt bởi các router.

CHƯƠNG LỚP

5 VẬN CHUYỂN

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Các giao thức hướng kết nối và không kết nối.**
- **Cổng và socket**
- **TCP**
- **UDP**

Lớp vận chuyển cung cấp một giao tiếp cho các ứng dụng mạng, bổ sung tính năng kiểm tra lỗi, điều khiển luồng và xác thực các lưu thông trên mạng. Chương này trình bày một số khái niệm quan trọng của lớp vận chuyển và giới thiệu qua hai giao thức TCP và UDP.

Kết thúc chương này bạn sẽ có thể :

- **Nắm được các nhiệm vụ cơ bản của lớp vận chuyển**
- **Giải thích được sự khác nhau giữa giao thức hướng kết nối và không kết nối**
- **Giải thích được việc các giao thức lớp vận chuyển cung cấp một giao tiếp cho các ứng dụng mạng qua các cổng và socket như thế nào**
- **Trình bày được sự khác nhau giữa TCP và UDP**
- **Nhận biết các trường trong phần tiêu đề TCP**
- **Mô tả được TCP mở và đóng kết nối như thế nào**
- **Mô tả được TCP sắp xếp tuần tự và báo nhận cho các dữ liệu truyền như thế nào**
- **Nhận biết các trường tạo thành tiêu đề UDP.**

5.1 Giới thiệu về lớp vận chuyển

Như đã trình bày trong **chương 3** và **chương 4**, lớp Internet TCP/ IP đã bao hàm đầy đủ các giao thức cơ bản, cung cấp thông tin địa chỉ cần thiết để dữ liệu có thể được truyền trên mạng. Tuy nhiên, việc gán địa chỉ và định tuyến chỉ là một phần của bức tranh tổng thể. Các nhà phát triển TCP/IP biết rằng cần phải có một lớp cao hơn lớp Internet có thể kết hợp với IP bằng cách bổ sung những tính năng cần thiết.

Cụ thể hơn, họ mong muốn các giao thức lớp vận chuyển có thể cung cấp:

- Một giao tiếp cho các ứng dụng mạng – nghĩa là, một con đường để các ứng dụng có thể truy cập vào mạng. Những nhà thiết kế mong muốn dữ liệu không chỉ được truyền đến máy đích mà phải truyền đến được những ứng dụng riêng biệt đang chạy trên máy đích.
- Một cơ chế đa hợp/ giải đa hợp. Trong trường hợp này, đa hợp có nghĩa là cho phép dữ liệu từ các ứng dụng và các máy tính khác nhau được truyền đến cùng ứng dụng tương ứng trên máy nhận. Hay nói cách khác, lớp vận chuyển phải có khả năng hỗ trợ đồng thời nhiều ứng dụng mạng và quản lý luồng dữ liệu đến lớp Internet. Ở đầu nhận, lớp vận chuyển phải có khả năng nhận dữ liệu từ lớp Internet và chuyển lên các ứng dụng. Khả năng này được gọi là giải đa hợp và nó cho phép nhiều ứng dụng mạng có thể được chạy đồng thời trên một máy tính, như duyệt web, mail và chia sẻ tập tin. Một khía cạnh khác của khả năng đa hợp/ giải đa hợp là một ứng dụng đơn lẻ có thể thực hiện được nhiều kết nối đồng thời với các máy tính khác nhau.
- Kiểm tra lỗi, điều khiển luồng và xác thực. Hệ thống giao thức cần phải có một lược đồ tổng quát để có thể đảm bảo dữ liệu được truyền đúng giữa các máy.

Yếu tố cuối cùng (kiểm tra lỗi, điều khiển luồng và xác thực) thu hút sự nghiên cứu nhiều nhất. Những yêu cầu về đảm bảo chất lượng luôn cân đối giữa các vấn đề về lợi ích và chi phí. Hệ thống đảm bảo chất lượng phức tạp cho phép tăng khả năng thành công trong việc phân phối qua mạng, nhưng kèm theo đó ta phải trả giá về lưu lượng tăng cao và thời gian xử lý chậm hơn. Đối với nhiều ứng dụng thì việc đảm bảo này không nhất thiết phải có. Do đó, lớp vận chuyển cung cấp hai cách để truy cập mạng, mỗi cách đều có sự giao tiếp và tính năng đa hợp/ giải đa hợp cần thiết cho các ứng dụng, nhưng lại đảm bảo chất lượng theo hai cách tiếp cận khác nhau, đó là:

- **Transport Control Protocol (TCP)** – có khả năng điều khiển luồng và kiểm soát lỗi bao quát để đảm bảo dữ liệu được phân phối thành công. TCP là giao thức hướng kết nối.

- **User Datagram Protocol (UDP)** – có khả năng kiểm tra lỗi đơn giản và được thiết kế để thay thế cho TCP khi tính năng điều khiển lỗi của TCP không cần thiết. UDP là giao thức không kết nối.

Chúng ta sẽ tìm hiểu kỹ hơn về các giao thức hướng kết nối và không kết nối cũng như về TCP và UDP trong phần sau của chương.

5.2 Các khái niệm lớp vận chuyển

Trước khi khảo sát chi tiết về TCP và UDP thì cần phải nắm qua một số khái niệm quan trọng sau:

- Giao thức hướng kết nối và không kết nối.
- Cổng và socket.
- Đa hợp hay còn gọi là ghép.

Những khái niệm này hết sức cần thiết để có thể hiểu được hoạt động của lớp vận chuyển. Bạn sẽ học về những khái niệm này trong phần sau.

5.2.1 Giao thức hướng kết nối và không kết nối

Để đáp ứng mức độ đảm bảo chất lượng thích hợp cho bất kỳ tình huống nào, những nhà phát triển đã đưa ra hai giao thức mạng:

- Giao thức hướng kết nối thiết lập và duy trì một kết nối giữa các máy tính có liên lạc với nhau cũng như theo dõi trạng thái của kết nối đó trong suốt quá trình truyền thông. Hay nói cách khác, mỗi gói dữ liệu truyền trong mạng đều phải được báo nhận, và máy gửi phải lưu lại thông tin trạng thái của gói để đảm bảo mỗi gói dữ liệu được nhận thành công hoặc truyền lại nếu cần thiết. Sau khi kết thúc việc truyền, nhận dữ liệu thì máy gửi và máy nhận sẽ đóng kết nối.
- Giao thức không kết nối gửi datagram một chiều đến máy đích và không quan tâm đến việc thông báo cho máy đích biết rằng dữ liệu đang ở trên đường truyền. Ngược lại, máy đích nhận dữ liệu và cũng không quan tâm đến việc phản hồi thông tin trạng thái cho máy gửi.

Hình 5-1 mô tả hai người đang đối thoại theo hướng có kết nối. Tất nhiên họ không thể thể hiện đầy đủ tính phức tạp của truyền thông số mà chỉ đơn giản mô tả khái niệm của giao thức hướng kết nối.

Hình 5-1 Một giao thức hướng kết nối



Hình 5-2 cho thấy nếu dùng giao thức không kết nối thì dữ liệu sẽ được truyền như thế nào.

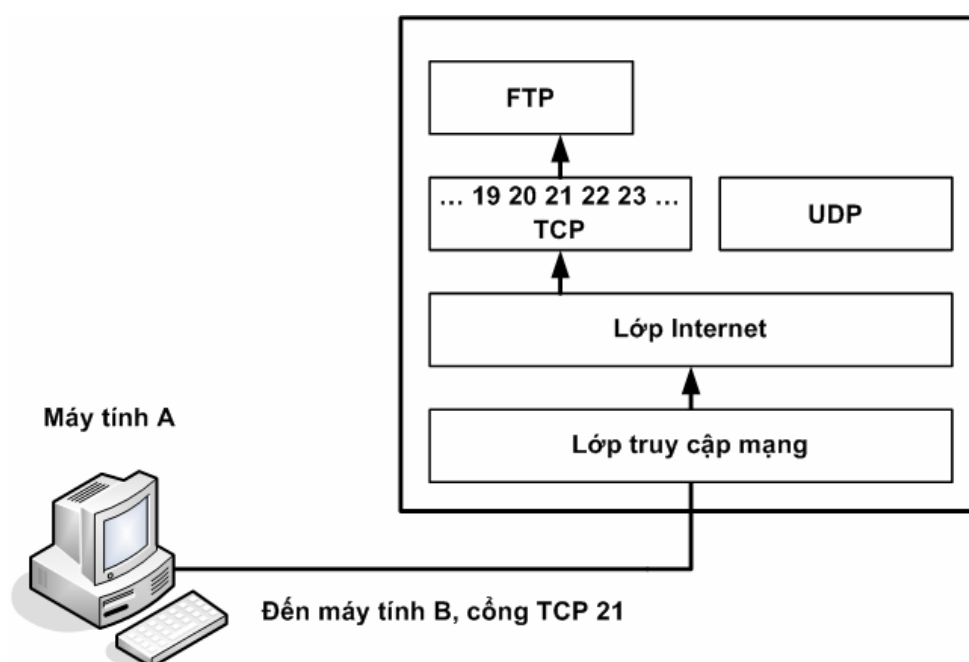
Hình 5-2 Một giao thức không kết nối



5.2.2 Cổng và socket

Lớp vận chuyển đóng vai trò như một giao tiếp giữa các ứng dụng mạng với mạng và đưa ra một phương pháp gửi dữ liệu đến từ mạng cho các ứng dụng cụ thể. Trong hệ thống TCP/IP, các ứng dụng có thể gửi dữ liệu qua giao thức TCP hay UDP bằng cách sử dụng số hiệu cổng. Một cổng là một địa chỉ nội được xác định trước hay đóng vai trò như là một con đường từ ứng dụng đến lớp vận chuyển và từ lớp vận chuyển ngược về ứng dụng (xem *hình 5-3*). Chẳng hạn như một máy khách liên lạc với một ứng dụng FTP trên máy chủ qua cổng 21 của giao thức TCP.

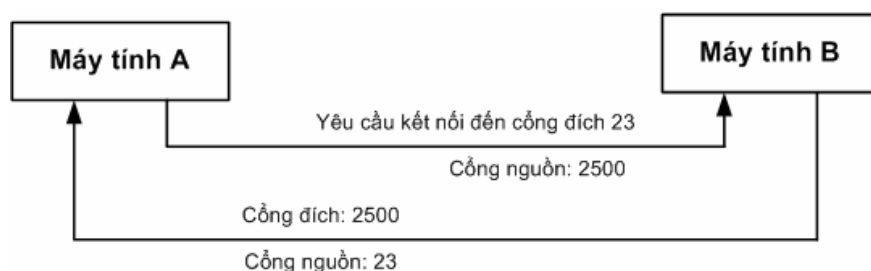
Hình 5-3 Một địa chỉ cổng đưa dữ liệu tới một ứng dụng cụ thể



Tiếp cận sát hơn lược đồ định vị ứng dụng cụ thể của lớp vận chuyển thì ta sẽ thấy dữ liệu TCP và UDP thực sự được gửi tới một socket. Một socket là một địa chỉ bao gồm IP và số hiệu cổng. Chẳng hạn như, socket 111.121.131.141.21 tham chiếu đến cổng 21 của máy tính có địa chỉ IP là 111.121.131.141.

Hình 5-4 trình bày cách máy tính sử dụng TCP trao đổi thông tin về socket khi chúng thiết lập một kết nối.

Hình 5-4 Trao đổi số hiệu socket nguồn và đích



Ví dụ sau sẽ trình bày rõ hơn về cách một máy tính truy cập vào một ứng dụng trên máy đích thông qua socket:

1. Máy tính A khởi tạo kết nối đến một ứng dụng trên máy tính B qua một cổng phổ biến. Một cổng phổ biến là một số hiệu cổng chỉ định đến một ứng dụng cụ thể được quy định bởi ICANN. **Bảng 5-1** và **bảng 5-2** liệt kê một vài cổng TCP và UDP phổ biến. Kết hợp với địa chỉ IP, cổng phổ biến trở thành địa chỉ socket đích cho máy A. Ngoài ra, phải có một trường dữ liệu nào đó trong yêu cầu thiết lập kết nối báo cho máy B biết phải sử dụng số hiệu socket nào khi gửi dữ liệu về A. Đó chính là địa chỉ socket nguồn của máy tính A.
2. Máy tính B nhận được yêu cầu từ máy tính A thông qua một cổng phổ biến và sẽ hồi đáp thông tin qua địa chỉ socket nguồn của máy A. Socket này trở thành địa chỉ đích của các bản tin được gửi từ ứng dụng trên máy tính B về ứng dụng trên máy tính A.

Bảng 5-1 Các cổng TCP phổ biến

Dịch vụ	Số hiệu cổng TCP	Mô tả ngắn gọn
tcpmux	1	Đa hợp dịch vụ cổng TCP
compressnet	2	Tiện ích quản lý
compressnet	3	Tiện ích nén
echo	7	Tiếng dội
discard	9	Hủy bỏ hoặc null
systat	11	Người dùng
daytime	13	Ngày giờ
netstat	15	Trạng thái mạng
gotd	17	Trích dẫn trong ngày

Dịch vụ	Số hiệu cổng TCP	Mô tả ngắn gọn
chargen	19	Phát sinh ký tự
ftp-data	20	Dữ liệu giao thức truyền tải tập tin
ftp	21	Điều khiển giao thức truyền tải tập tin
telnet	23	Kết nối mạng đầu cuối
smtp	25	Giao thức truyền mail đơn giản
nsw-fe	27	Hệ thống người dùng NSW
time	37	Máy chủ thời gian
name	42	Máy chủ tên host
domain	53	Máy chủ tên miền (DNS)
nameserver	53	Máy chủ tên miền (DNS)
DHCP	67	Giao thức cấu hình host động
gopher	70	Dịch vụ tìm kiếm Gopher
rje	77	Lối vào công việc từ xa
finger	79	Tìm người dùng trên mạng
http	80	Dịch vụ WWW
link	87	Liên kết TTY
Supdup	95	Giao thức SUPDUP
hostnames	101	Server tên host sri-nic
iso-tsap	102	ISO-TSAP
x400	103	Dịch vụ mail X.400
x400-snd	104	Gửi mail X.400
pop	109	Giao thức POP
pop2	109	Giao thức POP 2
pop3	110	Giao thức POP 3
portmap	111	
sunrpc	111	Dịch vụ SUN RPC
auth	113	Dịch vụ xác thực

Dịch vụ	Số hiệu cổng TCP	Mô tả ngắn gọn
sftp	115	Giao thức truyền tập tin bảo đảm
path	117	Dịch vụ UUCP path
uucp-path	117	Dịch vụ UUCP path
nntp	119	Giao thức truyền tải tin tức mạng người dùng
nbssession	139	Dịch vụ phiên NetBIOS
NeWS	144	Tin tức
tcprepo	158	Thư viện TCP

Bảng 5-2 Các cổng UDP phổ biến

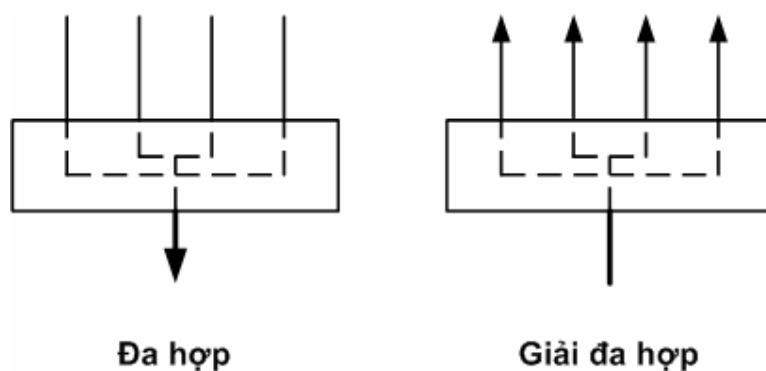
Dịch vụ	Số hiệu cổng UDP	Mô tả ngắn gọn
echo	7	Tiếng vọng
discard	9	Hủy bỏ hoặc null
systat	11	Người dùng
daytime	13	Ngày giờ
netstat	15	Trạng thái mạng
gotd	17	Trích dẫn trong ngày
chargen	19	Phát sinh ký tự
time	37	Máy chủ thời gian
name	42	Máy chủ tên host
domain	53	Máy chủ tên miền (DNS)
nameserver	53	Máy chủ tên miền (DNS)
bootps	67	Dịch vụ giao thức Bootstrap/DHCP
bootpc	68	Máy khách giao thức Bootstrap/DHCP
tftp	69	Giao thức truyền tập tin đơn giản
portmap	111	
sunrpc	111	Dịch vụ SUN RPC
ntp	123	Giao thức thời gian mạng
nbname	137	Tên NetBIOS

Dịch vụ	Số hiệu cổng UDP	Mô tả ngắn gọn
nbdatalogram	148	NetBIOS datagram
sgmp	153	
snmp	161	Giao thức quản lý mạng đơn giản
snmp-trap	162	Bẫy giao thức quản lý mạng đơn giản

5.2.3 Đa hợp/ Giải đa hợp

Hệ thống gán địa chỉ socket làm cho TCP và UDP có thể thực hiện một nhiệm vụ quan trọng khác của lớp vận chuyển: đa hợp và giải đa hợp. Như đã mô tả ở phần trước, đa hợp, hay ghép, là kỹ thuật tổ hợp nhiều nguồn đầu vào thành một đầu ra duy nhất, và giải đa hợp, hay tách, là việc nhận dữ liệu từ một nguồn duy nhất rồi phân phối cho nhiều đầu ra.

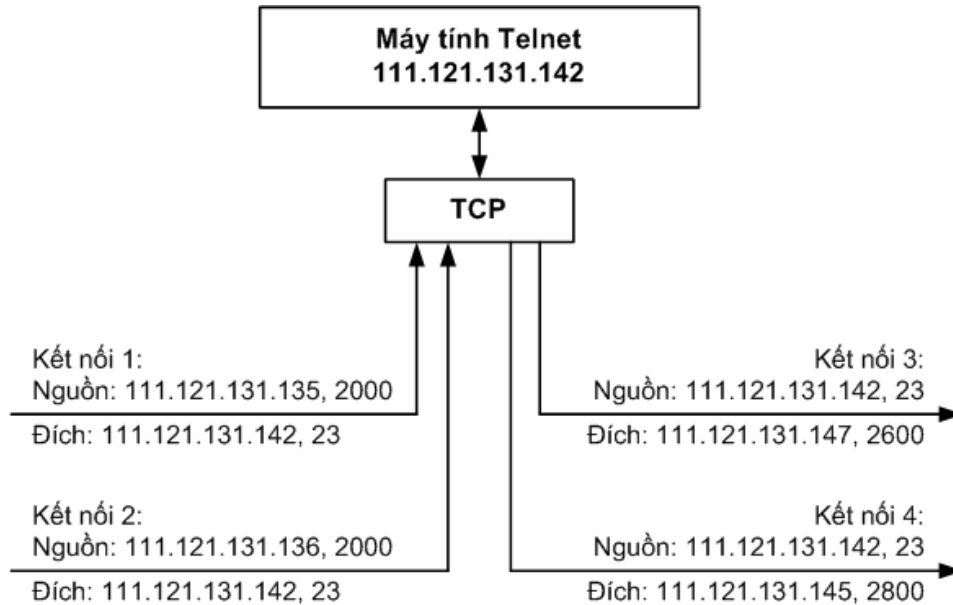
Hình 5-5 Đa hợp và giải đa hợp



Kỹ thuật đa hợp/ giải đa hợp làm cho các lớp thấp hơn của mô hình TCP/IP xử lý dữ liệu mà không quan tâm đến ứng dụng nào đã khởi tạo dữ liệu đó. Tất cả các liên kết với ứng dụng đều được giải quyết ở lớp vận chuyển, theo đó, dữ liệu đi và đến từ lớp Internet chỉ là một luồng đơn, độc lập với ứng dụng.

Chìa khoá của kỹ thuật đa hợp/giải đa hợp là địa chỉ socket. Vì địa chỉ socket bao gồm IP và số hiệu cổng nên nó cung cấp khả năng nhận dạng một ứng dụng cụ thể đang chạy trên một máy tính cụ thể. **Hình 5.6** mô tả hoạt động của một máy chủ Telnet. Tất cả máy khách đều sử dụng cổng phổ biến TCP 23 để liên lạc với máy chủ và socket đích của mỗi máy khách là duy nhất. Tương tự như vậy, tất cả các ứng dụng chạy trên máy chủ Telnet cũng đều sử dụng địa chỉ IP của máy chủ, nhưng chỉ có dịch vụ Telnet là sử dụng địa chỉ socket, gồm địa chỉ IP của máy chủ và cổng TCP 23.

Hình 5-6 Địa chỉ socket nhận dạng duy nhất một ứng dụng trên một máy chủ cụ thể



5.3 TCP và UDP

Như đã đề cập ở phần trước của chương, TCP là một giao thức hướng kết nối, cung cấp khả năng điều khiển lỗi và điều khiển luồng bao quát. UDP là giao thức không kết nối với chức năng điều khiển lỗi đơn giản hơn nhiều. Có thể nói rằng, TCP đảm bảo độ tin cậy và UDP đảm bảo về tốc độ. Những ứng dụng có hỗ trợ các phiên làm việc tương tác như Telnet hay FTP thì có khuynh hướng sử dụng TCP, trong khi những ứng dụng có thể tự kiểm tra lỗi hoặc không quan trọng vấn đề kiểm tra lỗi thì có khuynh hướng sử dụng UDP.

Một nhà phát triển phần mềm xây dựng một ứng dụng mạng có thể lựa chọn TCP hay UDP làm giao thức vận chuyển. Cần phải lưu ý là các kỹ thuật điều khiển đơn giản của UDP là hạn chế. Vì trước hết, ít đảm bảo về chất lượng không có nghĩa là chất lượng kém. Những phần điều khiển và kiểm tra bổ sung của TCP nhìn chung là không cần thiết đối với nhiều ứng dụng. Trong trường hợp việc điều khiển lỗi và điều khiển luồng là cần thiết thì các nhà phát triển thường ưu tiên tích hợp những chức năng điều khiển này vào trong chính ứng dụng để dễ dàng tùy biến theo những yêu cầu cụ thể và do đó họ thường sử dụng UDP cho việc truy cập mạng. Những dịch vụ được xây dựng trên nền UDP như dịch vụ lời gọi thủ tục từ xa (RPC) có thể hỗ trợ nhiều ứng dụng tiên tiến và phức tạp, nhưng những ứng dụng đó phải đảm trách điều khiển lỗi và điều khiển luồng hiệu quả hơn khi sử dụng TCP.

5.3.1 TCP: Giao thức truyền tải hướng kết nối

Chương này đã mô tả cách tiếp cận hướng kết nối của TCP trong truyền thông. TCP còn có một số tính năng quan trọng khác cần chú ý:

- Xử lý định hướng luồng – TCP xử lý dữ liệu trong một luồng. Hay nói cách khác, ở một thời điểm, TCP có thể chấp nhận dữ liệu một byte hơn là một khối dữ liệu được định dạng trước. TCP chia dữ liệu thành nhiều đoạn có chiều dài khác nhau trước khi chuyển qua lớp Internet.
- Sắp xếp lại thứ tự - Nếu dữ liệu đến không theo thứ tự, TCP phải có khả năng sắp xếp lại dữ liệu theo đúng thứ tự ban đầu.
- Điều khiển luồng - Chức năng điều khiển luồng của TCP đảm bảo việc truyền dữ liệu không bị sai hoặc bị tràn quá dung lượng máy nhận. Việc này đặc biệt được chú trọng trong điều kiện môi trường thay đổi với nhiều sự khác biệt về tốc độ xử lý của CPU và kích thước bộ đệm.
- Thứ tự ưu tiên và sự bảo mật - Mức độ ưu tiên và bảo mật có thể được thiết lập cho các kết nối TCP. Tuy nhiên, nhiều trình thực thi TCP không cung cấp những tính năng này.
- Đóng kết nối an toàn - việc đóng kết nối của TCP cũng được thực hiện cẩn thận như lúc khởi tạo kết nối. Chức năng này đảm bảo tất cả các đoạn dữ liệu được gửi và nhận trước khi kết nối bị đóng.

TCP còn đưa ra một hệ thống phức tạp các thông báo và báo nhận để hỗ trợ cấu trúc hướng kết nối. Phần sau đây sẽ khảo sát kỹ hơn về định dạng dữ liệu TCP, sự truyền dữ liệu TCP và các kết nối TCP. Bản chất kỹ thuật của phần này là xem xét tính phức tạp thực sự của TCP. Việc thảo luận về TCP còn nhấn mạnh thêm rằng một giao thức không chỉ dừng lại ở việc định dạng dữ liệu mà đó là một hệ thống các tiến trình tương tác và các thủ tục được xây dựng để thực hiện những mục đích xác định.

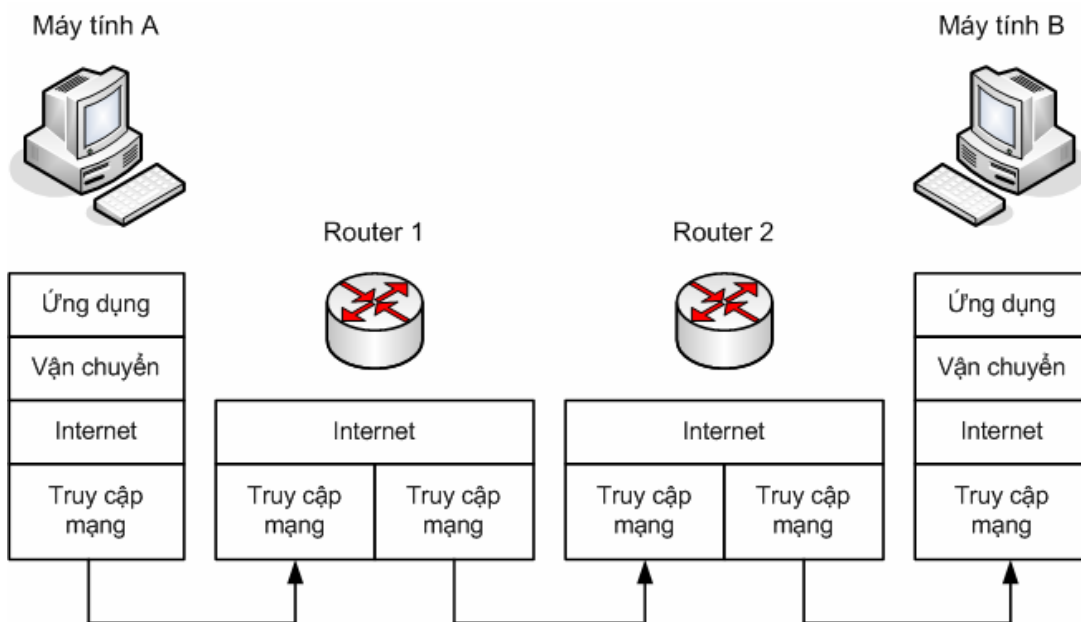
Như đã khảo sát ở **chương 1**, những hệ thống giao thức phân lớp như TCP/IP thực hiện việc trao đổi thông tin ngang cấp, giữa một lớp trên máy gửi với lớp tương ứng trên máy nhận. Hay cụ thể hơn, lớp truy cập mạng của máy gửi liên lạc với lớp truy cập của máy nhận, lớp Internet của máy gửi liên lạc với lớp Internet của máy nhận, và tương tự đối với các lớp khác.

Phần mềm TCP liên lạc với phần mềm TCP trên máy mà nó muốn thiết lập kết nối. Trong bất kỳ cuộc thảo luận nào về TCP, khi nói “Máy tính A thiết lập kết nối với máy tính B” thì có nghĩa là phần mềm TCP trên máy A thiết lập kết nối với phần mềm

TCP trên máy B, cả hai đều đang hoạt động nhân danh ứng dụng cục bộ. Sự phân biệt tinh tế này mang lại những thảo luận hấp dẫn xung quanh khái niệm xác thực điểm cuối.

Cần nhắc lại rằng các điểm cuối chịu trách nhiệm xác thực những sự liên lạc trong mạng TCP (điểm cuối là những nút mạng cố gắng thực hiện sự liên lạc – trái với những điểm trung gian là nút chuyển tiếp bản tin). Trong tình huống liên mạng, thông thường, dữ liệu được chuyển từ subnet nguồn đến subnet đích qua các router. Đa số những router này hoạt động ở lớp Internet – bên dưới lớp vận chuyển. (Chúng ta sẽ tìm hiểu kỹ hơn về router ở **chương 7, "Định tuyến"**). Điểm quan trọng là các router không liên quan gì với thông tin ở lớp vận chuyển. Nó chỉ đơn giản chuyển tiếp dữ liệu lớp TCP đóng trong các datagram IP đã gắn thông tin tiêu đề và gửi các datagram theo đúng đường đi của nó. Thông tin điều khiển và xác thực đã được mã hóa trong các đoạn dữ liệu TCP (segment) chỉ được sử dụng bởi phần mềm TCP của máy đích. Việc này làm tăng tốc độ định tuyến trong mạng TCP/IP (vì các router không tham gia vào trình tự đảm bảo chất lượng rất tỉ mỉ của TCP) và làm cho TCP có thể thực hiện đầy đủ vai trò của nó bằng cách cung cấp việc giám sát kết nối trong hoạt động mạng.

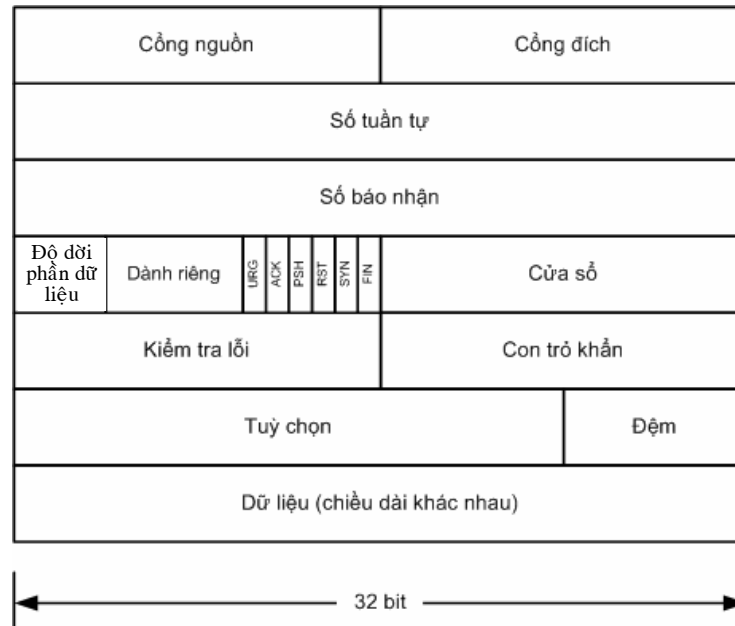
Hình 5-7 Các router chuyển tiếp chứ không xử lý dữ liệu lớp vận chuyển



5.3.1.1 Định dạng dữ liệu TCP

Định dạng tiêu đề TCP được cho ở **hình 5-8**. Sự phức tạp của cấu trúc này đã cho thấy sự phức tạp của TCP và các tính năng của nó.

Hình 5-8 Định dạng dữ liệu đoạn TCP (segment)



Trong đó, ý nghĩa các trường dữ liệu được mô tả cụ thể như sau:

- **Cổng nguồn (Source Port – 16 bit)** - Số hiệu cổng được chỉ định cho ứng dụng trên máy nguồn.
- **Cổng đích (Destination Port – 16 bit)** - Số hiệu cổng được chỉ định cho ứng dụng trên máy đích.
- **Số tuần tự (Sequence Number – 32 bit)** - Số thứ tự của byte đầu tiên trong đoạn dữ liệu cụ thể khi cờ SYN có giá trị khác 1. Nếu giá trị cờ SYN là 1 thì trường số tuần tự chứa số thứ tự ban đầu (ISN), được sử dụng để đồng bộ các số thứ tự và khi đó thì số thứ tự của octet đầu tiên sẽ lớn hơn giá trị trong trường số tuần tự 1 đơn vị, tức là ISN+1.
- **Số báo nhận (Acknowledgment Number – 32 bit)** - Số hiệu báo nhận của đoạn. Trường này có giá trị là số thứ tự kế tiếp mà máy nhận mong muốn nhận được, hay nói cách khác, là số thứ tự của byte cuối cùng nhận được cộng với 1.
- **Độ dời phần dữ liệu (Data offset – 4 bit)** - Trường này báo cho phần mềm TCP trên máy nhận biết được phần tiêu đề có kích thước bao nhiêu, cũng có nghĩa là dữ liệu được bắt đầu từ vị trí nào. Độ dời dữ liệu được biểu diễn bằng một số nguyên các từ 32bit.
- **Dành riêng (Reserved – 6 bit)** - Trường này sẽ được dự phòng cho sự phát triển của TCP trong tương lai và có giá trị là 0.
- **Các cờ điều khiển (Control flags - mỗi cờ 1 bit)** – Các cờ này cung cấp những thông tin quan trọng về đoạn dữ liệu, gồm:
 - ♦ URG - Nếu có giá trị 1, thì đoạn dữ liệu cần được xử lý ngay và trường con trỏ khẩn được xét đến.
 - ♦ ACK - Nếu có giá trị 1, thì trường số báo nhận được xem xét.

- ◆ PSH - Nếu có giá trị 1, phần mềm TCP sẽ đẩy toàn bộ dữ liệu được gửi theo một luồng đến ứng dụng nhận.
- ◆ RST - Nếu có giá trị 1, kết nối sẽ được thiết lập lại.
- ◆ SYN - Nếu có giá trị 1, thì các số tuần tự sẽ được đồng bộ, đánh dấu sự bắt đầu một kết nối.
- ◆ FIN - Nếu giá trị bằng 1, thì có nghĩa là máy tính gửi đã truyền hết dữ liệu. Cờ này được sử dụng để đóng một kết nối.
- **Cửa sổ (Window – 16 bit)** - Một tham số được sử dụng trong điều khiển luồng. Cửa sổ xác định dãy các số tuần tự phát sau số tuần tự báo nhận sau cùng mà máy gửi có thể truyền đi mà không chờ báo nhận.
- **Kiểm tra lỗi (Checksum – 16 bit)** - Trường này được sử dụng để kiểm tra tính đúng đắn của đoạn dữ liệu. Máy nhận thực hiện tính toán kiểm tra lỗi trên toàn bộ đoạn dữ liệu nhận được rồi so sánh với giá trị được lưu trong trường này. Việc tính toán kiểm tra lỗi cũng bao gồm phần tiêu đề giả (pseudo-header) với thông tin gán địa chỉ IP. Xem thêm phần tiêu đề giả UDP ở phần sau của chương.
- **Con trỏ khẩn (Urgent Pointer – 16 bit)** - Con trỏ độ dời chỉ đến số tuần tự đánh dấu sự bắt đầu của thông tin khẩn trong vùng dữ liệu.
- **Tùy chọn (Options)** - Xác định một trong các tập thiết lập tùy chọn.
- **Đệm (Padding)** - Các bit 0 được thêm vào (nếu cần thiết) để đảm bảo dữ liệu được bắt đầu đúng ở giới hạn 32 bit.
- **Dữ liệu (Data)** - Phần dữ liệu được truyền trong đoạn.

TCP yêu cầu tất cả các trường dữ liệu phải được quản lý chặt chẽ, báo nhận và xác thực khi được truyền trên mạng. Phần sau sẽ cho thấy làm thế nào phần mềm TCP sử dụng những trường này để quản lý các nhiệm vụ gửi và nhận dữ liệu.

5.3.1.2 Các kết nối TCP

Mọi thứ trong TCP đều xảy ra ở ngưỡng kết nối. TCP gửi và nhận dữ liệu thông qua một kết nối, bao gồm việc yêu cầu, mở và đóng kết nối theo tập luật của TCP.

Như đã đề cập ở phần trước của chương, một trong những mục đích của TCP là đưa ra một giao tiếp để ứng dụng có thể truy cập được mạng. Giao tiếp đó được cung cấp thông qua các cổng TCP, và để thực hiện một kết nối qua các cổng này thì giao tiếp TCP đến ứng dụng phải được mở. TCP hỗ trợ hai trạng thái mở sau:

- **Mở bị động (Passive open)** - Một tiến trình ứng dụng báo cho TCP biết nó đang chuẩn bị nhận các kết nối đến thông qua một cổng TCP. Do đó, cầu nối giữa TCP với ứng dụng được mở để chờ một yêu cầu kết nối đến.
- **Mở chủ động (Active open)** - Trạng thái này xảy ra khi một ứng dụng yêu cầu TCP khởi tạo một kết nối với một máy tính khác. Thực tế, TCP cũng có thể khởi tạo một kết nối tới một máy tính khác đang ở trạng thái mở chủ động, đó là trường hợp cả hai máy tính đều đang cố gắng mở một kết nối.

Thông thường, một ứng dụng mong muốn nhận các kết nối, chẳng hạn như FTP server, thì đặt cổng TCP của nó ở trạng thái mở bị động. Trên máy khách, trạng thái TCP của FTP client hầu như được đóng cho đến khi người dùng khởi tạo một kết nối đến FTP server, khi đó trạng thái của máy khách là mở chủ động. Sau đó, phần mềm TCP của máy tính có trạng thái mở chủ động (client) sau đó khởi tạo việc trao đổi các bản tin để thiết lập một kết nối. Sự trao đổi thông tin đó, thường được gọi là sự bắt tay 3 chiều (three-way handshake), sẽ được thảo luận kỹ hơn ở phần sau của chương.

Client là máy tính gửi yêu cầu hay nhận các dịch vụ từ máy tính khác trên mạng.

Server là máy tính cung cấp các dịch vụ cho những máy tính khác trên mạng.

TCP gửi những đoạn dữ liệu có chiều dài khác nhau, bên trong một đoạn, mỗi byte dữ liệu được chỉ định một số tuần tự. Máy nhận phải gửi một bản tin báo nhận cho mỗi gói nhận được với số thứ tự báo nhận là số thứ tự của byte cuối cùng trong gói nhận cộng thêm 1. Do đó, có thể nói truyền thông TCP là một hệ thống truyền và báo nhận. các trường số tuần tự và số báo nhận của phần tiêu đề TCP (*được trình bày ở phần trước*) giúp cho phần mềm TCP cập nhật đều đặn trạng thái của kết nối.

Số thứ tự của mỗi byte riêng biệt không được xét. Thay vào đó, trường số tuần tự ở phần tiêu đề chỉ lưu số thứ tự của byte đầu tiên của dữ liệu trong đoạn.

Có một ngoại lệ trong tập luật này. Nếu sự phân đoạn dữ liệu xảy ra lúc bắt đầu kết nối (xem phần bắt tay 3 chiều - *three-way handshake* ở phần sau của chương này), thì trường số tuần tự sẽ chứa giá trị ISN, có giá trị nhỏ hơn 1 đơn vị so với số tuần tự của byte đầu tiên trong đoạn (byte đầu tiên được gán số tuần tự là ISN+1).

Nếu đoạn được nhận thành công, máy nhận sử dụng trường số báo nhận để thông báo cho máy gửi biết được byte nào đã được nhận thành công. Trường số báo nhận trong bản tin báo nhận được gán giá trị là số tuần tự của byte cuối cùng trong gói được nhận cộng với 1. Hay nói cách khác, trường số báo nhận cho biết số tuần tự kế tiếp mà máy tính chuẩn bị nhận.

Nếu một bản tin báo nhận không được nhận trong khoảng thời gian cho phép thì máy gửi sẽ truyền lại dữ liệu, bắt đầu với byte liền sau byte đã được báo nhận cuối cùng.

5.3.1.3 Thiết lập một kết nối

Để hệ thống tuần tự/ báo nhận hoạt động đúng đắn, các máy tính phải đồng bộ các số tuần tự của nó. Hay nói cách khác, máy tính B phải biết được số tuần tự ban đầu (ISN) mà máy tính A đã sử dụng. Và máy tính A cũng phải được biết số ISN mà máy B sẽ sử dụng để truyền dữ liệu.

Sự đồng bộ các số tuần tự này được gọi là sự bắt tay ba chiều (three-way handshake). Sự bắt tay này xảy ra khi bắt đầu một kết nối TCP. Ba bước của sự bắt tay gồm:

1. Máy tính A gửi một đoạn dữ liệu với:

$SYN = 1$

$ACK = 0$

Số tuần tự = X (X là giá trị ISN của máy tính A)

Máy tính mở chủ động (máy A) gửi một đoạn dữ liệu với cờ SYN có giá trị 1 và cờ ACK có giá trị 0. SYN là viết tắt của từ đồng bộ (synchronize). Cờ này thông báo đang cố gắng mở một kết nối. Phần tiêu đề của đoạn đầu tiên này còn chứa số tuần tự ban đầu (ISN), được sử dụng để đánh dấu sự bắt đầu các số tuần tự của dữ liệu mà máy A sẽ truyền. Byte đầu tiên được truyền đến máy tính B sẽ có số tuần tự là ISN+1.

2. Máy tính B nhận đoạn dữ liệu của máy tính A và hồi đáp một đoạn dữ liệu có các giá trị:

$SYN = 1$ (vẫn còn trong pha đồng bộ)

$ACK = 1$ (trường số báo nhận sẽ chứa 1 giá trị)

Số tuần tự = Y, với Y là giá trị ISN của máy B.

Số báo nhận = M+1, trong đó M là giá trị số tuần tự của byte sau trong đoạn nhận được từ máy tính A.

3. Máy tính A gửi lại một đoạn dữ liệu cho máy B thông báo chấp nhận giá trị ISN của B với:

$SYN = 0$

$ACK = 1$

Số tuần tự = số tuần tự kế tiếp trong chuỗi (M+1)

Số báo nhận = N+1, với N là số tuần tự của byte sau cùng trong đoạn nhận được từ máy B.

Sau 3 bước bắt tay, kết nối sẽ được mở và các thành phần TCP sẽ thực hiện việc gửi, nhận dữ liệu có sử dụng lược đồ tuần tự/ báo nhận như đã mô tả ở phần trước của chương.

5.3.1.4 Điều khiển luồng TCP

Trường cửa sổ (window) trong phần tiêu đề TCP cung cấp kỹ thuật điều khiển luồng cho kết nối. Mục đích của trường cửa sổ là làm cho máy gửi không gửi dữ liệu quá nhiều và quá nhanh, để làm mất dữ liệu vì tốc độ xử lý dữ liệu đến của máy nhận có thể không nhanh bằng tốc độ truyền của máy gửi. Phương pháp điều khiển luồng được sử dụng bởi TCP được gọi là phương pháp cửa sổ trượt. Máy nhận sử dụng trường cửa sổ (cũng được gọi là trường kích thước bộ đệm) để xác định tập các số tuần tự sau số tuần tự được báo nhận sau cùng mà máy gửi được phép truyền. Máy gửi không thể truyền vượt quá kích thước này cho đến khi nó nhận được báo nhận kết tiếp.

5.3.1.5 Đóng một kết nối

Khi đến thời điểm đóng kết nối, máy tính đóng, giả sử là A, sẽ đặt một đoạn dữ liệu (segment) có giá trị cờ FIN là 1 vào hàng đợi. Sau đó, ứng dụng sẽ chuyển sang trạng thái chờ kết thúc (fin-wait). Trong trạng thái này, phần mềm TCP của máy A vẫn tiếp tục nhận và xử lý các đoạn dữ liệu trong hàng đợi nhưng không gửi thêm bất kỳ dữ liệu nào. Khi máy tính B nhận được đoạn dữ liệu FIN, nó sẽ hồi đáp báo nhận cho FIN, gửi các đoạn dữ liệu còn lại, và báo cho ứng dụng cục bộ là FIN đã được nhận. Máy B gửi một đoạn dữ liệu FIN cho máy A, máy A báo nhận, và kết nối được đóng.

5.3.2 UDP: Giao thức truyền tải không kết nối

UDP đơn giản hơn nhiều so với TCP, nó không thực hiện bất kỳ phương thức nào đã được liệt kê trong phần trước. Tuy nhiên, có một vài chú ý về UDP mà chúng ta nên quan tâm tới.

Đầu tiên, mặc dù đôi lúc UDP được mô tả là không có khả năng kiểm tra lỗi, nhưng thực tế, nó vẫn có khả năng thực hiện việc kiểm tra lỗi đơn giản. Nói đúng hơn, khả năng kiểm tra lỗi của UDP có giới hạn. Bản thân datagram UDP cũng có giá trị checksum mà máy nhận có thể sử dụng để kiểm tra tính đúng đắn của dữ liệu (thông thường việc kiểm tra checksum là một tùy chọn và có thể được vô hiệu trên máy nhận để tăng tốc độ xử lý dữ liệu đến). Datagram UDP cũng có một tiêu đề giả (pseudo-header) chứa địa chỉ đích của datagram, và đó là phương tiện để kiểm tra những datagram bị truyền sai địa chỉ. Nếu máy UDP nhận một datagram được truyền đến một cổng không hoạt động hoặc không được xác định thì nó sẽ gửi một bản tin ICMP báo cho máy nguồn biết rằng không đến được cổng.

Thứ hai, UDP không sắp xếp lại dữ liệu như TCP. Việc sắp xếp lại thứ tự dữ liệu là rất quan trọng trong những mạng lớn, như Internet do các đoạn dữ liệu đi theo những đường khác nhau và có độ trì hoãn khác nhau trên các bộ đệm của router. Trong

các mạng cục bộ, việc thiếu tính năng này của UDP vẫn có thể đảm bảo được độ tin cậy dữ liệu.

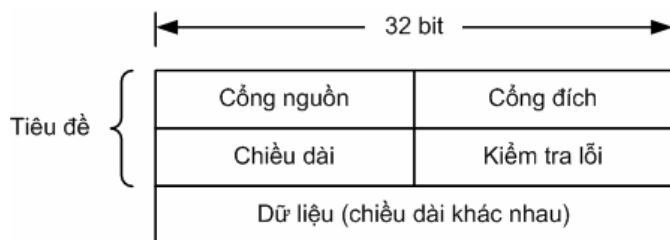
Thông tin thêm

Với thiết kế không kết nối, UDP trở thành giao thức được lựa chọn khi quảng bá dữ liệu trong mạng. Quảng bá là trạng thái mà một bản tin được tất cả các máy tính trong cùng một subnet nhận và xử lý. Cần phải biết rằng, nếu máy tính nguồn đồng thời mở một kết nối TCP cho mỗi các máy tính trong cùng subnet để gửi một bản tin broadcast đơn giản, thì hiệu suất mạng có thể sẽ bị giảm đáng kể.

Mục đích chính của giao thức UDP là chuyển các datagram lên lớp ứng dụng. Bản thân UDP rất đơn giản nên cấu trúc tiêu đề của nó cũng không phức tạp. RFC 768 mô tả giao thức này chỉ trong 3 trang. Như đã đề cập ở phần đầu, UDP không thực hiện việc truyền lại những datagram bị loại bỏ hoặc bị hỏng, không sắp xếp các datagram nhận được theo trật tự, không loại bỏ các datagram trùng, không báo nhận cho các datagram đã nhận, và cũng không thực hiện quá trình thiết lập hoặc ngắt kết nối. UDP là kỹ thuật được các chương trình ứng dụng sử dụng để gửi và nhận datagram mà không cần một kết nối TCP nào. Các ứng dụng có thể cung cấp bất kỳ hay tất cả những chức năng này nếu nó cần thiết cho mục đích của ứng dụng.

Phần tiêu đề của UDP gồm 4 trường 16 bit. **Hình 5.9** trình bày tiêu đề cấu trúc của một datagram UDP.

Hình 5-9 Tiêu đề và trường dữ liệu của datagram UDP



Datagram UDP gồm các trường sau:

- **Cổng nguồn (Source Port)** - trường này chiếm 16 bit đầu tiên của phần tiêu đề UDP. Nó chứa số hiệu cổng UDP của ứng dụng gửi datagram. Giá trị chứa trong trường cổng nguồn được ứng dụng nhận sử dụng làm địa chỉ trả về khi nó gửi một hồi đáp. Trường này là một tùy chọn và ứng dụng gửi cũng không nhất thiết phải gửi kèm số hiệu cổng của nó. Nếu ứng dụng gửi không sử dụng giá trị cổng này, thì nó sẽ thay thế bằng 16 bit 0. Rõ ràng, nếu không có địa chỉ cổng nguồn, thì ứng dụng nhận sẽ không thể nào hồi đáp được. Tuy nhiên, trong trường hợp gửi một bản tin snmr-trap thì chức năng này được sử dụng vì đó là bản tin một hướng và nó không cần hồi đáp.
- **Cổng đích (Destination Port)** - 16 bit - chứa địa chỉ cổng mà phần mềm UDP của máy nhận sử dụng để phân phối datagram này.

- **Chiều dài (Length)** - trường 16 bit này chứa thông tin chiều dài tính theo đơn vị octet của datagram UDP. Chiều dài này gồm cả phần tiêu đề UDP và phần dữ liệu. Vì phần tiêu đề UDP gồm có 8 octet nên giá trị tối thiểu của trường này là 8.
- **Kiểm tra lỗi (checksum)** - trường 16 bit này được sử dụng để xác định datagram nào bị sai lệch trong quá trình truyền. Giá trị kiểm tra lỗi là kết quả của một phép tính đặc biệt được thực hiện trên chuỗi dữ liệu nhị phân. Đối với UDP, giá trị này được tính toán dựa trên một tiêu đề giả, tiêu đề UDP, phần dữ liệu UDP và có thể cả những octet 0 được thêm vào để chiều dài của dữ liệu đưa vào tính tổng lỗi là một số chẵn các octet. Giá trị kiểm tra lỗi được tạo ra ở nguồn và được kiểm tra lại ở đích cho phép ứng dụng máy khách có thể xác định được datagram có bị sai hay không.

Bởi vì phần tiêu đề thực của UDP không có địa chỉ IP nguồn và đích nên rất có thể datagram bị phân phối sai máy tính hoặc sai dịch vụ. Phần dữ liệu được sử dụng để tính toán kiểm tra lỗi là một chuỗi các giá trị được trích ra từ tiêu đề IP hay còn gọi là tiêu đề giả. Tiêu đề giả cung cấp thông tin địa chỉ IP đích để máy tính nhận có thể xác định được datagram nào đã bị truyền sai địa chỉ.

5.4 Một lưu ý về tường lửa (firewall)

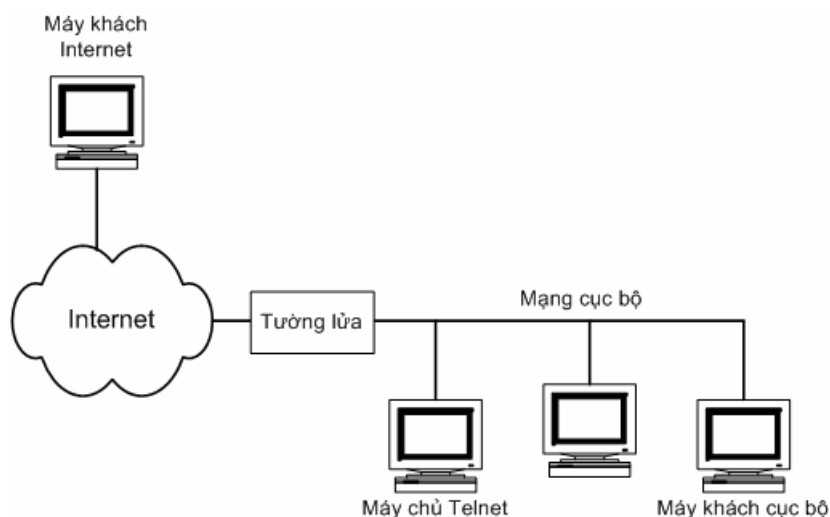
Tường lửa là một hệ thống bảo vệ mạng cục bộ khỏi bị tấn công bởi những người dùng không được phép đang cố gắng truy cập vào mạng cục bộ từ mạng toàn cầu (Internet). Tường lửa là một thuật ngữ Internet, đó là một máy tính được trang bị rất nhiều chức năng và cũng có nhiều định nghĩa về nó. Chương này sẽ trình bày một số chức năng chính của tường lửa.

Một chức năng quan trọng của tường lửa là ngăn chặn việc truy cập đến những cổng TCP và UDP đặc biệt. Thực tế, đôi khi tường lửa (firewall) lại là một động từ, có nghĩa là chặn đứng truy cập đến một cổng.

Ví dụ, để khởi tạo một phiên Telnet với máy chủ (server), máy khách (client) phải gửi một yêu cầu đến địa chỉ cổng phổ biến (well-known) của Telnet, đó là cổng TCP 23. (Telnet là một tiện ích cho phép máy khách có vai trò như một đầu cuối của máy chủ. Chúng ta sẽ nghiên cứu kỹ hơn về telnet ở **chương 10, “Truyền tập tin và các tiện ích truy cập”**). Việc sử dụng telnet trái phép có thể dẫn đến sự không an toàn trong bảo mật. Để tăng tính bảo mật, máy chủ có thể được cấu hình để ngưng việc sử dụng cổng 23 cho dịch vụ Telnet; để làm được việc đó, máy chủ có thể đơn giản là không tiếp tục chạy ứng dụng Telnet; nhưng giải pháp này cũng ngăn cản cả những người dùng trong mạng cục bộ sử dụng dịch vụ Telnet. Một giải pháp khác là cài đặt một tường lửa (**hình 5-10**) và cấu hình để chặn những truy cập vào cổng 23. Kết quả là những người dùng trong mạng cục bộ, bên trong tường lửa, vẫn truy cập tự do đến cổng TCP 23 trên máy chủ. Những người dùng từ Internet, bên ngoài mạng cục bộ, không truy cập được cổng TCP 23 của máy chủ, do đó, không thể xâm nhập vào máy

chủ qua dịch vụ Telnet. Trong thực tế, người dùng từ Internet không thể sử dụng Telnet để truy cập đến bất kỳ máy tính nào bên trong mạng cục bộ.

Hình 5-10 Minh họa một tường lửa điển hình



Hình 5-10 minh họa việc sử dụng Telnet và cổng TCP 23. Tường lửa có thể ngăn chặn bất kỳ hay toàn bộ những truy cập đến các cổng làm nguy hại đến khả năng bảo mật. Những người quản trị mạng thường ngăn chặn các truy cập đến tất cả các cổng ngoại trừ những cổng thực sự cần thiết, như cổng xử lý các email đến. Có nhiều thiết bị thể hiện sự có mặt của công ty trên Internet, như máy chủ web (web server), được đặt bên ngoài tường lửa sao cho truy cập đến thiết bị Internet này sẽ không trở thành những truy cập trái phép đến mạng cục bộ.

Thông tin thêm

Tường lửa có thể ngăn chặn những người dùng bên ngoài truy cập vào các dịch vụ bên trong mạng cũng như ngăn những người dùng bên trong truy cập các dịch vụ bên ngoài mạng.

Tóm tắt

Chương này đã trình bày một số chức năng cơ bản của lớp vận chuyển của chồng giao thức TCP/IP. Chúng ta đã khảo sát các giao thức hướng kết nối và không kết nối, đa hợp và giải đa hợp, cổng và socket. Chương này cũng giới thiệu về các giao thức lớp vận chuyển, TCP và UDP, cũng như đã mô tả một số chức năng quan trọng của TCP và UDP. Chúng ta cũng đã biết được TCP thực hiện sự chứng thực đầu cuối như thế nào, đã tìm hiểu về định dạng dữ liệu, điều khiển luồng, khắc phục lỗi của TCP và cả thủ tục bắt tay ba chiều (*three-way handshake*) để mở một kết nối. Chương này cũng đã trình bày về định dạng của phần tiêu UDP.

CHƯƠNG

6 PHẦN CỨNG MẠNG

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Cầu (Bridge)**
- **Bộ tập trung dây (Hub) và bộ chuyển mạch (Switch)**
- **Bộ định tuyến (Router)**
- **Kỹ thuật chuyển đổi địa chỉ mạng (Network Address Translation)**

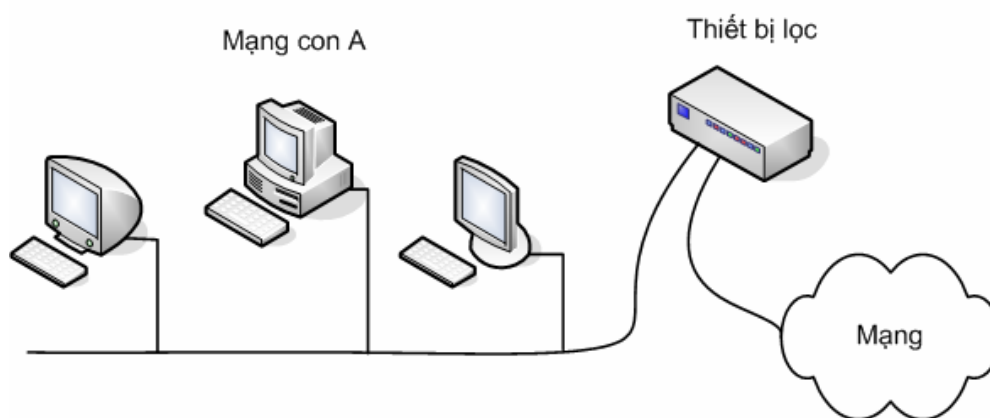
Ngoài máy tính và dây nối, hầu như tất cả các mạng dù là nhỏ nhất đều có những thiết bị bổ sung để thực hiện việc kết nối, giảm lưu lượng và tăng hiệu suất mạng. Một vài thiết bị, chẳng hạn như bộ định tuyến (router) và bộ chuyển mạch (switch), được sử dụng để chia nhỏ mạng. Một số thiết bị khác, như hub, lại tăng tính thuận tiện kết nối trong các mạng ethernet. Switch là thiết bị cũng tương tự hub nhưng có thêm một số tính năng của bridge. Chương này khảo sát về những thiết bị mạng quan trọng và cũng như các chức năng của nó trong mạng TCP/IP.

Kết thúc chương này bạn sẽ có thể :

- Giải thích tại sao những nhà quản trị mạng lại chia nhỏ mạng
- Mô tả bridge
- Mô tả router
- Mô tả hub
- Mô tả switch
- Giải thích sự khác nhau giữa định tuyến tĩnh và động.

6.1 Mạng được chia nhỏ

Như đã đề cập ở chương trước, các phương thức truy cập mạng như CSMA/CD (đối với ethernet) và token passing (token ring) được thiết kế cho những mạng có số lượng máy tính hạn chế. Một mạng lớn phải cung cấp những phương tiện lọc và định hướng lưu lượng để tránh tình trạng quá tải. Vì thế, những mạng lớn thường được chia thành nhiều đoạn mạng nhỏ hơn. Mỗi đoạn mạng được tách biệt với các mạng khác bằng một số thiết bị lọc. Nếu địa chỉ nguồn và đích đều thuộc cùng một đoạn mạng thì thiết bị lọc sẽ không cho phép dữ liệu được truyền ra mạng lớn hơn (**hình 6.1**). Trong thực tế, việc phân đoạn mạng ngăn chặn một phần lưu lượng đáng kể, vì các máy tính ở khá gần nhau (cùng một phân đoạn). Hầu như cũng chia sẻ thông tin với nhau trên cùng 1 phân đoạn nhiều hơn là ra khỏi phân đoạn mạng này. Chẳng hạn như hai máy tính trong cùng một văn phòng có thể đều đặn trao đổi tập tin, chia sẻ máy in và thỉnh thoảng liên lạc với một máy tính thứ ba ở một nơi khác của tòa nhà.



Hình 6-1 Một thiết bị lọc

Thiết bị lọc lưu lượng (như trong **hình 6.1**) đôi khi được gọi là thiết bị kết nối, mặc dù cụm từ này thỉnh thoảng được sử dụng để mô tả một thiết bị không có chức năng lọc như repeater. Mục đích chính của các thiết bị kết nối gồm:

Điều khiển lưu lượng: Như đã đề cập ở phần trước, một mạng lớn cần phải có một phương tiện lọc và tách ly lưu lượng mạng.

- **Kết nối:** Các thiết bị kết nối có thể kết nối các mạng vật lý không cùng dạng (như ethernet với token ring). Một số thiết bị công chuyển đổi giao thức còn có thể kết nối giữa một mạng sử dụng giao thức này với một mạng sử dụng giao thức khác (như một mạng NetWare sử dụng giao thức IPX/SPX có thể kết nối với mạng Internet sử dụng giao thức TCP/IP).
- **Gán địa chỉ phân cấp:** Một lược đồ gán địa chỉ chẳng hạn như hệ thống gán địa chỉ IP (xem **chương 3, “Lớp Internet”**, và **chương 4, “Phân mạng con”**) cung

cấp một hệ thống phân phối phân cấp, theo đó, địa chỉ mạng như là một con đường và địa chỉ host là một ngôi nhà trên con đường đó. Việc phân đoạn mạng là một biểu thị vật lý của khái niệm gán địa chỉ luận lý này.

- **Phục hồi tín hiệu:** Các thiết bị kết nối có thể phục hồi tín hiệu mạng do đó có thể tăng tối đa kích thước cấp của mạng.

Hiện nay có rất nhiều loại thiết bị kết nối, tất cả đều có vai trò quản lý lưu lượng trong mạng TCP/IP. Phần sau đây sẽ khảo sát về các thiết bị :

- Bridges
- Hubs
- Switches
- Routers

6.1.1 Bridge

Bridge là một thiết bị kết nối thực hiện nhiệm vụ lọc và chuyển tiếp các gói tin theo địa chỉ vật lý. Bridge hoạt động ở lớp liên kết dữ liệu (data link) trong mô hình OSI (được mô tả ở **chương 2, “Lớp truy cập mạng”**, trong phần Lớp truy cập mạng TCP/IP). Trong những năm gần đây, bridge trở nên ít phổ biến vì sự có mặt của nhiều thiết bị mạng đa năng như switch. Tuy nhiên, sự đơn giản của bridge là một điểm khởi đầu tốt cho quá trình khảo sát các thiết bị kết nối mạng.

Mặc dù bridge không phải là một bộ định tuyến, nhưng nó vẫn có bảng định tuyến để phân phối thông tin. Bảng định tuyến dựa trên địa chỉ vật lý này khác hơn và đơn giản hơn nhiều so với bảng định tuyến được mô tả ở phần sau của chương này.

Một bridge lắng nghe các đoạn mạng mà nó kết nối vào và xây dựng thành một bảng định tuyến cho biết những địa chỉ vật lý nào thì thuộc đoạn mạng nào. Khi dữ liệu được truyền trên một trong những phân đoạn mạng, bridge kiểm tra địa chỉ đích của dữ liệu và tra cứu bảng định tuyến. Nếu địa chỉ đích thuộc đoạn mạng mà bridge nhận dữ liệu này thì nó sẽ bỏ qua. Còn nếu địa chỉ đích thuộc một đoạn mạng khác thì bridge sẽ chuyển tiếp dữ liệu đến đoạn mạng thích hợp. Nếu địa chỉ đích không có trong bảng định tuyến thì bridge sẽ chuyển tiếp dữ liệu đến tất cả các đoạn mạng ngoại trừ đoạn mạng mà nó nhận được dữ liệu.

Thông tin thêm

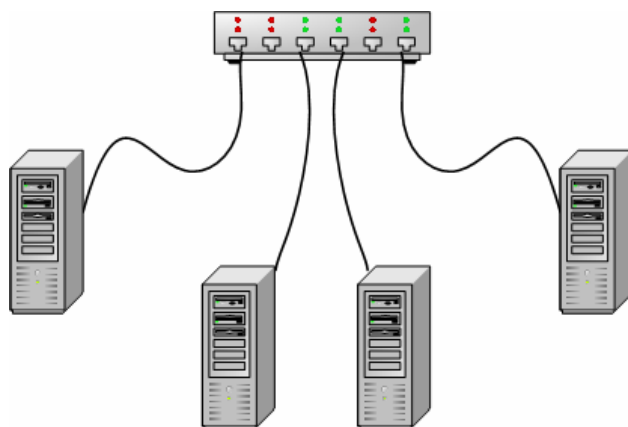
Cần phải nhớ rằng những địa chỉ vật lý của phần cứng được bridge sử dụng thì khác với những địa chỉ IP luận lý.

Bridge là một thiết bị không đắt và đã từng là một phương tiện lọc lưu lượng phổ biến trong các mạng cục bộ (LAN), được sử dụng để tăng số lượng máy tính tham gia vào mạng. Vì bridge chỉ sử dụng những địa chỉ vật lý lớp truy cập mạng và không quan tâm đến địa chỉ luận lý trong phần tiêu đề của IP datagram nên nó không hữu ích để kết nối các mạng khác

loại. Bridge cũng không tham gia vào việc định tuyến IP và các lược đồ phân phối đang được sử dụng để chuyển tiếp dữ liệu trong những mạng lớn như mạng Internet.

6.1.2 Hub

Cho đến một vài năm trước đây, nhiều mạng ethernet vẫn còn sử dụng một mô hình kết nối các máy tính bằng một sợi cáp đồng trục liên tục. Vài năm gần đây, mô hình mạng ethernet sử dụng hub loại 10BASE-T trở nên phổ biến rộng rãi. Hầu hết các mạng ethernet hiện nay đều sử dụng một switch hay hub làm trung tâm để kết nối các máy tính trong mạng (*hình 6.2*).



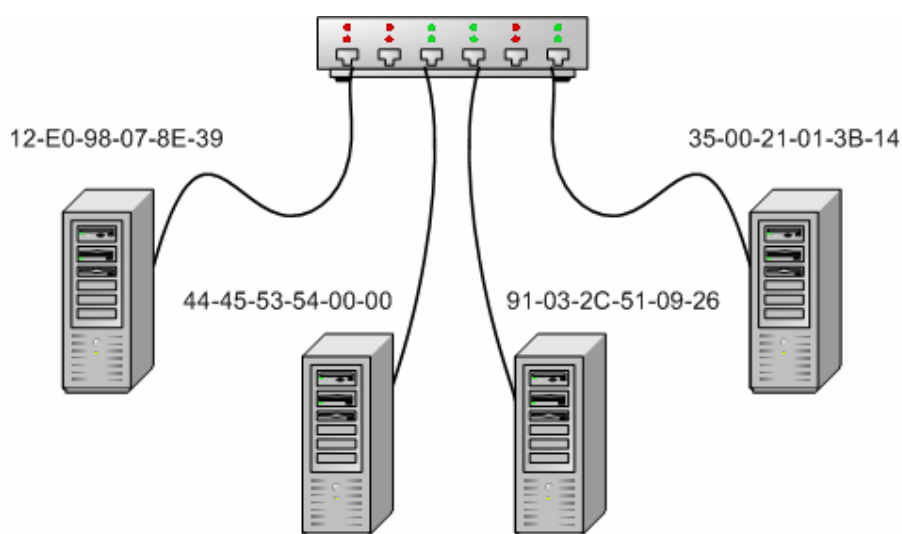
Hình 6-2 Một mạng ethernet sử dụng hub

Như đã đề cập ở *chương 2, “Lớp truy cập mạng”*, khái niệm ethernet được gán cho tất cả các máy tính cùng chia sẻ môi trường truyền dẫn. Mỗi sự truyền dẫn đều được các bộ tương thích mạng (adapter) lắng nghe. Một ethernet hub nhận dữ liệu từ một cổng và phát đi tất cả các cổng còn lại (xem *hình 6.2*). Hay nói cách khác, mạng hoạt động giống như trường hợp tất cả các máy tính được kết nối với nhau bằng một đường dây liên tục. Hub không lọc hoặc định tuyến dữ liệu mà thực hiện việc nhận và truyền lại các tín hiệu.

Một trong những lý do chính của sự phát triển các mạng ethernet sử dụng hub là nhằm làm đơn giản hoá hệ thống dây nối trong mạng. Mỗi máy tính được kết nối với hub thông qua một dây đơn. Một máy tính có thể dễ dàng tách ra và kết nối lại. Trong một văn phòng, thông thường các máy tính được gom thành những nhóm nhỏ, khi đó, một hub có thể đáp ứng được việc này và thực hiện việc kết nối đến các hub khác ở những phần mạng khác nhau. Với việc tất cả các sợi cáp được kết nối đến một thiết bị đơn lẻ, các nhà cung cấp đã sớm nhận ra những cơ hội đổi mới. Những hub phức tạp được gọi là hub thông minh cũng đã bắt đầu xuất hiện. Các hub thông minh này có nhiều tính năng bổ sung như khả năng phát hiện một đường truyền bị lỗi và khóa một cổng (port).

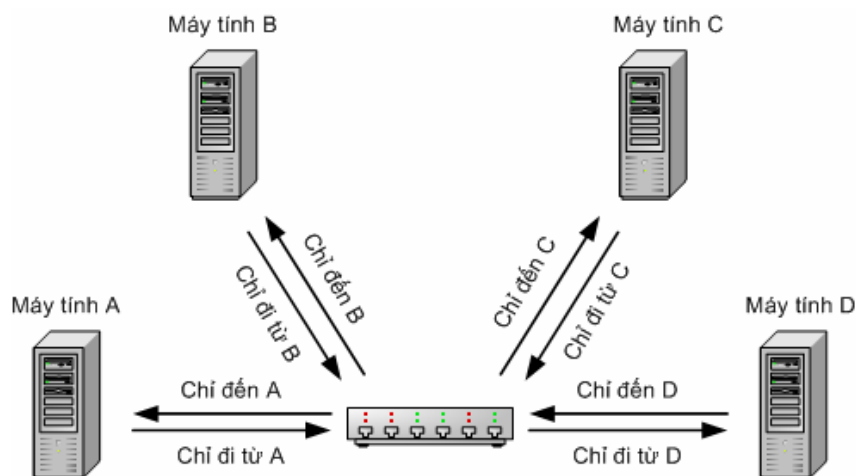
6.1.3 Switch

Một mạng ethernet được xây dựng với hub đã phải đối mặt với một trở ngại lớn: hiệu suất của mạng càng giảm khi lưu lượng càng tăng. Một máy tính không thể truyền dữ liệu nếu đường truyền không rỗi. Hơn nữa, mỗi thiết bị tương thích mạng phải nhận và xử lý tất cả các frame có trên ethernet. Từ hạn chế đó, một phiên bản thông minh của hub, được gọi là switch, được phát triển để giải quyết vấn đề này. Về cơ bản, switch cũng tương tự như hub đã được mô tả trong **hình 6.2**. Mỗi máy tính cũng kết nối đến switch bằng một đường dây đơn lẻ. Tuy nhiên, switch thông minh hơn hub trong việc gửi dữ liệu nhận được từ một cổng. Hầu hết các switch liên kết với mỗi cổng bằng địa chỉ vật lý của thiết bị tương thích mạng kết nối với cổng đó (**hình 6.3**). Khi một máy tính liên kết với một cổng thực hiện việc truyền một frame, switch kiểm tra địa chỉ đích của frame và gửi nó đến cổng có liên kết với địa chỉ đích đó. Hay nói cách khác, switch chỉ gửi frame đến thiết bị cần nhận nó. Các thiết bị tương thích tại các máy tính không phải kiểm tra lại các frame được truyền trên mạng. Switch giảm được những sự truyền dẫn không cần thiết và do đó nó tăng được hiệu suất sử dụng mạng.



Hình 6-3 Một switch liên kết mỗi port với một địa chỉ vật lý

Cần lưu ý rằng, loại switch được mô tả ở trên chỉ hoạt động với địa chỉ vật lý (xem **chương 2, "Lớp truy cập mạng"**), không phải địa chỉ IP. Switch không phải là bộ định tuyến (router). Thực ra switch tương tự như bridge, hay chính xác hơn, nó giống như gồm nhiều bridge được tập trung trong một thiết bị. Switch tách biệt mỗi sự kết nối mạng của nó để chỉ có dữ liệu đến hay đi từ máy tính ở đầu cuối của kết nối đi vào đường dây (**hình 6.4**).



Hình 6-4 Một switch tách biệt mỗi máy tính để giảm lưu lượng

Hiện nay có rất nhiều bộ chuyển mạch (switch) đang lưu hành, nhưng chỉ có hai phương pháp chuyển mạch phổ biến là:

- Cut-through: Theo phương pháp này, switch thực hiện việc chuyển tiếp frame ngay khi có địa chỉ đích.
- Lưu trữ và chuyển tiếp (Store and forward): Switch nhận đầy đủ frame mới thực hiện việc chuyển tiếp. Phương pháp này làm chậm tiến trình truyền, nhưng đôi khi nó lại tăng hiệu suất tổng thể vì nó lọc được những phân mảnh và những frame vô ích.

Trong những năm gần đây, switch trở nên rất phổ biến. Các mạng LAN lớn thường sử dụng một số các switch kết nối với nhau có sự phân lớp để đạt được hiệu quả tối đa.

Switch đã làm nên một cuộc cách mạng lớn với những sự đầu tư khổng lồ nghiên cứu về công nghệ lọc và chuyển tiếp dữ liệu. Ngày nay, các nhà cung cấp xem định nghĩa switch cơ bản ở trên chỉ là một trường hợp đặc biệt trong số một danh mục lớn các loại switch. Theo các nhà cung cấp, về mặt tổng quát thì switch là một thiết bị đưa ra những quyết định chuyển tiếp dựa trên những thông tin trong phần tiêu đề giao thức. Những switch phức tạp hơn còn có thể hoạt động được ở những lớp giao thức cao hơn, do đó, sự quyết định chuyển tiếp cũng sẽ dựa trên nhiều loại thông số hơn.

Theo cách tiếp cận tổng quát hơn về chuyển mạch, các thiết bị được phân loại dựa trên lớp giao thức OSI cao nhất mà nó có thể hoạt động. Tham khảo **hình 1.2** để hiểu thêm về mối quan hệ giữa các lớp giao thức OSI với các lớp TCP/IP. Các lớp thường được đánh số từ dưới lên. Theo đó, switch hoạt động ở lớp liên kết dữ liệu của mô hình OSI, được gọi là switch lớp 2. Những switch có khả năng chuyển tiếp dữ liệu dựa trên thông tin địa chỉ IP ở lớp mạng của mô hình OSI được gọi là switch lớp 3

(cũng có thể xem switch lớp 3 là một loại bộ định tuyến (router). Chúng ta sẽ tìm hiểu về router ở phần sau của chương).

Các switch lớp 4 có thể chuyển tiếp dữ liệu dựa trên nội dung tiêu đề lớp vận chuyển. Như đã khảo sát ở **chương 5, “Lớp vận chuyển”**, lớp vận chuyển chứa thông tin về số hiệu cổng của dịch vụ liên kết với đường truyền. Một switch có khả năng đọc được số hiệu cổng thì có thể xác định được dịch vụ hoặc ứng dụng đang thực hiện việc truyền, nhận dữ liệu. Cụ thể hơn, một switch lớp 4 có thể xác định được các dữ liệu đến được định tuyến đến một web server, mail server hay telnet server. Với khả năng này, các switch lớp 4 có thể kết hợp với một số nhiệm vụ như cân bằng tải, điều khiển truy nhập hay ưu tiên lưu lượng mạng để đáp ứng tiêu chuẩn chất lượng dịch vụ.

Tiếp tục khảo sát những switch phức tạp hoạt động ở những lớp cao của chồng giao thức OSI. Như đã đề cập ở **chương 1, “TCP/IP làm việc như thế nào”**, mô hình TCP/IP không chia nhỏ vai trò của lớp cao như việc phân thành các lớp phiên, lớp trình bày, lớp ứng dụng của mô hình OSI. Tuy nhiên các dịch vụ giống nhau đều được thực hiện ở lớp ứng dụng của TCP/IP. Sự chuyển mạch ở lớp 7, đôi khi còn được gọi là sự chuyển mạch lớp 4-7 hoặc 5-7, có được tất cả các thông tin được mã hóa trong những phần tiêu đề của chồng giao thức và có thể phân chia lưu lượng theo phiên, theo ứng dụng hay theo giao tiếp.

Tất nhiên, một thiết bị có thể thực hiện nhiều chức năng thì khả năng quá tải càng lớn. Sự chuyển mạch giao thức lớp cao sẽ không trở thành hiện thực nếu không có các phần cứng mới hơn, tốc độ xử lý nhanh hơn, và trong tình trạng mạng thông thường, đôi khi những thiết bị tinh vi này lại không cần thiết so với sự phức tạp và chi phí của nó. Tuy nhiên, trong những trường hợp khác, chức năng cân bằng tải của những switch lớp cao có thể đem lại nhiều lợi ích về chi phí và tăng hiệu suất sử dụng mạng.

6.1.4 Router

Router là một thiết bị lọc lưu lượng dựa trên địa chỉ luận lý, nó hoạt động ở lớp Internet (lớp mạng trong mô hình OSI) có sử dụng địa chỉ IP trong phần tiêu đề của lớp Internet.

Router là một thành phần rất quan trọng của bất kỳ mạng TCP/IP cỡ lớn nào. Không có router thì mạng Internet cũng trở nên vô hiệu. Trên thực tế, mạng Internet sẽ không bao giờ phát triển mạnh mẽ như ngày nay nếu không có sự phát triển của router và các giao thức định tuyến TCP/IP.

Một mạng lớn, chẳng hạn như mạng Internet, có rất nhiều router cung cấp nhiều đường đi từ nút mạng nguồn đến nút mạng đích. Các router hoạt động độc lập nhưng

hệ thống phải đảm bảo dữ liệu phải được định tuyến chính xác và hiệu quả trong quá trình hoạt động liên mạng.

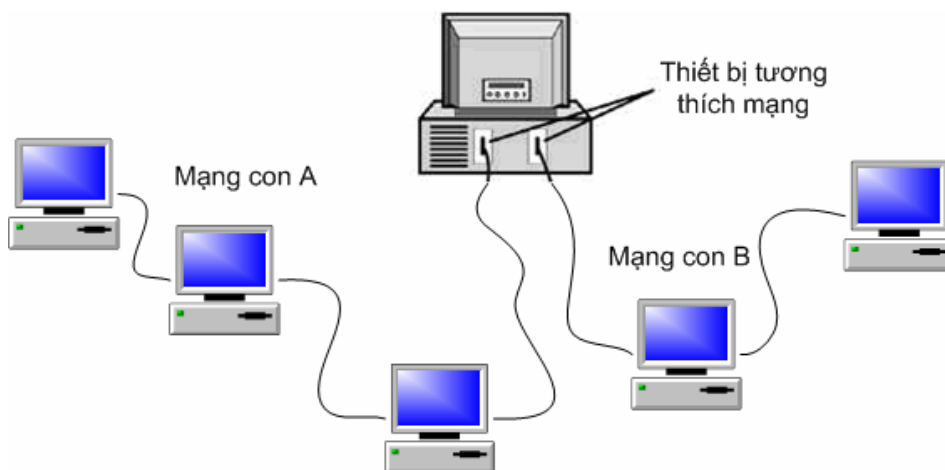
Router phức tạp hơn nhiều so với bridge. Router thay đổi thông tin tiêu đề lớp truy nhập mạng khi nó truyền dữ liệu từ một mạng này sang mạng khác, do đó, router có thể kết nối các loại mạng khác nhau. Rất nhiều router còn lưu lại cả những thông tin chi tiết về đường đi ngắn nhất được tính toán dựa trên khoảng cách, băng thông và thời gian truyền (chúng ta sẽ khảo sát một số giao thức định tuyến ở phần sau của chương).

6.2 Định tuyến trong TCP/IP

Định tuyến trong TCP/IP là một chủ đề được trình bày trong RFC 162 và có thể được viết thành nhiều cuốn sách. Điều đáng nói về định tuyến TCP/IP là khả năng làm việc chính xác và hiệu quả của nó. Một người dùng có thể sử dụng trình duyệt Internet và kết nối đến một máy tính ở Trung Quốc hay Phần Lan mà không phải chuyển tiếp yêu cầu qua hàng loạt thiết bị trên thế giới. Cho dù là một mạng nhỏ, router vẫn đóng vai trò hết sức quan trọng trong việc điều khiển lưu lượng và đảm bảo tốc độ truyền tối đa. Phần này trình bày một số khái niệm quan trọng để có thể hiểu được sự định tuyến trong TCP/IP.

6.2.1 Thế nào là một bộ định tuyến?

Cách tốt nhất để mô tả một bộ định tuyến, hay router, là tìm hiểu về hình dạng và hoạt động của nó. Một router đơn giản nhất trông giống như một máy tính với 2 bộ tương thích mạng. Những router ban đầu thực chất là những máy tính với 2 hay nhiều bộ tương thích (được gọi là các máy tính đa kết nối). **Hình 6.5** trình bày một máy tính đa kết nối hoạt động như một router.



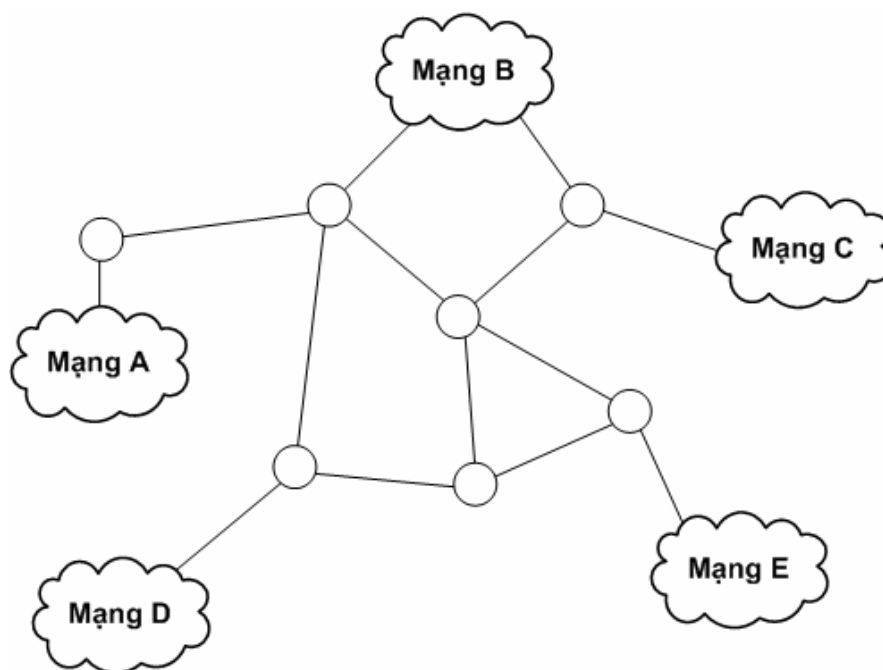
Hình 6-5 Một máy tính đa kết nối hoạt động như một router

Đầu tiên, cần chú ý rằng, địa chỉ IP tương ứng với bộ tương thích chứ không phải với máy tính. Máy tính ở **hình 6.5** có 2 địa chỉ ứng với 2 bộ tương thích. Trên thực tế, hai bộ tương thích này có thể thuộc 2 subnet IP khác nhau, tương ứng với hai mạng vật lý khác nhau. Trong **hình 6.5**, phần mềm giao thức trên máy tính đã kết nối có thể nhận dữ liệu từ phân đoạn A, kiểm tra địa chỉ IP, nếu nó thuộc phân đoạn B, phần mềm sẽ thay thế phần tiêu đề lớp truy cập mạng bằng phần tiêu đề có chứa địa chỉ vật lý của phân đoạn B và chuyển dữ liệu sang phân đoạn B. Trong trường hợp đơn giản này, máy tính đã kết nối hoạt động tương tự như một router.

Để hiểu được toàn bộ mạng hoạt động thế nào, cần nắm những vấn đề sau:

- Router có nhiều hơn 2 cổng (bộ tương thích) và có thể kết nối với nhiều hơn 2 mạng. Theo đó, sự quyết định chuyển tiếp dữ liệu cũng trở nên phức tạp hơn và số lượng đường đi cũng tăng theo.
- Mỗi mạng kết nối với router được kết nối với nhiều mạng khác. Hay nói cách khác, router biết được địa chỉ mạng của những mạng mà nó không kết nối trực tiếp và router phải có chiến lược chuyển tiếp dữ liệu có địa chỉ mạng như thế.
- Một mạng gồm nhiều router thì dữ liệu có nhiều đường đi khác nhau và mỗi router phải có phương thức lựa chọn đường đi hợp lý.

Cấu hình đơn giản trong **hình 6.5** kết hợp với ba vấn đề phức tạp trên đã cho thấy cái nhìn chi tiết hơn về vai trò của router (**hình 6.6**).



Hình 6-6 Định tuyến trong một mạng phức tạp

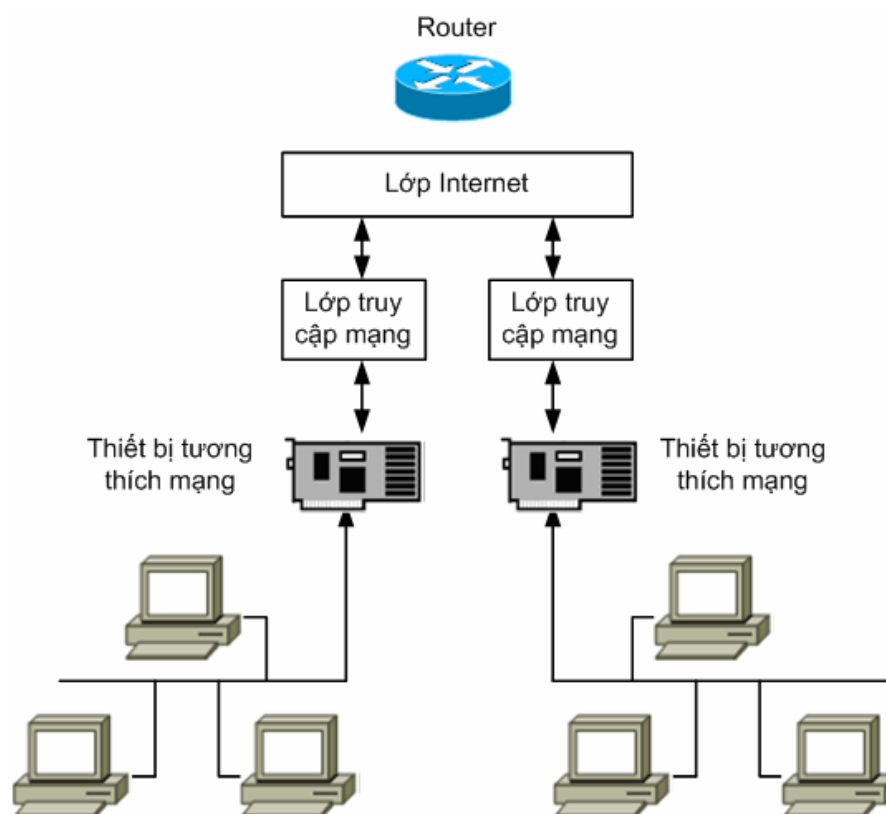
Trong những mạng ngày nay, phần lớn các router không phải là các máy tính đa kết nối. Một thiết bị chuyên dụng trong định tuyến sẽ có hiệu quả cao hơn nhiều. Thiết bị định tuyến được thiết kế đặc biệt để thực hiện hiệu quả các chức năng định tuyến, trong khi đó một máy tính thuần túy cũng không đảm bảo được toàn bộ các chức năng này.

6.2.2 Giới thiệu về định tuyến

Việc xây dựng một bộ định tuyến đơn giản đã được mô tả ở phần trước, và ở phần này, vai trò của nó được trình bày tổng quát hơn với những điểm lưu ý sau:

1. Router nhận dữ liệu từ một trong những mạng kết nối với nó.
2. Router chuyển dữ liệu nhận được lên lớp Internet. Hay nói cách khác, router bỏ đi phần tiêu đề lớp truy cập mạng và tái hợp lại (nếu cần thiết) datagram IP.
3. Router kiểm tra địa chỉ đích trong phần tiêu đề IP. Nếu địa chỉ đích thuộc mạng đã gửi dữ liệu đến thì router bỏ qua dữ liệu này (dữ liệu có thể đã đến đích vì nó được truyền trên mạng của máy tính đích).
4. Nếu đích đến của dữ liệu là một mạng khác thì router sẽ tra cứu trong bảng định tuyến để biết được phải chuyển tiếp dữ liệu đến đâu.
5. Sau khi router xác định được kết nối nào sẽ nhận dữ liệu, nó sẽ chuyển dữ liệu xuống lớp truy cập mạng để truyền tiếp qua kết nối đó.

Tiến trình định tuyến được mô tả ở **hình 6.7**. Bảng định tuyến được mô tả ở bước 4 là một nhân tố cực kỳ quan trọng, nó cùng với giao thức xây dựng bảng định tuyến là hai dấu hiệu đặc trưng của router. Hầu như mọi sự thảo luận về router đều xoay quanh vấn đề làm thế nào router xây dựng được bảng định tuyến và làm thế nào các giao thức định tuyến tập trung được thông tin định tuyến của một tập các router trong một hệ thống nhất.



Hình 6-7 Tiến trình định tuyến

Có hai loại định tuyến được đặt tên dựa trên cách mà nó thu thập được thông tin bảng định tuyến, đó là :

- **Định tuyến tĩnh:** Đối với loại định tuyến này, người quản trị mạng phải nhập các thông tin định tuyến bằng tay.
- **Định tuyến động:** Đối với loại này, bảng định tuyến được xây dựng một cách tự động dựa trên những thông tin có được từ việc sử dụng các giao thức định tuyến.

Định tuyến tĩnh có thể có ích trong một vài trường hợp, nhưng đối với một hệ thống mà người quản trị mạng phải nhập tất cả thông tin định tuyến bằng tay thì cũng có một số hạn chế nhất định. Trước hết, định tuyến tĩnh không thích hợp với những mạng lớn có hàng trăm tuyến đường. Thứ hai, việc định tuyến tĩnh, cho dù là đối với một mạng nhỏ nhất, vẫn đòi hỏi sự đầu tư khá nhiều về thời gian của người quản trị mạng, không những chỉ tạo ra mà còn phải cập nhật thường xuyên những thông tin định tuyến. Tương tự như vậy, một router tĩnh không thể đáp ứng được những thay đổi rất nhanh trong mạng, chẳng hạn như trong trường hợp một router bị hỏng.

Thông tin thêm

Hầu hết các router động đều cho phép người quản trị tùy chọn định tuyến động và cấu hình một đường đi tĩnh đến một địa chỉ cụ thể. Những đường đi tĩnh đã được cấu hình như thế đôi lúc được sử dụng để gỡ rối mạng. Trong những trường hợp khác, đường đi tĩnh được sử dụng để tăng tốc độ kết nối hoặc để chia sẻ lưu lượng mạng.

6.2.3 Bảng định tuyến

Trước khi khảo sát các giao thức định tuyến động, chúng ta cần nắm được một số khái niệm quan trọng. Vai trò của bảng định tuyến và các yếu tố khác của lớp Internet là phân phối dữ liệu đến mạng cục bộ thích hợp. Khi dữ liệu đến mạng cục bộ, các giao thức truy cập mạng sẽ xem xét sự phân phối của nó. Do đó, bảng định tuyến không cần lưu trữ các địa chỉ IP cụ thể mà chỉ cần lưu lại địa chỉ mạng (xem lại **chương 3, “Lớp Internet”, chương 4, “Phân mạng con”** về địa chỉ máy và địa chỉ mạng trong một địa chỉ IP cụ thể).

Nội dung của một bảng định tuyến cơ bản được trình bày trong **hình 6.8**. Một bảng định tuyến cần phải ánh xạ địa chỉ mạng đích trong datagram với địa chỉ IP của chặng kế tiếp - điểm dừng tiếp theo của datagram trên đường đi của nó. Cần lưu ý rằng, bảng định tuyến có sự phân biệt giữa những mạng kết nối trực tiếp với router và những mạng được kết nối gián tiếp qua những router khác. Chặng tiếp theo cũng có thể là mạng đích (nếu nó kết nối trực tiếp) hoặc chỉ là một router trên đường đi đến mạng đích. Trong **hình 6.8**, cổng giao tiếp của router là cổng mà router sử dụng để chuyển tiếp dữ liệu.

Đích đến	Node kế tiếp	Giao diện cổng router
129.14.0.0	Kết nối trực tiếp	1
150.27.0.0	131.100.18.6	3
155.111.0.0	Kết nối trực tiếp	2
165.48.0.0	129.14.16.1	1

Hình 6-8 Bảng định tuyến

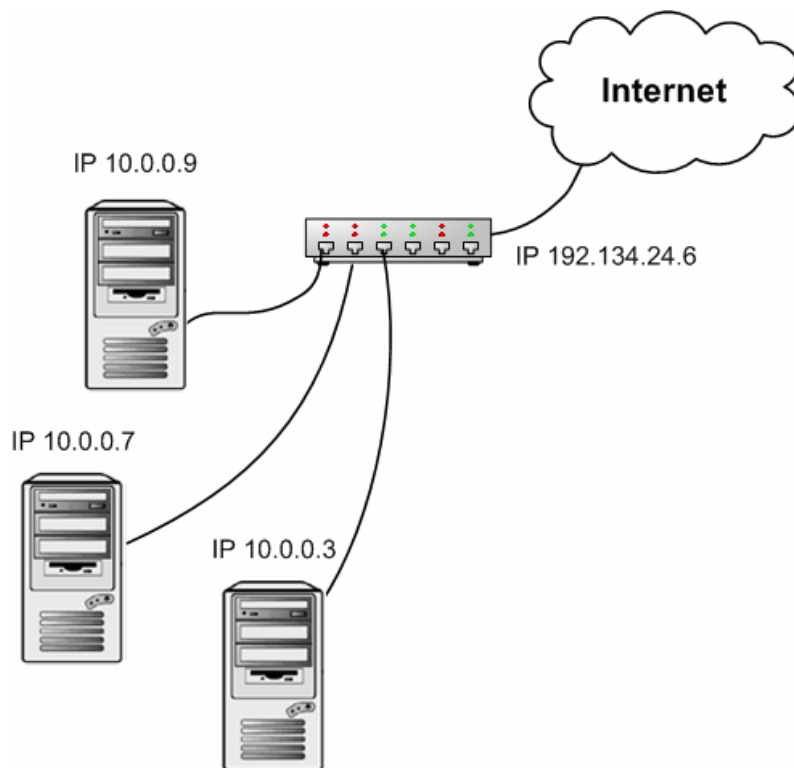
Mục chặng kế tiếp trong bảng định tuyến là chia khoá để hiểu được định tuyến động. Trong một mạng phức tạp, có thể có rất nhiều đường đi đến một đích cụ thể, và router phải xác định được chặng kế tiếp của những đường đi này là gì. Một router định tuyến động sẽ dựa trên những giao thức định tuyến để đưa ra quyết định này.

Thông tin thêm

Một máy chủ (host), giống như một router, cũng có thể có một bảng định tuyến nhưng vì nó không thực hiện các chức năng định tuyến nên bảng định tuyến của nó không phức tạp. Những máy tính này thường sử dụng một router mặc định hoặc gateway mặc định. Gateway mặc định là một router sẽ nhận datagram nếu datagram đó không phân phối được trong mạng cục bộ hoặc đến một router khác.

6.3 Chuyển đổi địa chỉ mạng (NAT)

Như chúng ta đã thấy, các thiết bị mạng ngày càng trở nên phức tạp. Một tiến bộ mới là sự xuất hiện của các router thực hiện chức năng chuyển đổi địa chỉ mạng (NAT). Một thiết bị NAT sẽ làm ẩn đi những chi tiết của mạng cục bộ và che dấu sự tồn tại của mạng cục bộ. **Hình 6.9** mô tả một NAT trong mạng Internet. Thiết bị NAT có vị trí như là một gateway kết nối các máy tính trong mạng cục bộ với Internet. Đằng sau thiết bị NAT, mạng cục bộ có thể sử dụng bất kỳ không gian địa chỉ nào. Nó cũng không nhất thiết phải sử dụng các địa chỉ Internet được chỉ định vì lúc này, mạng cục bộ không phải là một phần của Internet. Thiết bị NAT hoạt động như một sự uỷ quyền của mạng cục bộ trên mạng Internet. Khi một máy tính cục bộ cố gắng thực hiện kết nối đến một địa chỉ Internet, thiết bị NAT sẽ thực hiện sự kết nối đó. Tất cả các gói tin nhận được từ Internet đều được chuyển đổi theo lược đồ địa chỉ của mạng cục bộ và sau đó được chuyển tiếp đến máy tính đã khởi tạo kết nối.



Hình 6-9 Một thiết bị chuyển đổi địa chỉ mạng

Một thiết bị NAT sẽ làm tăng tính bảo mật của mạng bởi vì nó có thể ngăn chặn sự tấn công từ bên ngoài vào mạng cục bộ. Đối với mạng bên ngoài, thiết bị NAT giống như một máy đơn được kết nối Internet. Nếu kẻ tấn công biết được địa chỉ của một máy trong mạng cục bộ, hắn cũng không thể mở một kết nối đến mạng cục bộ vì sơ đồ gán địa chỉ cục bộ độc lập với không gian địa chỉ của Internet. Một thiết bị NAT cũng sẽ tiết kiệm được số lượng địa chỉ Internet cần thiết cho một tổ chức. Chỉ có thiết bị NAT mới được truy cập từ Internet. Tính kinh tế của việc tiết kiệm được ít địa chỉ Internet và khả năng bảo mật của mạng riêng đã làm cho thiết bị NAT trở nên rất phổ biến trong các mạng cục bộ và mạng intranet.

Thông tin thêm

Bảo mật là một vấn đề không đơn giản, ngay cả việc bảo mật bằng thiết bị NAT cũng bị đe dọa. Một số thiết bị NAT cho phép người quản trị có thể truy cập được từ Internet và tính năng này dễ gây ra nguy hiểm cho mạng bên trong nếu nó không được quản lý chặt chẽ.

Một thiết bị NAT là một hình thức của một máy chủ uỷ quyền (proxy server). Máy chủ uỷ quyền là một máy tính hoạt động đại diện cho các máy tính khác. Theo đó, những máy tính này sẽ độc lập với Internet và máy chủ uỷ quyền đảm nhiệm vai trò liên lạc với mạng bên ngoài cũng như thực hiện việc truyền, hồi đáp cho các máy tính thích hợp bên trong mạng cục bộ.

Tóm tắt

Chương này đã khảo sát một số thiết bị mạng phổ biến. Chúng ta đã tìm hiểu rõ hơn về bridge, hub và switch. Chương kế tiếp sẽ trình bày kỹ hơn về vấn đề định tuyến trong mạng TCP/IP.

CHƯƠNG

7

ĐỊNH TUYẾN

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Chuyển tiếp IP**
- **Định tuyến trực tiếp và gián tiếp**
- **Các giao thức định tuyến**

Kết thúc chương này bạn sẽ có thể :

- Trình bày được sự chuyển tiếp IP và cách thức hoạt động của nó
- Phân biệt được định tuyến vector khoảng cách (distance vector) và định tuyến trạng thái liên kết (link state)
- Nắm được vai trò của những router lõi, router nội, router ngoại
- Hiểu được các giao thức định tuyến nội phổ biến: RIP và OSPF.

7.1 Giới thiệu về định tuyến trong TCP/IP

Cơ sở hạ tầng xây dựng những mạng toàn cầu như mạng Internet sẽ không thể hoạt động nếu không có các router. TCP/IP được thiết kế để hoạt động trên router và mọi sự tìm hiểu về TCP/IP sẽ không hoàn thiện nếu không tìm hiểu về hoạt động của router. Như chúng ta đã khảo sát ở chương trước, một router tham gia vào tiến trình liên lạc phức tạp với những router khác trên mạng để xác định được đường đi tốt nhất cho mỗi đích đến. Trong chương này, chúng ta sẽ tìm hiểu về router, bảng định tuyến và các giao thức định tuyến.

7.2 Trở lại vấn đề router

Chúng ta cũng đã biết được vai trò của router là chuyển tiếp datagram dựa trên địa chỉ IP. Do đó, có thể nói router là một thiết bị mạng thực hiện sơ đồ định vị IP như đã thảo luận ở **chương 3, “Lớp Internet”**. **Hình 6.2** đã minh họa router giống như một máy tính với nhiều card mạng được kết nối với nhiều phân đoạn mạng. Khi router nhận được một datagram từ một trong các cổng của mình, nó sẽ phân tích datagram đó để xác định địa chỉ IP đích. Nếu địa chỉ đích thuộc cùng phân đoạn mạng với địa chỉ nguồn thì không cần thực hiện việc chuyển tiếp dữ liệu và router sẽ bỏ qua datagram đó. Nếu địa chỉ đích thuộc một phân đoạn mạng khác, router sẽ chuyển tiếp datagram theo thông tin được xây dựng trong bảng định tuyến.

Router trở nên rất cần thiết vì những lý do sau:

- Router cung cấp kỹ thuật phân phối quan trọng cho việc gán địa chỉ IP (xem **chương 3, “Lớp Internet”** và **chương 4, “Phân mạng con”**). Hệ thống phân cấp hiệu quả và thích hợp cho các mạng và các mạng con đòi hỏi phải có những thiết bị mạng thực hiện việc định tuyến datagram dựa trên địa chỉ IP.
- Router thực hiện việc lọc lưu lượng, do đó mỗi host không phải theo dõi những bản tin được gán địa chỉ đến một host khác. Như đã khảo sát ở **chương 6, “Phản ứng mạng”**, switch cũng lọc lưu lượng, nhưng đa số switch đều sử dụng địa chỉ vật lý do đó không hiệu quả trong những mạng lớn.
- Router che dấu được những chi tiết của mạng vật lý. Vì việc chuyển tiếp IP xảy ra bên trên lớp truy cập mạng nên các router có thể kết nối được với những mạng không cùng loại. Một máy tính trong một mạng ethernet LAN ở Connecticut có thể liên lạc với một máy tính trong một mạng token ring LAN ở Istanbul cho dù những bộ tương thích mạng của 2 loại mạng này không tương thích với nhau.

Thật khó có thể trình bày mọi chủ đề về router mà chỉ gói gọn trong một chương. Những hình ảnh và những mô tả đôi khi được đơn giản hoá để người đọc dễ dàng nắm bắt khái niệm. Trong khi đó, những lợi ích thực sự của router được thể hiện rõ ở những mạng lớn, đa dạng và định tuyến động, nơi mà một nhóm các router liên tục chia sẻ thông tin để giữ đường truyền thông suốt.

7.2.1 Vài nét về chuyển tiếp IP (IP forwarding)

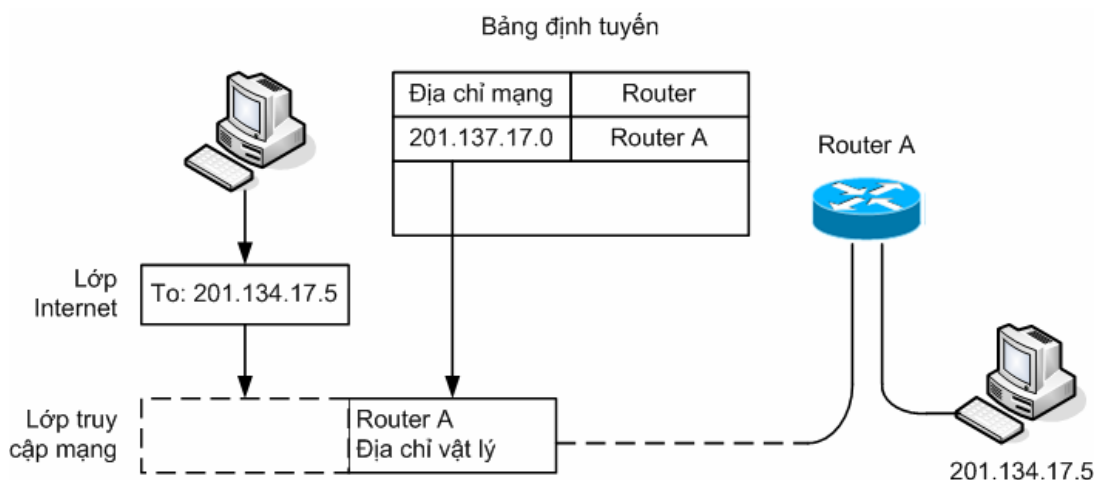
Cả host và router đều có bảng định tuyến nhưng bảng định tuyến của host thì đơn giản hơn nhiều so với của router. Bảng định tuyến của một máy tính đơn có thể có 2 dòng: một là lộ trình mạng cục bộ và hai là lộ trình mặc định của những gói tin không thể phân phối trong mạng cục bộ. Thông tin định tuyến đơn giản này cũng đủ để chuyển một datagram đến đích của nó. Trong phần sau của chương, chúng ta sẽ biết được vai trò của router phức tạp hơn nhiều.

Như đã tìm hiểu ở **chương 3, “Lớp Internet”**, phần mềm TCP/IP sử dụng ARP để phân giải địa chỉ IP thành địa chỉ vật lý bên trong mạng cục bộ. Nhưng nếu địa chỉ IP không nằm bên trong mạng cục bộ thì điều gì sẽ xảy ra ? Như đã giải thích ở **chương 3**, nếu địa chỉ IP không thuộc mạng cục bộ, thì máy tính sẽ gửi datagram đến một router. Đến đây, vấn đề bắt đầu trở nên phức tạp hơn. Phần tiêu đề IP (**hình 3.3**) chỉ liệt kê địa chỉ IP đích và nguồn. Nó không đủ chỗ trống để lưu lại địa chỉ của các router trung gian thực hiện việc chuyển tiếp các datagram đến đích. Cần lưu ý rằng tiến trình chuyển tiếp IP thật ra không gán địa chỉ của router vào phần tiêu đề của IP mà thay vào đó, máy host chuyển datagram và địa chỉ IP của router xuống lớp truy cập mạng, ở đó, phần mềm giao thức sẽ sử dụng một tiến trình tra cứu riêng để gói kèm datagram trong một frame rồi phân phối đến router. Hay nói cách khác, địa chỉ IP của datagram chỉ đến host nhận dữ liệu. Địa chỉ vật lý của frame được sử dụng để chuyển tiếp datagram đến router trong mạng cục bộ là địa chỉ của cổng giao tiếp trên router.

Có thể tóm tắt tiến trình này như sau:

1. Khi một host muốn gửi một datagram, nó kiểm tra lại bảng định tuyến của mình.
2. Nếu datagram không phân phối được trong mạng cục bộ, máy host sẽ trích ra trong bảng định tuyến địa chỉ IP của router liên kết với địa chỉ đích (trong trường hợp host này đang nằm trong một mạng cục bộ thì địa chỉ IP của router cũng giống như địa chỉ của gateway mặc định). Sau đó, địa chỉ IP của router được phân giải thành địa chỉ vật lý bằng giao thức ARP.
3. Tiếp theo, datagram (được định tuyến đến host ở xa) được chuyển qua lớp truy cập mạng cùng với địa chỉ vật lý của router nhận.

4. Bộ tương thích mạng của router sẽ nhận frame vì lúc này địa chỉ vật lý đích của frame chính là địa chỉ vật lý của router.
5. Router mở frame và chuyển datagram lên lớp Internet.
6. Router kiểm tra địa chỉ IP của datagram. Nếu địa chỉ IP đó khớp với địa chỉ của router, dữ liệu sẽ được chính router nhận. Còn nếu không khớp, router sẽ kiểm tra bảng định tuyến của nó để tìm ra đường đi thích hợp với địa chỉ đích của datagram và chuyển tiếp datagram đó.
7. Nếu datagram không thể phân phối được trên bất kỳ phân đoạn mạng nào liên kết với router, router sẽ gửi datagram đó đến một router khác và tiến trình sẽ lặp lại (quay lại bước 1) cho đến khi router cuối cùng có thể phân phối trực tiếp datagram đó đến host đích.

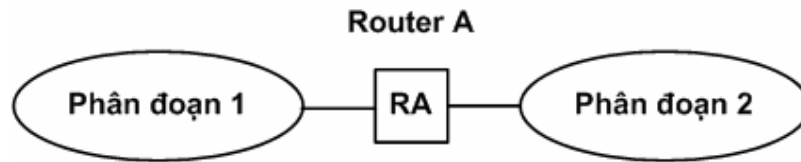


Hình 7-1 Tiến trình chuyển tiếp IP

Tiến trình chuyển tiếp dữ liệu được mô tả ở bước 6 là một đặc trưng quan trọng của router. Lưu ý rằng nếu một thiết bị có 2 card mạng thì hoạt động vẫn không giống router. Nếu thiết bị không có phần mềm hỗ trợ chuyển tiếp IP thì dữ liệu sẽ không thể truyền từ giao tiếp này sang một giao tiếp khác. Khi một máy tính không được cấu hình định tuyến IP nhận được một datagram có đích đến là một máy tính khác thì nó sẽ bỏ qua datagram đó.

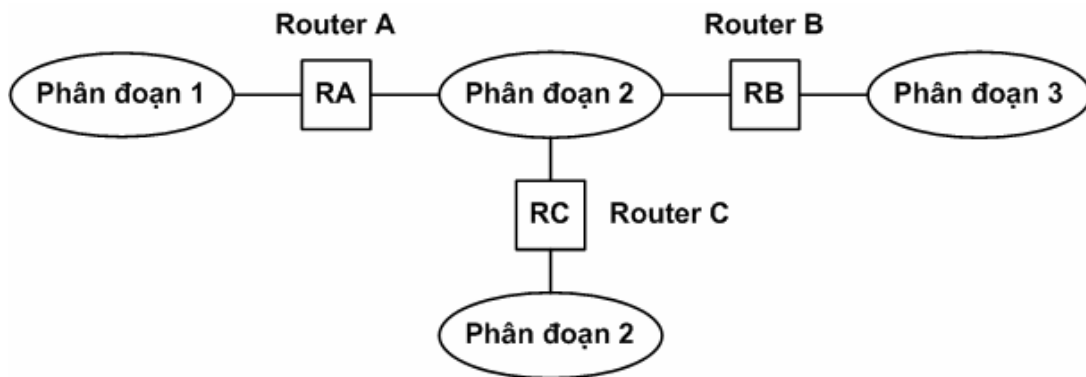
7.2.2 Định tuyến trực tiếp và gián tiếp

Nếu một router chỉ kết nối với 2 mạng con thì bảng định tuyến của nó sẽ rất đơn giản. Theo **hình 7.2**, router được kết nối với tất cả các mạng con và nó sẽ không bao giờ biết được một địa chỉ IP không kết hợp với một cổng của nó. Hay nói cách khác, router này có thể định tuyến trực tiếp bất kỳ datagram nào.



Hình 7-2 Một router kết nối 2 phân đoạn mạng có thể định tuyến trực tiếp tới mỗi phân đoạn

Tiếp tục khảo sát một mạng phức tạp hơn ở **hình 7.3**. Trong trường hợp này, router A không kết nối với phân đoạn 3 và sẽ không tìm thấy phân đoạn 3 nếu không có một vài hỗ trợ. Trường hợp này được gọi là định tuyến gián tiếp. Hầu hết các mạng định tuyến phụ thuộc vào mức độ định tuyến gián tiếp nào đó. Một mạng lớn có thể có hàng tá router, trong đó không có nhiều hơn một hoặc hai mạng kết nối trực tiếp tới mỗi đoạn mạng. Chúng ta sẽ xem xét những mạng như thế này ở phần sau của chương. Bây giờ, một câu hỏi được đặt ra ở **hình 7.3** là: Làm thế nào router A tìm thấy phân đoạn 3? và làm thế nào router A biết được phải chuyển những datagram có địa chỉ đích là phân đoạn 3 sang router B chứ không phải là router C.



Hình 7-3 Một router phải thực hiện định tuyến gián tiếp nếu nó phải chuyển tiếp các datagram sang những mạng không kết nối trực tiếp với nó

Có hai cách để router biết được các lộ trình gián tiếp là:

- Từ người quản trị hệ thống.
- Từ những router khác.

Hai tùy chọn này tương ứng với hai phương pháp định tuyến tĩnh và động đã được trình bày ở **chương 6, "Phần cứng mạng"**. Một là người quản trị hệ thống có thể nhập các đường đi trực tiếp vào bảng định tuyến. Cách này là định tuyến tĩnh. Một cách khác là router B có thể thông báo cho router A về phân đoạn 3, và đây chính là định tuyến động. Việc định tuyến động mang lại nhiều lợi ích thiết thực. Đầu tiên, nó không cần sự đầu tư về nhân sự. Thứ hai, nó sẵn sàng đáp ứng với những thay đổi của mạng. Nếu một mạng mới được kết nối với router B, router B có thể thông báo với router A về sự thay đổi này.

Trong khi đó, định tuyến tĩnh có thể mang lại hiệu quả đối với những mạng nhỏ, đơn giản và cố định. Nó có thể chấp nhận được đối với một mạng đơn giản như **hình 7.3**, nhưng khi số lượng router tăng, định tuyến tĩnh trở nên không thích hợp. Số lượng đường đi sẽ tăng lên rất nhiều khi thêm một phân đoạn vào mạng. Quan trọng hơn, sự ảnh hưởng của đường đi tĩnh trong một mạng lớn có thể dẫn đến những đường đi dài, thiếu hiệu quả, thậm chí có thể bị lặp.

Lưu ý rằng chúng ta có thể cấu hình định tuyến tĩnh ở **hình 7.3** theo cách mặc định. Trong trường hợp đó, router A sẽ không thấy được phân đoạn 3. Nó chỉ có thể chuyển bất kỳ datagram có địa chỉ mà nó không biết đến router B và router B sẽ quyết định hoạt động tiếp theo. Cần nhắc lại rằng trường hợp này có thể thực hiện được dễ dàng trong những mạng nhỏ như trong **hình 7.3**. Tuy nhiên, lộ trình mặc định là một đường đi tĩnh và việc cấu hình các đường đi mặc định cho các router trong một mạng phức tạp thì dễ mắc phải một số hạn chế của định tuyến tĩnh làm giảm hiệu suất mạng.

Vì những lý do này mà các router hiện đại đã sử dụng một dạng định tuyến động nào đó. Các router kết nối với nhau để chia sẻ thông tin về các phân đoạn mạng, các đường đi, và mỗi router xây dựng một bảng định tuyến của mình bằng cách sử dụng những thông tin có được trong tiến trình liên lạc này. Phần sau đây sẽ mô tả về cơ chế hoạt động của định tuyến động.

Thông tin thêm

Router đôi khi còn sử dụng kết hợp cả định tuyến động và định tuyến tĩnh. Người quản trị hệ thống có thể cấu hình một vài đường đi tĩnh và chỉ định những đường đi khác được định tuyến động. Những đường đi tĩnh đôi lúc còn được sử dụng để ép lưu lượng đi theo một đường cố định. Chẳng hạn, một người quản trị hệ thống có thể cấu hình các router để lưu lượng đi theo một đường truyền có băng thông rộng.

7.2.3 Các thuật toán định tuyến động

Những router trong cùng một nhóm thực hiện việc trao đổi thông tin đầy đủ về hệ thống mạng để mỗi router có thể xây dựng một bảng định tuyến mô tả những con đường cho các datagram đi đến một phân đoạn mạng cụ thể. Điều gì đã giúp cho các router thực hiện việc truyền thông một cách chính xác? Một router xây dựng bảng định tuyến của nó như thế nào? Chúng ta có thể khẳng định rằng hoạt động của router hoàn toàn dựa trên bảng định tuyến. Hiện nay có rất nhiều giao thức định tuyến đang được sử dụng nhưng chúng ta có thể phân loại các giao thức này thành hai phương thức định tuyến sau:

- Định tuyến vector khoảng cách (distance vector).
- Định tuyến trạng thái liên kết (link state).

Những phương pháp này được hiểu như là những cách khác nhau để liên lạc và thu thập các thông tin định tuyến. Phần sau đây sẽ thảo luận về định tuyến vector

khoảng cách và trạng thái liên kết. Và tiếp theo đó, chúng ta sẽ khảo sát về hai giao thức định tuyến sử dụng hai phương pháp này là: RIP (giao thức định tuyến vector khoảng cách) và OSPF (giao thức định tuyến trạng thái liên kết).

Thông tin thêm

Vector khoảng cách và trạng thái liên kết là hai lớp giao thức định tuyến và sự thực hiện thực sự của mỗi giao thức còn có nhiều chi tiết và chức năng bổ sung hơn nữa. Nhiều router cũng hỗ trợ các kịch bản khởi động, các mục định tuyến tĩnh, và những chức năng khác để mô tả định tuyến vector khoảng cách hoặc trạng thái liên kết.

7.2.3.1 Định tuyến vector khoảng cách

Định tuyến vector khoảng cách (còn được gọi là định tuyến Bellman-Ford) là một phương pháp định tuyến đơn giản, hiệu quả và được sử dụng trong nhiều giao thức định tuyến. Nó đã từng chiếm ưu thế trong công nghệ định tuyến và hiện vẫn còn khá phổ biến, mặc dù gần đây, nhiều phương pháp định tuyến phức tạp (như định tuyến trạng thái liên kết) đã được phát triển rộng rãi.

Vector khoảng cách được thiết kế để giảm tối đa sự liên lạc giữa các router cũng như lượng dữ liệu trong bảng định tuyến. Bản chất của định tuyến vector khoảng cách là một router không cần biết tất cả các đường đi đến các phân đoạn mạng - nó chỉ cần biết phải truyền một datagram được gán địa chỉ đến một phân đoạn mạng đi theo hướng nào. Khoảng cách giữa các phân đoạn mạng được tính bằng số lượng router mà datagram phải đi qua khi được truyền từ phân đoạn mạng này đến phân đoạn mạng khác. Router sử dụng thuật toán vector khoảng cách để tối ưu hoá đường đi bằng cách giảm tối đa số lượng router mà datagram đi qua. Tham số khoảng cách này chính là số chặng phải qua (hop count).

Thông tin thêm

Phương pháp định tuyến đã được giới thiệu ở **chương 6** chính là phương pháp định tuyến vector khoảng cách.

Định tuyến vector khoảng cách hoạt động như sau :

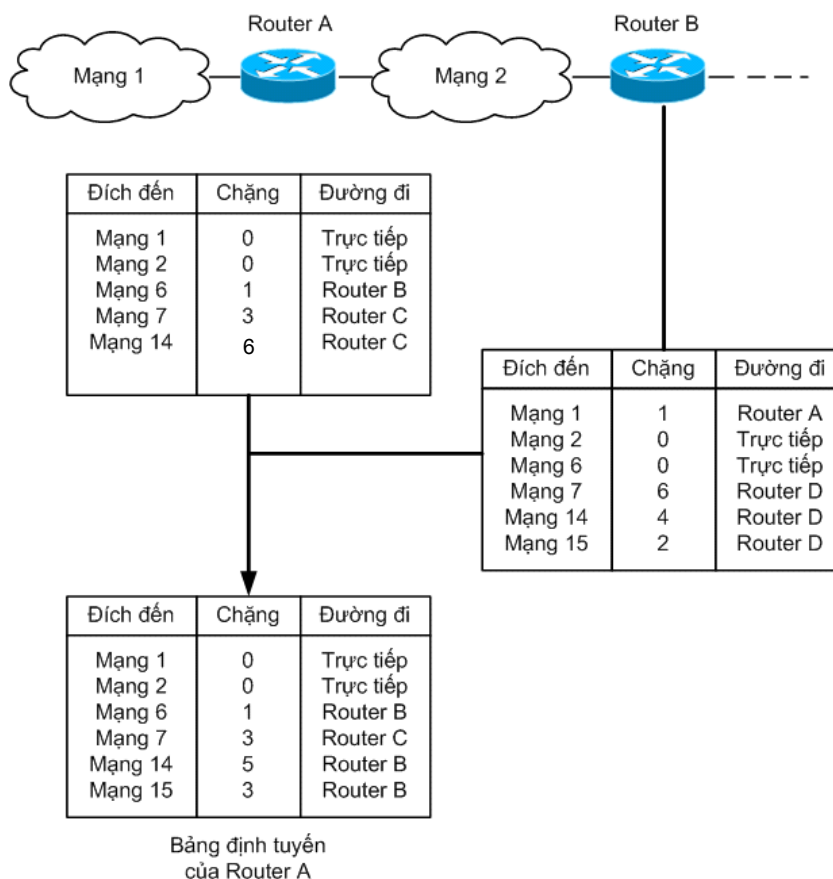
1. Khi router A khởi tạo, nó nhận biết các phân đoạn mạng mà nó kết nối trực tiếp và lưu lại các phân đoạn mạng này trong bảng định tuyến của nó. Giá trị hop count của mỗi phân đoạn mạng được kết nối trực tiếp là 0 vì datagram sẽ không phải truyền qua bất cứ router nào khi đi từ A đến một phân đoạn mạng kết nối trực tiếp.
2. Định kỳ, router sẽ nhận được một bảng báo cáo trạng thái của mỗi router kế cận. Bảng này liệt kê mọi phân đoạn mạng mà router kế cận biết được và giá trị hop count đến mỗi phân đoạn đó.

3. Khi router A nhận được bảng báo cáo từ router kế cận, nó tích hợp những thông tin định tuyến mới vào bảng định tuyến của nó như sau:

- A. Nếu router B biết được phân đoạn mạng mà hiện tại chưa có trong bảng định tuyến của router A thì router A sẽ thêm phân đoạn mạng này vào bảng định tuyến của nó. Đường đi đến phân đoạn mạng mới này là router B, nghĩa là, nếu router A nhận một datagram có địa chỉ là phân đoạn mới này thì nó sẽ chuyển tiếp datagram đó đến router B. Giá trị hop count của phân đoạn mới này bằng giá trị hop count của nó đối với router B cộng với 1, vì router A xa phân đoạn mới hơn router B một chặng.
- B. Nếu router B liệt kê một phân đoạn đã có trong bảng định tuyến của router A thì router A cộng một vào giá trị hop count mới nhận được từ B và so sánh giá trị hop count mới này với giá trị hop count có trong bảng định tuyến. Nếu đường đi qua B tốt hơn (ít chặng hơn) đường đi mà router A đã biết trước đó thì router A sẽ cập nhật lại bảng định tuyến của nó và xem router B là đường đi của những datagram có địa chỉ đích là phân đoạn mạng đang xét.
- C. Nếu giá trị hop count của đường đi qua B đến phân đoạn mạng đang xét (giá trị hop count nhận được từ B cộng với 1) lớn hơn giá trị hop count đang có trong bảng định tuyến của A thì đường đi qua B sẽ không được sử dụng. Router A vẫn tiếp tục sử dụng đường đi đã được lưu trong bảng định tuyến của nó.

Với mỗi chu kỳ cập nhật, router có được một bức tranh hoàn chỉnh hơn về mạng hiện tại. Thông tin về các đường đi được lan truyền dần trên mạng. Giả sử không có gì thay đổi trên mạng thì router vẫn biết được những đường đi hiệu quả nhất đến từng phân đoạn mạng.

Một ví dụ về sự cập nhật của phương pháp định tuyến vector khoảng cách được trình bày trong **hình 7.4**. Lưu ý rằng, trong ví dụ này, những cập nhật khác đã xảy ra vì cả router A và B đều biết về những mạng mà nó không trực tiếp kết nối. Trong trường hợp này, router B có một đường đi hiệu quả hơn đến phân đoạn mạng 14, vì vậy, router A phải cập nhật bảng định tuyến của nó để gửi dữ liệu đến đoạn mạng 14 qua router B. Router A có đường đi tốt hơn đến đoạn mạng 7, do đó, bảng định tuyến sẽ không có gì thay đổi cho con đường tới mạng 7.



Hình 7-4 Sự cập nhật trong định tuyến vector khoảng cách

Thông tin thêm

Những đích đến đã được liệt kê trong **hình 7.4** (mạng 1, mạng 2, ...) hoặc là mạng IP hoặc là mạng con IP, tùy từng trường hợp.

7.2.3.2 Định tuyến trạng thái liên kết

Định tuyến vector khoảng cách là một phương pháp thích hợp nếu ta giả định hiệu quả của đường đi phụ thuộc vào số lượng router mà datagram phải đi qua. Giả sử này là một điểm khởi đầu khá tốt, tuy nhiên, trong một vài trường hợp thì điều này lại trở nên quá đơn giản. Theo đó, định tuyến vector khoảng cách không phù hợp lắm đối với một mạng lớn gồm rất nhiều router. Khi đó, mỗi router phải duy trì một mục trong bảng định tuyến cho mỗi đích, và các mục này đơn thuần chỉ chứa các giá trị vector và hop count. Router cũng không thể tiết kiệm năng lực của mình khi đã biết nhiều về cấu trúc mạng. Hơn nữa, toàn bộ bảng giá trị khoảng cách và hop count phải được truyền giữa các router cho dù hầu hết các thông tin này không thực sự cần thiết trao đổi giữa các router. Các nhà nghiên cứu máy tính bắt đầu đặt ra nhiều câu hỏi và cuối cùng định

tuyến trạng thái liên kết đã được ra đời từ những thảo luận này. Định tuyến trạng thái liên kết hiện nay là thay thế chính cho định tuyến vector khoảng cách.

Bản chất của định tuyến trạng thái liên kết là mỗi router sẽ xây dựng bên trong nó một sơ đồ cấu trúc mạng. Định kỳ, mỗi router cũng gửi ra mạng những thông điệp trạng thái. Những thông điệp này liệt kê những router khác trên mạng kết nối trực tiếp với router đang xét và trạng thái của liên kết. Các router sử dụng các bản tin trạng thái nhận được từ các router khác để xây dựng sơ đồ mạng. Khi một router chuyển tiếp dữ liệu, nó sẽ chọn đường đi đến đích tốt nhất dựa trên những điều kiện hiện tại.

Giao thức trạng thái liên kết đòi hỏi nhiều thời gian xử lý trên mỗi router, nhưng giảm được sự tiêu thụ băng thông, bởi vì mỗi router không cần thiết phải gửi toàn bộ bảng định tuyến của mình. Hơn nữa, Router cũng dễ dàng theo dõi lỗi trên mạng vì bản tin trạng thái từ một router không thay đổi khi lan truyền trên mạng (ngược lại, đối với phương pháp vector khoảng cách, giá trị hop count tăng lên mỗi khi thông tin định tuyến đi qua một router khác).

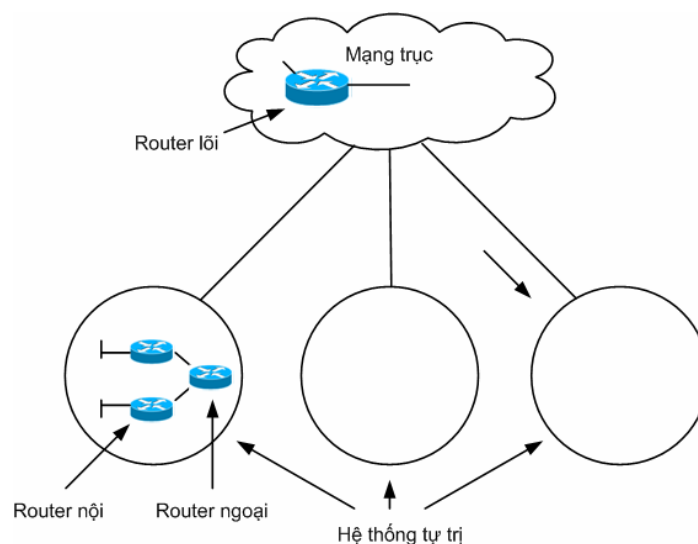
7.3 Định tuyến trong những mạng phức tạp

Phần lớn chương này đều tập trung vào trường hợp chỉ có một router hoặc một nhóm router đơn lẻ. Trên thực tế, một vài mạng lớn gồm có cả hàng trăm router. Mạng Internet thì gồm có hàng ngàn router. Trong những mạng lớn như mạng Internet thì việc tất cả các router cùng chia sẻ những thông tin cần thiết để hỗ trợ các phương pháp định tuyến như đã mô tả ở trên là rất khó khả thi. Nếu một router phải biên soạn và xử lý các thông tin định tuyến cho mỗi router trên Internet thì lưu lượng mạng và kích thước của bảng định tuyến sẽ sớm bị quá tải. Nhưng thực tế, mỗi router trên Internet không cần thiết phải biết những thông tin về các router khác. Một router trong một phòng mạch ở Istanbul có thể hoạt động liên tục trong nhiều năm mà không phải biết những thông tin về một router khác tại công ty sơn ở Lima, Peru. Nếu mạng được tổ chức hiệu quả thì hầu hết các router chỉ cần trao đổi thông tin giao thức định tuyến với những router kề cận.

Trong hệ thống mạng ARPAnet, một nhóm các router lõi hoạt động như một mạng xương sống (*backbone*) trung tâm liên kết các mạng riêng lẻ được cấu hình và quản lý tự trị. Những router lõi biết được mỗi mạng cho dù nó không cần phải biết về mỗi mạng con. Mỗi datagram chỉ cần tìm thấy được đường đi đến một router lõi thì nó có thể đến được bất kỳ một vị trí nào trong hệ thống. Những router trong các mạng nhánh của lõi không cần biết về các mạng khác trên thế giới mà chỉ cần biết gửi dữ liệu giữa chúng và làm thế nào để đến các router lõi.

Hệ thống này được mô phỏng như hệ thống trong **hình 7.5**. Những router lõi trong mạng trực truyền các bản tin giữa các mạng với nhau. Kết nối với mạng lõi là

những mạng được quản lý độc lập được gọi là các hệ thống tự trị (autonomous system). Một hệ thống tự trị có thể là một mạng của một tổ chức hay công ty, và trong thời gian gần đây, nó còn là một hệ thống mạng được kết nối Internet qua một nhà cung cấp dịch vụ (ISP). Người sở hữu hệ thống tự trị sẽ quản lý các chi tiết về cấu hình của các router trong hệ thống. Những router nội nằm bên trong hệ thống tự trị chia sẻ thông tin và xây dựng những bảng định tuyến hoàn chỉnh mô tả thiết kế bên trong của mạng. Một bản tin được gán địa chỉ đến một mạng khác sẽ được chuyển tiếp sang hệ thống lõi. Những router ngoại (*exterior*) cũng không kém phần quan trọng. Router ngoại được chỉ định để trao đổi thông tin với những mạng khác. Do đó, lượng thông tin liên mạng router bên trong mạng đang xét được giảm đi vì chỉ có những router ngoại mới thực hiện sự trao đổi thông tin định tuyến ra khỏi phạm vi mạng đang xét.



Hình 7-5 Kiến trúc router trên internet

Mỗi loại router sử dụng một giao thức và thuật toán khác nhau để xây dựng bảng định tuyến. Chúng ta sẽ tìm hiểu kỹ hơn về những giao thức định tuyến này ở phần sau của chương. Trước hết, cần phân biệt những loại router sau:

- Router lõi (Core Router) – Router lõi lưu trữ thông tin đầy đủ về những router lõi khác. Về cơ bản, bảng định tuyến của nó là sơ đồ vị trí các hệ thống tự trị kết nối vào mạng lõi. Những router lõi không xử lý những thông tin chi tiết của các router bên trong hệ thống tự trị. Nó có thể sử dụng các giao thức định tuyến như Gateway-to-Gateway Protocol (GGP) hay gần đây là giao thức định tuyến SPREAD.
- Router ngoại (Exterior Router) – Router ngoại không phải là những router lõi thực hiện sự trao đổi thông tin định tuyến giữa các mạng tự trị. Nó duy trì những thông tin định tuyến của nó và những mạng tự trị lân cận nhưng không có một sơ đồ về một mạng liên kết hoàn chỉnh. Những router ngoại thường sử dụng giao thức định tuyến EGP (Exterior Gateway Protocol). Hiện nay, giao thức EGP nguyên bản đã lỗi thời,

nhưng những giao thức định tuyến mới được sử dụng trong các router ngoại vẫn thường dựa trên EGP. Một phiên bản giao thức EGP đang sử dụng hiện nay là BGP (Border Gateway Protocol). Một router ngoại cũng phải tham gia vào hệ thống tự trị của nó như một router nội thông thường.

- Router nội (Interior Router) - Những router nằm bên trong hệ thống tự trị cùng chia sẻ thông tin định tuyến được gọi là những router nội. Những router này sử dụng một lớp các giao thức định tuyến gọi là IGP (Interior Gateway Protocol). Tiêu biểu trong các giao thức này là giao thức thông tin định tuyến - RIP (Routing Information Protocol) và giao thức ưu tiên đường đi ngắn nhất – OSPF (Open Shortest Path First). Chúng ta sẽ tìm hiểu kỹ hơn về RIP và OSPF ở phần sau của chương này. Những người quản lý mạng tự trị sẽ thiết kế cấu hình các router trong mạng và lựa chọn giao thức định tuyến thích hợp.

Một điều quan trọng cần chú ý là các router bên trong một trong các mạng tự trị cũng có thể có một cấu hình phân cấp. Một hệ thống tự trị lớn có thể bao gồm nhiều nhóm router nội và các router ngoại chuyển thông tin định tuyến giữa các nhóm nội này. Các nhà quản lý của hệ thống tự trị này có toàn quyền thiết kế một cấu hình router làm việc trên mạng này và tùy ý chọn các giao thức định tuyến.

Thông tin thêm

Ngày nay, hệ thống Internet trở nên rất phức tạp, ngay cả mạng lõi ARPAnet được mô tả ở trên cũng chỉ là một trường hợp rất đơn giản. Mạng lõi Internet được minh họa như một đám mây dày đặc với một mạng tự trị ở một đầu và một mạng tự trị khác mở nhánh sang các mạng khác.

7.4 Khảo sát các router nội

Như đã tìm hiểu ở phần trước, những router nội hoạt động trong một hệ thống tự trị. Một router nội phải biết được toàn bộ các phân đoạn mạng kết nối với các router khác trong cùng nhóm với nó, nhưng không cần phải biết các thông tin về mạng bên ngoài hệ thống tự trị. Rất nhiều giao thức định tuyến nội đang có sẵn. Một người quản trị mạng phải chọn một giao thức định tuyến nội thích hợp với điều kiện của mạng và tương thích với phần cứng mạng. Phần sau sẽ thảo luận kỹ hơn về những giao thức định tuyến nội quan trọng:

- Giao thức thông tin định tuyến (RIP)
- Giao thức ưu tiên đường đi ngắn nhất (OSPF)

RIP là một giao thức vector khoảng cách và OSPF là giao thức trạng thái liên kết. Mỗi giao thức còn có những vấn đề và chi tiết khác mà không được đề cập trong các phương pháp ở phần trước.

Thông tin thêm

Hầu hết các router hiện nay đều hỗ trợ nhiều giao thức định tuyến khác nhau.

7.4.1 Giao thức thông tin định tuyến (RIP)

RIP là một giao thức vector khoảng cách, xác định đường đi tối ưu dựa trên hop count (xem lại phần “Định tuyến vector khoảng cách” trong chương này). RIP được phát triển tại đại học California, Berkeley và lần đầu tiên được sử dụng phổ biến trong các phiên bản BSD của hệ điều hành Unix. Mặc dù dường như RIP đang lỗi thời nhưng nó vẫn là một giao thức định tuyến phổ biến và hiện vẫn đang được sử dụng rộng rãi. Sự xuất hiện của phiên bản RIP II đã khắc phục được một số hạn chế của RIP I. Nhiều router hiện nay có hỗ trợ cả RIP I và RIP II.

Thông tin thêm

RIP được thực thi trên hệ thống Unix và Linux dưới dạng daemon định tuyến. Như đã mô tả ở phần trước, RIP (giao thức vector khoảng cách) đòi hỏi các router phải lắng nghe những bản tin về đường đi và hop count từ các router khác. Những thành phần tham gia vào RIP được phân thành hai lớp: chủ động và bị động. Một nút RIP chủ động là một router tham gia vào tiến trình trao đổi dữ liệu vector khoảng cách. Thành phần RIP chủ động gửi bảng định tuyến của nó cho những router khác và lắng nghe những bản cập nhật từ những router đó. Một thành phần RIP bị động lắng nghe cập nhật của các router khác nhưng không phân tán bảng định tuyến của nó. Một nút RIP bị động tiêu biểu là một máy host thông thường (cần nhắc lại rằng host cũng cần có bảng định tuyến).

Khi tìm hiểu về định tuyến vector khoảng cách ở phần trước, bạn có lẽ tự hỏi những gì sẽ xảy ra khi hop count nhận được có độ lớn bằng với giá trị hop count đã tồn tại trong bảng định tuyến. Trong trường hợp của RIP, nếu hai đường đi khác nhau đến cùng một đích có cùng giá trị hop count thì đường đi đã có sẵn trong bảng định tuyến sẽ được tiếp tục sử dụng. Điều này tránh được những dao động về đường đi không cần thiết có thể phát sinh khi một router thay đổi liên tục một mục trong bảng định tuyến có liên quan đến hop count.

Một router sử dụng RIP sẽ phát tán bản tin cập nhật theo chu kỳ 30 giây, đồng thời nó cũng yêu cầu bản tin cập nhật ngay sau đó. Giống như những giao thức vector khoảng cách khác, RIP hoạt động có hiệu quả trong những mạng ổn định. Nếu số lượng router tăng, nhiều vấn đề sẽ bắt đầu phát sinh do độ hội tụ chậm của các bảng định tuyến. Vì lý do này, RIP đã đưa ra một giới hạn về số lượng hop tối đa tính từ router đầu tiên đến router đích. Giá trị hop count giới hạn này là 15. Ngưỡng này đã giới hạn kích thước của một nhóm router, nhưng nếu các router được sắp xếp phân cấp thì nó có thể mở rộng kích thước của nhóm lớn hơn 15 hop.

Mặc dù phương pháp vector khoảng cách không đặc biệt quan tâm đến tốc độ đường truyền và loại mạng vật lý, RIP vẫn cho phép người quản trị mạng lựa chọn đường đi bằng cách nhập các giá trị hop count lớn cho những lộ trình không hiệu quả.

Giao thức RIP thuần túy được thay thế dần dần bởi những giao thức định tuyến mới hơn, chẳng hạn như OSPF, mà chúng ta sẽ tìm hiểu trong phần kế tiếp.

7.4.2 Giao thức ưu tiên đường đi ngắn nhất (OSPF)

OSPF là giao thức định tuyến nội được phát triển gần đây và dần dần thay thế RIP trong rất nhiều mạng. Đó là một giao thức định tuyến trạng thái liên kết, xuất hiện lần đầu tiên vào năm 1989 trong RFC 1131 và liên tục được cập nhật. RFC 2328 mô tả OSPF phiên bản 2 và một vài RFC sau đó đã thêm vào những phần thay đổi và bổ sung của OSPF.

Mỗi router trong một nhóm router OSPF được gán một số nhận dạng router. Số nhận dạng này là địa chỉ IP cao nhất kết hợp với router (nếu router sử dụng giao tiếp loopback, số nhận dạng router sẽ là địa chỉ loopback cao nhất. Xem **chương 3, “Lớp Internet”** để hiểu thêm về địa chỉ loopback).

Như chúng ta đã tìm hiểu trong phần đầu của chương, các router trạng thái liên kết xây dựng một sơ đồ địa hình mạng bên trong. Những router khác sử dụng số nhận dạng router để nhận biết một router nằm trong mạng. Mỗi router đều biểu diễn mạng theo dạng hình cây mà bản thân nó là gốc. Cây mạng này được gọi là cây đường dẫn ngắn nhất (SPT – Shortest Path Tree). Những đường dẫn qua mạng cũng chính là những đường nhánh qua SPT. Router tính toán chi phí cho mỗi lộ trình. Chi phí này có thể gồm các thông số số lượng các router và các tham số khác, chẳng hạn như tốc độ và độ tin cậy của liên kết.

7.5 Định tuyến không phân lớp (classless)

Như chúng ta đã khảo sát ở **chương 3** và **chương 4**, hệ thống định tuyến TCP/IP được thiết kế xung quanh khái niệm địa chỉ mạng, phụ thuộc vào các lớp địa chỉ (A,B hoặc C) của IP. Và ở **chương 4**, hệ thống lớp địa chỉ có một số hạn chế, đôi khi lại là một phương pháp thiếu hiệu quả nếu chỉ định một khối địa chỉ cho một nhà cung cấp đơn lẻ. Định tuyến miền Internet không phân lớp (Classless Internet Domain Routing - CIDR) đã cung cấp một phương pháp khác để gán địa chỉ và xác định các đường đi (xem mục “Định tuyến miền Internet không phân lớp” ở **chương 4**). Hệ thống CIDR xác định một host thông qua một cặp địa chỉ/mặt nạ, ví dụ: 204.21.128.0/17. Số mặt nạ tượng trưng cho số lượng các bit địa chỉ liên kết với địa chỉ mạng. Hệ thống CIDR đưa ra phương pháp định tuyến hiệu quả hơn nếu giao thức định tuyến có hỗ trợ nó. CIDR giảm được những thông tin cần thiết phải truyền giữa các router vì nó cho phép router

thay thế nhiều lớp mạng bằng một thành phần duy nhất. Những giao thức gần đây, chẳng hạn như OSPF hoặc BGP4 có hỗ trợ cách gán địa chỉ không phân lớp, nhưng những giao thức khác, như RIP, lại không hỗ trợ CIDR.

Tóm tắt

Chương này giúp chúng ta tiếp cận gần hơn với định tuyến. Chúng ta đã khảo sát về các phương pháp định tuyến: vector khoảng cách và trạng thái liên kết. Chúng ta cũng đã tìm hiểu về chuyển tiếp IP, các router lõi, router ngoại, router nội. Cuối chương, chúng ta cũng đã khảo sát về hai giao thức định tuyến nội: RIP và OSPF.

CHƯƠNG

8

PHÂN GIẢI TÊN

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Phân giải tên host**
- **DNS**
- **NetBIOS**

Trong **chương 1, "TCP/IP làm việc như thế nào?"**, chúng ta biết về phân giải tên, một kỹ thuật hiệu quả để liên kết một tên miền dạng chuỗi ký tự với địa chỉ IP 32 bit. Tiến trình phân giải tên nhận vào một tên của máy tính và phân giải tên thành địa chỉ tương ứng. Trong chương này chúng ta sẽ nghiên cứu về tên host, tên miền và tên miền đầy đủ (FQDNs - fully qualified domain names). Chúng ta cũng nghiên cứu về một hệ thống phân giải tên NetBIOS sử dụng rộng rãi trong mạng Microsoft.

Kết thúc chương này bạn sẽ có thể :

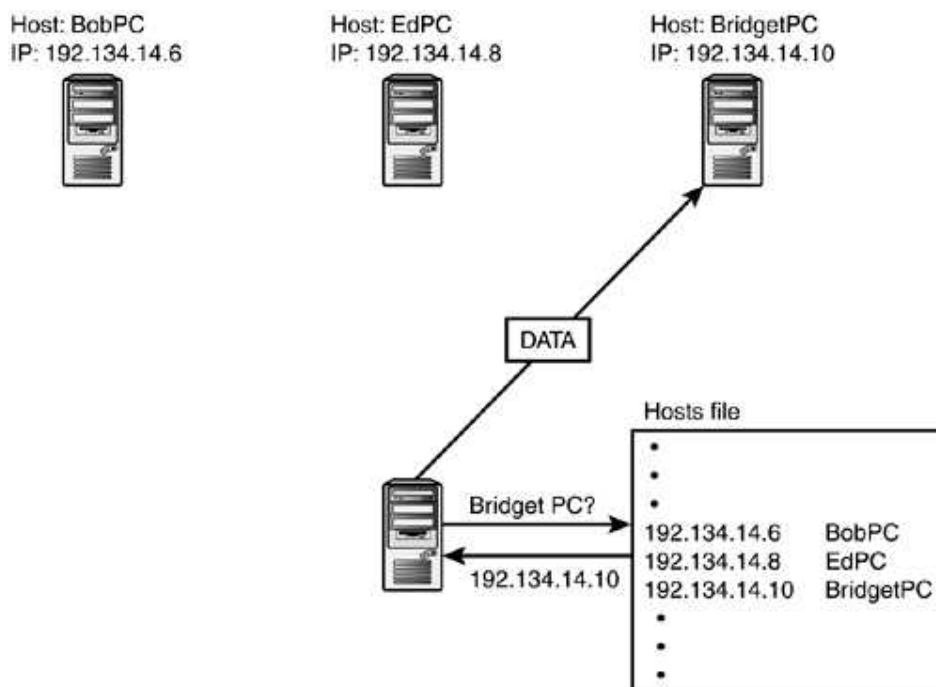
- Giải thích cơ chế làm việc của phân giải tên
- Giải thích sự khác nhau giữa tên host (hostname), tên miền (domain name) và tên miền đầy đủ (FQDN)
- Mô tả phân giải tên host
- Mô tả phân giải tên DNS
- Mô tả phân giải tên NetBIOS.

8.1 Thế nào là phân giải tên?

Vào thời điểm phát triển ban đầu của TCP/IP, người dùng nhận thấy nhớ địa chỉ IP của mỗi máy tính trên mạng là một việc khó khăn. Người dùng tại các trung tâm nghiên cứu sẽ không đủ thời gian để nhớ máy A tại tòa nhà số 6 có địa chỉ 100.12.8.14 hoặc 100.12.8.18. Các chuyên gia máy tính đã nghiên cứu một cách mới để thực hiện nhiệm vụ đó một cách tự động. Mỗi lần người lập trình ghi ra một tên host thì máy tính sẽ quan tâm tới việc chuyển trực tiếp tên đó ra địa chỉ IP tương ứng. Hệ thống tên host đã được phát triển sớm với TCP/IP. Trong hệ thống này, mỗi máy được ấn định một tên gồm một chuỗi ký tự gọi là tên host (hostname). Nếu hệ điều hành muốn biết một tên tương ứng với địa chỉ IP nào, hệ điều hành truy vấn một tập tin host (xem **hình 8.1**). Tập tin host bao gồm một danh sách các mối kết hợp giữa tên host-với-địa chỉ IP. Nếu một tên mà nằm trong danh sách các tên host thì máy tính sẽ đọc ra được địa chỉ IP tương ứng với tên đó. Máy tính thay thế mỗi tên host trong câu lệnh bằng địa chỉ IP tương ứng và thực thi câu lệnh.

Hệ thống tập tin host làm việc tốt trong các mạng cục bộ nhỏ. Nhưng hệ thống này làm việc không hiệu quả trong các mạng lớn. Các kết hợp host-và-địa chỉ chỉ lưu trong một tập tin đơn lẻ và hiệu quả tìm kiếm sẽ giảm khi tập tin được mở rộng. Trong mạng dùng ARP có một tập tin gọi là hosts.txt lưu trữ một danh sách liên kết tên-và-địa chỉ, và người quản trị cục bộ phải liên tục cập nhật tập tin hosts.txt theo trạng thái mạng hiện hành. Hơn nữa, không gian tên host bản chất là phẳng. Mọi nút đều ngang nhau, và hệ thống phân giải tên không tận dụng được tính hiệu quả của cấu trúc phân cấp của không gian địa chỉ IP. Ngay cả khi các kỹ sư của mạng ARP có thể giải quyết được các vấn đề này, thì hệ thống tập tin host vẫn không làm việc được với mạng lớn hơn với hàng triệu nút giống như Internet. Các kỹ sư đã biết đến sự cần thiết của hệ thống phân giải tên phân cấp.

- Trách nhiệm phân giải tên được phân bổ cho một nhóm các server phân giải tên đặt biệt. Mỗi server này lưu trữ một bảng các kết hợp tên_với_địa chỉ. Những máy tính khác trên mạng có thể truy vấn các server này về thông tin ánh xạ giữa tên-và-địa chỉ IP.
- Cấp quyền phân giải tên cục bộ cho các nhà quản trị cục bộ. Nói cách khác, thay vì duy trì một bản sao tập trung của tất cả cặp tên-và-địa chỉ, chúng ta cho nhà quản trị mạng A phân giải tên cho mạng A, và nhà quản trị mạng B cấu hình phân giải tên cho mạng B. Theo cách đó, các cá nhân chịu trách nhiệm về bất cứ sự thay đổi nào trên một mạng, cũng có trách nhiệm đảm bảo những thay đổi này được phản ánh trong cơ sở hạ tầng phân giải tên.



Hình 8-1 Phân giải tên host

Những yếu tố trên đã dẫn đến hệ thống tên miền (DNS). DNS là phương pháp phân giải tên sử dụng trên Internet và là nguồn gốc của các tên Internet phổ biến như `www.unixreview.com` và `www.slashdot.org`. Như chúng ta sẽ thấy trong chương tiếp theo, DNS chia không gian tên thành từng cấp gọi là miền. Tên miền có thể bao gồm tên host và nó được gọi là tên miền đầy đủ (FQDN). Ví dụ: Một máy tính với tên `maybe` trong miền `whitehouse.gov` sẽ có FQDN là `maybe.whitehouse.gov`.

Chương này mô tả phân giải tên host và phân giải tên DNS. Chúng ta cũng sẽ biết về NetBIOS, một trong những hệ thống phân giải tên miền phổ biến sử dụng trên mạng Microsoft.

8.2 Phân giải tên miền sử dụng các tập tin host

Như chúng ta đã biết trong phần trước, một tập tin host là một tập tin chứa một bảng gồm các kết hợp tên host và địa chỉ IP. Phân giải Tên host đã được phát triển trước DNS nhưng cách phân giải này hiện nay vẫn được sử dụng trong một số mạng, đặc biệt là các mạng nhỏ không cần thêm các chi phí cho quá trình điều hành DNS. Một vài mạng sử dụng tập tin host cho việc tìm kiếm cục bộ và DNS cho truy vấn từ xa, như truy cập Internet. Cấu hình phân giải tên host cho mạng nhỏ thường rất đơn giản. Hệ điều hành hỗ trợ TCP/IP nhận ra tập tin host và sử dụng nó cho việc phân giải mà không cần sự can thiệp hoặc là rất ít từ người dùng. Chi tiết của quá trình cấu hình rất khác nhau, phụ thuộc vào hoàn cảnh.

Các bước cấu hình DHCP tổng quát như sau:

1. Ấn định một địa chỉ IP và một tên host cho mỗi máy tính.
2. Tạo một tập tin host ánh xạ địa chỉ IP và tên host của mỗi máy tính. Tập tin host thường có tên là `hosts`, kết hợp thêm phần mở rộng, nó có tên là `hosts.txt`.
3. Đặt tập tin host ở một vị trí xác định trên mỗi máy tính. Vị trí khác nhau tùy thuộc vào hệ điều hành.

Tập tin host bao gồm nhiều mục, mỗi mục tương ứng cho mỗi host mà máy tính cần liên lạc, nó cho phép ta nhập vào địa chỉ IP tương ứng với tên host, FQDN, hoặc là những biệt danh khác. Thông thường tập tin host luôn chứa một địa chỉ loopback, `127.0.0.1`. Địa chỉ loopback được sử dụng cho việc chuẩn đoán TCP/IP và đại diện cho chính máy đó. Phương pháp này quản lý IP tĩnh, nghĩa là sau khi nhập vào thì địa chỉ phải được thay đổi bằng tay.

Sau đây là một ví dụ cho biết tập tin host sẽ như thế nào (địa chỉ IP của hệ thống phía bên trái, theo sau bởi tên host và một chú thích bổ sung về mục này):

127.0.0.1	localhost	#this machine
198.1.14.2	bobscomputer	#Bob's workstation
198.1.14.128	r4downtown	#gateway

Khi một ứng dụng của máy tính cần phân giải tên sang địa chỉ IP, hệ thống đầu tiên so sánh tên riêng của nó với tên yêu cầu. Nếu không trùng, hệ thống sẽ xem trong tập tin host có tên của máy tính trong danh sách hay không. Nếu có, địa chỉ IP được trả về cho máy tính cục bộ, và ARP được thực hiện để xác định địa chỉ phần cứng tương ứng của địa chỉ IP này. Và sau đó liên lạc giữa hai máy tính được thiết lập.

Nếu bạn đang sử dụng tập tin host cho việc phân giải tên, cứ mỗi thay đổi trong mạng thì bạn phải chỉnh sửa tập tin host cho mỗi máy tính. Bạn có thể sử dụng một số chương trình chỉnh sửa văn bản để chỉnh sửa tập tin host. Trên hệ thống Unix, sử dụng Vi, Pico, hoặc là Emacs; trên Windows, sử dụng Notepad; trên DOS, sử dụng Edit. Một vài hệ thống cũng cung cấp công cụ cấu hình TCP/IP và tương tác với giao diện người dùng để chỉnh sửa tập tin host.

Khi bạn tạo và chỉnh sửa tập tin host, phải đảm bảo các điều sau:

- Địa chỉ IP phải đặt bên trái và cách biệt với tên host ít nhất một hoặc nhiều khoảng trắng.
- Các tên phải cách biệt ít nhất một khoảng trắng.

- Những tên bổ sung đặt trên một dòng đơn sẽ là bí danh cho tên đầu tiên.
- Tập tin được duyệt (bởi máy tính) từ trên xuống dưới. Địa chỉ IP đầu tiên so trùng sẽ được sử dụng. Khi tìm thấy mẫu tin trùng, quá trình tìm kiếm dừng lại.
- Bởi vì cơ chế tìm từ trên xuống dưới, nên bạn nên đặt những tên sử dụng thường xuyên phía trên danh sách. Nó có thể giúp bạn tăng tốc độ xử lý.
- Các chú giải được đặt ở bên phải của ký tự #.
- Ghi nhớ rằng tập tin host là tĩnh; bạn phải thay đổi bằng tay mỗi khi địa chỉ IP thay đổi.
- Cấu hình không đúng tập tin host (lỗi chính tả trong tập tin host) có thể gây ra vấn đề cho việc phân giải địa chỉ. Nếu một địa chỉ sai được trả về cho ứng dụng qua tiến trình phân giải địa chỉ, ứng dụng sẽ không hoạt động đúng chức năng.
- Mặc dù FQDNs được cho phép làm việc với tập tin host, việc sử dụng chúng trong tập tin host có thể gây ra vấn đề khó khăn cho nhà quản trị trong việc chuẩn đoán lỗi. Người quản trị cục bộ điều khiển tập tin host thì không cần điều khiển việc phân phối địa chỉ IP và tên host cho các mạng ở xa. Do đó, nếu một server ở xa được gán một địa chỉ IP mới, và FQDN trong tập tin host cục bộ không được cập nhật, thì tập tin host vẫn tiếp tục chỉ tới địa chỉ IP cũ.

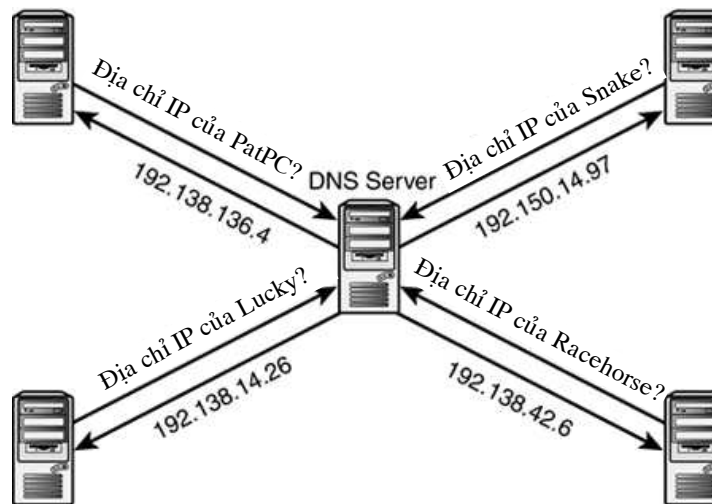
Một tập tin host là một phương thức rất hiệu quả và là cách đơn giản để quản lý việc phân giải tên trong mạng TCP/IP nhỏ. Còn một vài chi tiết khác tùy thuộc vào hệ điều hành. Bạn có thể tra cứu tài liệu của nhà sản xuất để biết thêm chi tiết.

8.3 Phân giải tên DNS

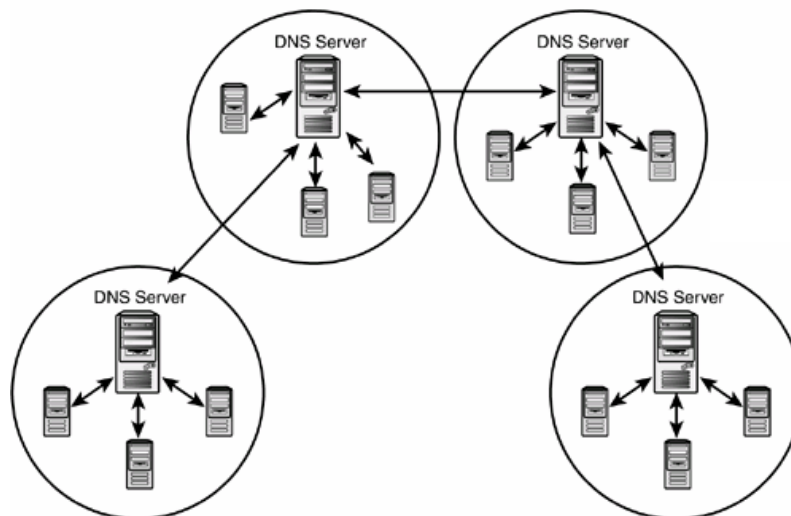
Người thiết kế DNS mục đích muốn tránh việc cập nhật tập tin phân giải cho mỗi máy tính. Thay vào đó DNS đặt dữ liệu phân giải trên một hoặc vài server đặc biệt. Máy chủ DNS cung cấp việc phân giải tên miền cho mạng (xem **hình 8.2**). Nếu một máy tính trên mạng bắt gặp một tên mà nó không phân giải được, nó sẽ gửi truy vấn đến server để tìm địa chỉ IP tương ứng với tên đó. Nếu máy chủ DNS có địa chỉ, nó gửi địa chỉ trở lại cho máy tính yêu cầu. Máy tính sau đó sử dụng địa chỉ IP thay cho tên host và thực thi câu lệnh. Khi có một sự thay đổi xảy ra cho mạng (ví dụ như có một máy tính mới hoặc có một sự thay đổi tên), người quản trị mạng chỉ việc thay đổi cấu hình DNS (trên máy chủ DNS). Thông tin mới sẽ có giá trị cho bất kỳ máy tính nào khởi tạo truy vấn máy chủ DNS. Máy chủ DNS có thể tối ưu hóa việc tìm kiếm và có thể hỗ trợ cơ sở dữ liệu lớn hơn so với việc tìm trên tập tin host công kênh.

Một máy chủ DNS thể hiện trên **hình 8.2** cung cấp nhiều thuận lợi hơn cho việc phân giải tên so với phương pháp dùng tập tin host. Người ta sử dụng một chuẩn cấu hình DNS đơn cho một mạng cục bộ và mang đến nhiều hiệu quả hơn trong việc sử dụng tài nguyên mạng. Tuy nhiên, cấu hình thể hiện trên **hình 8.2** vẫn chưa giải quyết được vấn đề quản lý phân quyền trong một cấu trúc hạ tầng mạng lớn. Giống như trong trường hợp dùng tập tin host, cấu hình trong **hình 8.2** sẽ không phù hợp cho một

mạng khổng lồ như Internet. Name server trong **hình 8.2** không thể tổ chức hiệu quả với cơ sở dữ liệu gồm một mục cho mỗi host trên Internet, vì cơ sở dữ liệu này sẽ rất lớn, không thể làm được. Bất cứ ai cấu hình cho các server sẽ phải biết mỗi thay đổi trên Internet liên quan đến bất kỳ host nào ở bất kỳ nơi đâu trên thế giới. Một giải pháp tốt hơn, là chúng ta để cho mỗi văn phòng hoặc cơ quan cấu hình một name server riêng cho mình hoạt động như trong **hình 8.2** và sau đó cung cấp phương tiện cho các server nói chuyện với nhau (xem **hình 8.3**).



Hình 8-2 Một máy chủ DNS cung cấp dịch vụ phân giải tên miền cho mạng



Hình 8-3 Trong các mạng lớn hơn, máy chủ DNS liên lạc với nhau để cung cấp dịch vụ phân giải địa chỉ

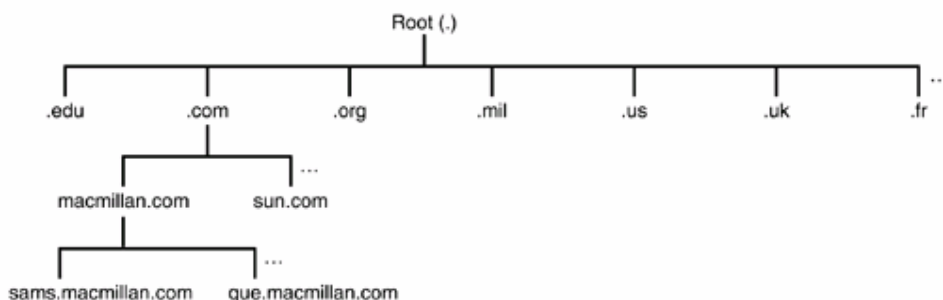
Trong sơ đồ này, khi một DNS client gửi một yêu cầu phân giải tới name server, name server sẽ làm các công việc sau :

- Nếu name server tìm thấy yêu cầu địa chỉ trong cơ sở dữ liệu riêng của nó, nó sẽ ngay lập tức gửi yêu cầu tới client.
- Nếu name server không tìm thấy địa chỉ trong các bản ghi của riêng nó, nó sẽ truy vấn các name server khác để tìm địa chỉ và gửi địa chỉ cho client.

Bạn có thể thắc mắc tên server đầu tiên nào mà name server liên hệ khi bắt đầu tiến trình truy vấn để tìm ra địa chỉ.

Thật ra, tiến trình này kết hợp chặt chẽ với việc thiết kế không gian tên miền DNS. Ghi nhớ rằng DNS không làm việc trực tiếp với tên host. Như đã mô tả trong các chương trước, DNS làm việc với tên miền đầy đủ (FQDNs). Một FQDN bao gồm một tên host và một tên xác định miền.

Không gian tên DNS là một sự sắp xếp đa cấp các miền (**Hình 8.4**). Một miền là một tập hợp các máy tính thuộc cùng một tổ chức có tên giống nhau ở phần chung của không gian tên (có nghĩa là cùng mang chung tên miền). Tại đỉnh cao nhất của cây DNS là một nút gọi là gốc (*root*). Gốc đôi khi thể hiện dưới dạng dấu chấm (.), mặc dù ký tự thật sự của gốc là ký tự null. Cấp dưới gần nhất của gốc là một nhóm các tên miền được gọi là miền cấp cao (TLD – Top Level Domain). **Hình 8.4** thể hiện một số TLD cho không gian tên nổi tiếng nhất trên thế giới là Internet. Mức trên cùng tên miền bao gồm các tên miền quen thuộc như .com, .org, và .edu, cũng như tên miền các quốc gia, như là .us (Mỹ), .uk (Anh), .fr (Pháp), và .jp (Nhật Bản).



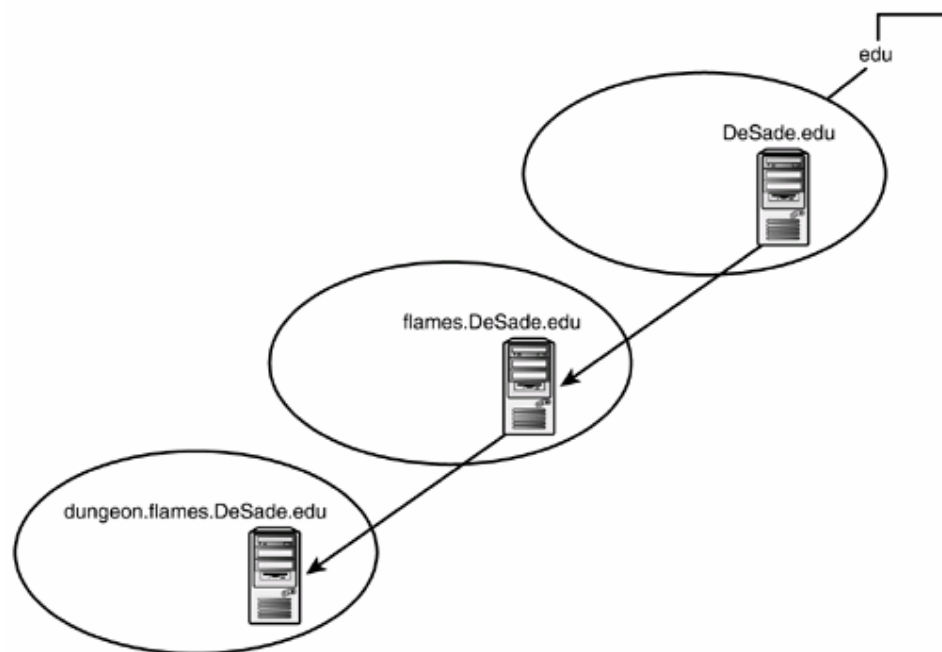
Hình 8-4 Không gian tên miền DNS

Thông tin thêm

Nhóm các tên miền cấp cao được công bố gần đây gồm .biz, .coop, .info, và .museum.

Dưới mỗi tên miền cấp trên cùng là một cấp khác của miền (trong trường hợp của Internet) được quản lý bởi các công ty, cơ quan, hoặc tổ chức. Tên các cơ quan nằm phía trước các tên miền trên cùng. Ví dụ, trong **hình 8.5**, đại học DeSade có tên

miền DeSade.edu. Tổ chức có thẩm quyền với tên miền có thể tạo một hoặc nhiều tên miền nhỏ phụ thêm. Tại mỗi mức, tên của miền cục bộ là phần trước của tên miền cha. Ví dụ, văn phòng lo việc giải trí của DeSade có tên miền flames.DeSade.edu (chỉ ra trong **hình 8.5**) và phòng tiếp khách (thường được sinh viên gọi với tên "dungeon") có tên miền dungeon.flames.DeSade.edu. Trong mọi trường hợp thì hệ thống DNS hỗ trợ tới 127 mức tên miền, nhưng một tên miền quá dài sẽ không thuận tiện khi sử dụng.



Hình 8-5 Sơ đồ gần đúng của DNS

Thông tin thêm

Nếu như bạn làm việc nhiều với Internet, bạn có thể thấy các tên miền mở rộng nhiều cấp (như trong **hình 8.5**) thì thường không phổ biến. Các Website, đặc biệt đông nhất là.com, thường được tham khảo qua tên miền của tổ chức với www làm phần mở đầu: www.ibm.com. Tuy nhiên, lưu ý rằng một Website có thể được phục vụ bởi một server đơn hoặc một nhóm các server tại một vị trí. Các tên miền đa cấp có thể gặp thường xuyên trong trường hợp truy cập tài nguyên trên các máy của một tổ chức lớn trải rộng trên nhiều vị trí. TLD trong khu vực công cộng (.gov) có khuynh hướng tạo ra các tên có nhiều cấp.

Tên miền thể hiện một chuỗi các miền đi từ đỉnh của cây xuống. Name server trong miền sams.com sẽ lưu giữ các thông tin phân giải tên cho mọi host nằm trong sams.com. Với thẩm quyền với tên miền đó, server có thể ủy quyền việc phân giải địa chỉ tên miền con cho một server khác. Ví dụ, server có thẩm quyền với tên miền sams.com có thể ủy quyền tên miền con edit.sams.com cho một name server khác. Các mẫu tin phân giải tên cho tên miền con edit.sams.com có thể nằm trên name server được ủy quyền trên tên miền con đó. Thẩm quyền cho việc phân giải địa chỉ thực hiện

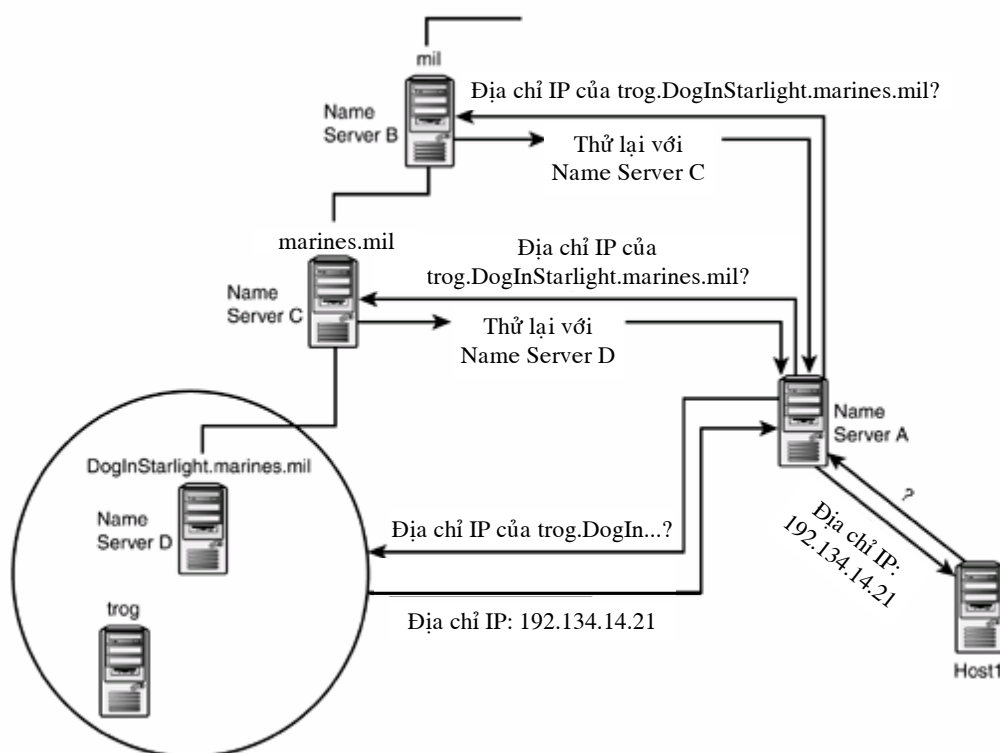
thông qua cây, và nhà quản trị sở hữu một tên miền có thể điều khiển ánh xạ tên-với-địa chỉ của host trong miền đó.

Khi một host trên mạng cần địa chỉ IP, nó thường gửi truy vấn đệ quy tới server gần nhất. Truy vấn này có nội dung, "hãy chỉ cho tôi địa chỉ IP liên kết với tên này hoặc chỉ cho tôi nơi tìm ra chúng." Nếu name server không thể tìm ra địa chỉ trong số các mẫu tin riêng của nó, nó sẽ khởi tạo tiến trình truy vấn một name server khác để tìm ra địa chỉ. Tiến trình này thể hiện như trong **hình 8.6**. Name server A sử dụng một quá trình truy vấn lặp đi lặp lại như vậy để tìm ra địa chỉ. Truy vấn lặp lại gửi cho name server kế tiếp "hoặc là gửi cho tôi địa chỉ IP hoặc là cho tôi một manh mối để tôi có thể tìm ra nó."

Tiến trình phân giải địa chỉ DNS được diễn ra như sau (chỉ ra trong **hình 8.6**):

Host1 gửi một truy vấn tới name server A hỏi về địa chỉ IP liên kết với tên miền trog.DogInStarlight.marines.mil.

Name server A kiểm tra trong các mẫu tin của nó để xem nó có thể đáp ứng yêu cầu không. Nếu server A có địa chỉ, nó sẽ trả lại địa chỉ cho Host1.



Hình 8-6 Tiến trình phân giải địa chỉ

Nếu name server A không có địa chỉ, nó sẽ bắt đầu tiến trình tìm địa chỉ. Name server A lặp lại yêu cầu phân giải địa chỉ cho server B, name server trên cùng phân giải cho miền .mil, để hỏi xem địa chỉ liên kết với tên trog.DogInStarlight.marines.mil.

Name server B sẽ không đáp ứng được yêu cầu đó, nhưng nó có thể gửi cho name server A địa chỉ của server C, name server của marines.mil.

Name server A gửi lại yêu cầu phân giải địa chỉ tới server C, name server C sẽ không đáp ứng được yêu cầu đó, nhưng nó có thể gửi cho name server A địa chỉ của server D, name server của DogInStarlight.marines.com.

Name server A lại lặp lại yêu cầu này tới server D, name server D tìm địa chỉ tương ứng với host trog.DogInStarlight.marines.mil và gửi địa chỉ này cho server A. Server A sau đó gửi địa chỉ này cho Host1.

Host1 sẽ thực hiện quá trình kết nối với host trog.DogInStarlight.marines.mil.

Quá trình này xảy ra hàng ngàn lần(nếu không nói là hàng triệu lần) mỗi ngày trên Internet. Biểu đồ đơn giản này không thể hiện hết được các tính chất phức tạp khác của mạng hiện đại, bao gồm địa chỉ cache, DHCP, và DNS động. Tuy nhiên, chức năng của liên kết các mạng TCP/IP phụ thuộc vào hình thức phân giải địa chỉ DNS này.

Một điều quan trọng cần ghi nhớ là mạng không yêu cầu phải có mỗi name server riêng cho mỗi node trên cây tên miền. Một name server có thể xử lý nhiều miền và ngược lại nhiều server phục vụ cho một miền.

8.4 Đăng ký một miền

Internet chỉ là một ví dụ của không gian tên miền DNS. Bạn không cần phải kết nối vào Internet để sử dụng DNS. Nếu bạn không kết nối vào Internet, bạn không phải lo lắng về việc đăng ký tên miền riêng của bạn. Tuy nhiên, các công ty muốn sử dụng một tên miền riêng (như là BuddysCars.com) phải đăng ký tên đó với nơi có thẩm quyền cấp tên miền. ICANN là cơ quan quản lý việc đăng ký tên miền, nhưng nó ủy quyền cho các nhóm khác quản lý đăng ký các TLD cụ thể khác. Dịch vụ đăng ký tên miền phục vụ cho TLD được liệt kê dưới đây.

.com, .org, và .net - Một số công ty có thẩm quyền cung cấp dịch vụ phân giải tên miền cho các tên miền cấp cao phổ biến như .com, .org, và .net. Xem website ICANN tại <http://www.icann.com>.

.gov - Tên miền **.gov** dành riêng cho cơ quan chính phủ liên bang Mỹ. Các tên của bang và chính quyền địa phương nằm trong một nhánh của TLD U.S. Dịch vụ đăng ký cho tên miền .gov nằm tại <http://www.registration.fed.gov>.

.mil - Tên miền .mil trực thuộc quân đội Mỹ. Dịch vụ đăng ký tại <http://www.nic.mil>.

8.5 Quản lý DNS

Khi thực hiện DNS trong mạng, bạn nên chọn ít nhất một server có trách nhiệm lưu trữ tên miền của bạn. Nó được coi như là server tên miền chính của bạn, nó sẽ lấy thông tin về các vùng mà nó quản lý từ các tập tin cục bộ. Bất cứ thay đổi nào cho tên miền của bạn đều thực hiện trên server này.

Rất nhiều mạng cũng có một hoặc nhiều server dự phòng, hoặc là name server thứ cấp. Nếu bất cứ chuyện gì xảy ra cho server chính, máy này sẽ tiếp tục thực hiện công việc thay cho server chính. Server thứ cấp lấy thông tin từ tập tin zone của server chính. Khi sự trao đổi thông tin này thực hiện, nó được xem như một sự chuyển zone.

Loại server thứ ba được gọi là caching-only server (server chỉ đệm). Cache là một phần của bộ nhớ máy tính, lưu giữ các dữ liệu được yêu cầu truy cập thường xuyên. Với một caching-only server, nó đáp ứng các truy vấn từ client trên mạng cục bộ cho các yêu cầu phân giải tên. Nó truy vấn máy chủ DNS khác về tên miền và các máy tính cung cấp dịch vụ như Web và FTP. Khi nó nhận thông tin từ máy chủ DNS, nó lưu thông tin vào bộ nhớ cache của nó để có thể sử dụng lại trong trường hợp thông tin này được yêu cầu lần nữa.

Caching-only server được máy tính client trong mạng cục bộ sử dụng để phân giải tên. Những máy chủ DNS khác trên Internet sẽ không biết chúng và do đó sẽ không truy vấn chúng. Đây là cách để giảm tải cho các server. Việc duy trì một caching-only server không phức tạp trong trường hợp bạn có một site từ xa và máy tính client đã phân giải tên và không cần gì nhiều hơn nữa.

Cache được cấu hình trước với các địa chỉ IP của 9 máy chủ DNS mức gốc. Nếu máy tính truy cập Internet qua một router, nó sẽ sẵn sàng làm việc. Máy tính client có thể bao gồm địa chỉ IP của máy chủ DNS này trong danh sách thứ tự tìm kiếm của chúng, và máy chủ DNS sẽ bắt đầu đáp ứng yêu cầu bằng việc liên lạc với máy chủ DNS khác và tự động thêm các mẫu tin vào bộ nhớ cache của nó.

Thông tin thêm

DNS phải được thực hiện như là một dịch vụ hoặc một daemon chạy trên máy máy chủ DNS. Các Server Windows đã có sẵn dịch vụ DNS, nhưng một số các nhà quản trị mạng lại ưa thích sử dụng DNS của các công ty khác. Thế giới Unix có một số lựa chọn trong việc thực hiện DNS, nhưng lựa chọn phổ biến nhất là hệ thống tên miền Internet Berkeley (BIND).

8.5.1 Cấu hình máy chủ DNS

Một nhóm các host DNS trong cấu hình tập hợp các máy chủ DNS được gọi là **zone**. Trong một mạng đơn giản, một zone có thể là một miền DNS hoàn chỉnh. Lấy ví dụ, tên miền `punyisp.com` có thể được coi như một zone duy nhất để cấu hình DNS. Trong những mạng phức tạp, cấu hình DNS cho một miền con đôi khi được ủy quyền cho một zone khác phục vụ cho miền con đó. Ủy quyền zone cho phép các nhà quản trị mạng có sự hiểu biết trực tiếp hơn về một mạng con quản lý cấu hình DNS cho mạng con đó. Ví dụ, nhà quản trị DNS cho tên miền `cocacola.com` có thể ủy quyền cấu hình DNS của tên miền con `dallas.cocacola.com` cho một zone điều khiển bởi nhà quản trị DNS ở Dallas, người có thể quan sát chặt chẽ mọi host trong `dallas.cocacola.com`.

Bạn có thể hỏi sự khác biệt giữa zone và miền là gì? Một điều cần lưu ý là ngoài sự khác nhau khó thấy về ngữ nghĩa (một domain là một sự chia nhỏ không gian tên và một zone là một tập hợp các host). Các khái niệm zone và domain hoàn toàn không tương đương với nhau. Để đọc phần này cần ghi nhớ các điều sau:

- Các thành viên trong một miền con cũng là thành viên trong miền cha. Lấy ví dụ, host trong `dallas.cocacola.com` cũng nằm trong `cocacola.com`. Nhưng trái ngược lại, nếu một zone của `dallas.cocacola.com` được ủy quyền, một host trong `dallas.cocacola.com` thì không phải là thành phần của zone `cocacola.com`.
- Nếu một miền con không được ủy quyền một cách rõ ràng, nó không yêu cầu một zone phân biệt và đơn giản được gộp chung trong tập tin zone của miền cha.

Chi tiết của việc ủy quyền zone DNS phụ thuộc trên ứng dụng máy chủ DNS. Bây giờ cần nhớ rằng, zone thể hiện tập cấu hình của một nhóm các máy chủ DNS và host, và nhà quản trị DNS có thể ủy quyền các phần trong không gian tên miền cho các zone khác để quản trị được hiệu quả hơn.

8.5.2 Tập tin Zone

Như trong phần trước, zone DNS là một đơn vị quản trị đại diện cho một tập hợp các máy tính trong một phần không gian tên miền DNS. Cấu hình DNS của một zone lưu trữ trong một tập tin zone. Máy chủ DNS sẽ truy cập các thông tin trong tập tin zone để đáp ứng cho các truy vấn và đưa ra các yêu cầu. Một tập tin zone là một tập tin text với một cấu trúc chuẩn. Nội dung của tập tin zone bao gồm nhiều mẫu tin tài nguyên. Mỗi mẫu tin tài nguyên nằm trên một dòng cung cấp các thông tin hữu ích về cấu hình DNS. Một vài loại mẫu tin tài nguyên phổ biến:

soa - (Start of Authority). Mẫu tin SOA cho biết Name server có thẩm quyền đối với zone đó.

NS - (Name Server). Mẫu tin NS cho biết Name Server của zone. Một zone có thể có nhiều name server (và do đó có nhiều bản ghi NS) nhưng chỉ có một mẫu tin SOA cho name server có thẩm quyền.

A - Mẫu tin A ánh xạ tên DNS với địa chỉ IP.

PTR - Mẫu tin PTR ánh xạ địa chỉ IP với tên DNS.

CNAME - CNAME là một tên ngắn gọn. Mẫu tin CNAME ánh xạ một bí danh với một tên host thực thể hiện bởi mẫu tin A .

Do đó, tập tin zone sẽ cho máy chủ DNS biết:

- Máy chủ DNS có thẩm quyền đối với Zone.
- Các máy chủ DNS (thẩm quyền và không thẩm quyền) trong zone
- Các ánh xạ tên DNS sang địa chỉ IP trong zone
- Bí danh (tên khác) của host trong zone

Các loại mẫu tin tài nguyên khác cung cấp thông tin về các chủ đề như mail servers (mẫu tin MX), ánh xạ IP sang tên DNS (mẫu tin PTR), và các dịch vụ nổi tiếng (mẫu tin WKS). Một tập tin zone có dạng như sau:

```
@ IN SOA boris.cocacola.com. hostmaster.cocacola.com. (
    201.9      ; serial number incremented with each
                ; file update
    ;
    3600      ; refresh time (in seconds)
    1800      ; retry time (in seconds)
    4000000   ; expiration time (in weeks)
    3600)     ; minimum TTL
IN NS horace.cocacola.com.
IN NS boris.cocacola.com.
;
; Host to IP address mappings
;
localhost IN A 127.0.0.1
chuck     IN A 181.21.23.4
amy       IN A 181.21.23.5
darrah    IN A 181.21.23.6
joe       IN A 181.21.23.7
bill      IN A 181.21.23.8
;
; Aliases
;
ap        IN CNAME amy
db        IN CNAME darrah
bu        IN CNAME bill
```

Ghi chú rằng mẫu tin SOA bao gồm một vài tham số điều khiển tiến trình cập nhật dữ liệu zone từ server chính sang các server thứ cấp. Ngoài số serial cho biết phiên bản của chính tập tin zone, còn có một số tham số thể hiện một số thông tin sau :

Thời gian làm tươi (Refresh time) – Là khoảng thời gian định kỳ máy chủ DNS thứ cấp sẽ truy vấn server chính để cập nhật thông tin.

Thời gian thử lại (Retry time) – Là khoảng thời gian đợi để thử lại nếu quá trình cập nhật không thành công.

Thời gian hết hạn (Expiration time) – Giới hạn thời gian mà server thứ cấp còn lưu một mẫu tin mà không có cập nhật lại.

Thời gian sống tối thiểu (Minimum TTL) – Thời gian sống mặc định của các mẫu tin zone.

Phần bên phải ngoài cùng của mẫu tin SOA là địa chỉ email của người chịu trách nhiệm cho zone đó. Thay thế dấu chấm đầu tiên bằng ký hiệu @ để hình thành một địa chỉ email.

Ví dụ trên là một trường hợp đơn giản nhất của tập tin zone. Những tập tin lớn hơn có thể bao gồm hàng trăm mẫu tin địa chỉ và những mẫu tin ít phổ biến khác thể hiện những khía cạnh khác của cấu hình. Tên của tập tin zone và trong một vài định dạng có thể khác nhau tùy thuộc vào phần mềm máy chủ DNS. Ví dụ trên là dạng BIND (Berkeley Internet Name Domain) thông dụng, một dạng name server phổ biến nhất trên Internet.

Một điều cần nhớ rằng, việc thực hành cấu hình các dịch vụ bằng cách thao tác các tập tin văn bản đang giảm dần đi. Rất nhiều chương trình ứng dụng máy chủ DNS cung cấp giao diện người dùng che dấu đi các thông tin chi tiết về tập tin zone.

DNS động (mô tả trong chương này) còn cung cấp một cách khác mà không cần tới các chi tiết về cấu hình.

8.5.3 Tập tin Zone truy vấn ngược

Một loại tập tin zone khác rất cần thiết cho việc phân giải DNS là tập tin truy vấn ngược. Tập tin này được sử dụng khi client cung cấp địa chỉ IP và yêu cầu tên host tương ứng. Trong địa chỉ IP, phần bên trái nhất là phần chung và phần bên phải nhất là phần riêng. Trong khi đó trong tên miền thì ngược lại: phần bên trái nhất là phần riêng và phần bên phải như là `com` hoặc `edu`, là phần chung. Để tạo tập tin zone ngược bạn phải đảo ngược địa chỉ mạng để phần chung và phần riêng có cùng thứ tự như trong tên miền. Lấy ví dụ, zone cho mạng `192.59.66.0` sẽ có tên `66.59.192.in-addr.arpa`.

Mọi mẫu tin trong tập tin này luôn có host ID theo sau bởi `.in-addr.arpa`. Phần `in-addr` ám chỉ địa chỉ đảo ngược, và phần `arpa` xác định một mức domain trên cùng khác và là ARPAnet mạng tiền thân của Internet.

Thông tin thêm

Các mạng lớp A và B có tên zone đảo ngược ngắn hơn, do chúng chứa ít bit địa chỉ mạng hơn. Ví dụ, trong mạng lớp A `43.0.0.0`, có zone đảo ngược sẽ là `43.in-addr.arpa`. Trong mạng lớp B `172.58.0.0`, có zone đảo ngược là `58.172.in-addr.arpa`.

8.5.4 Những tiện ích cho DNS

Bạn có thể sử dụng bất cứ tiện ích mạng nào hỗ trợ phân giải tên để kiểm tra xem mạng của bạn đang phân giải tên đúng hay không. Một trình duyệt Web, một FTP client, một Telnet client, hoặc lệnh Ping có thể cho bạn biết hoạt động của quá trình phân giải địa chỉ. Nếu bạn có thể kết nối tới một tài nguyên sử dụng địa chỉ IP của nó nhưng không thể kết nối với tài nguyên đó khi sử dụng hostname hoặc FQDN, thì đó là lỗi do việc phân giải địa chỉ.

Nếu máy tính của bạn sử dụng một tập tin hosts và cũng sử dụng DNS, hãy nhớ vô hiệu hoặc tạm thời đổi tên tập tin host tạm thời khi bạn kiểm thử DNS. Ngược lại rất khó để xác định một tên được phân giải bởi tập tin hosts hoặc do DNS. Phần sau sẽ mô tả cách sử dụng lệnh Ping để kiểm tra DNS. Phần tiếp theo sẽ mô tả tiện ích NSLookup, dùng cho việc cấu hình DNS và sửa lỗi.

8.5.5 Kiểm tra phân giải địa chỉ với Ping

Một tiện ích đơn giản và hữu ích là lệnh Ping dùng để kiểm tra cấu hình DNS. Ping gửi một tín hiệu sang một máy tính khác và đợi trả lời. Nếu trả lời đến, bạn sẽ biết hai máy tính đã kết nối. Nếu bạn biết địa chỉ IP của máy ở xa, bạn có thể ping máy tính bằng địa chỉ IP:

```
ping 198.1.14.2
```

Nếu lệnh thành công, bạn sẽ biết máy tính của bạn có kết nối với máy từ xa bằng địa chỉ IP như trên không.

Bây giờ cố gắng thử ping máy ở xa bằng tên DNS:

```
ping williepc.remotenet.com
```

Nếu bạn ping máy tính ở xa bằng địa chỉ IP nhưng không thể ping bằng tên DNS, bộ phận phân giải địa chỉ có thể làm việc không đúng. Nếu bạn có thể ping bằng tên DNS, thì bạn có thể an tâm về bộ phận giải tên đang làm việc tốt.

8.5.6 Kiểm tra phân giải địa chỉ với NSLookup

Tiện ích NSLookup cho phép bạn có thể truy vấn các máy chủ DNS và xem thông tin về các mẫu tin tài nguyên của nó, và nó hữu ích trong việc sửa lỗi DNS. Công cụ NSLookup hoạt động ở hai chế độ:

- **Chế độ xử lý theo lô** - Trong chế độ này, bạn khởi động NSLookup và nhập vào các tham số. NSLookup thực hiện yêu cầu theo tham số nhập vào, hiển thị kết quả và sau đó dừng lại.
- **Chế độ tương tác** - Trong chế độ tương tác, bạn khởi động NSLookup mà không cần nhập vào các tham số. NSLookup sau đó sẽ yêu cầu bạn nhập các tham số. Khi bạn nhập tham số, NSLookup thực hiện yêu cầu, hiển thị kết quả và sau đó trở về chế độ dòng lệnh, và đợi bạn nhập các tham số kế tiếp. Hầu hết các nhà quản trị sử dụng chế độ tương tác bởi vì nó thuận tiện cho việc thực hiện một chuỗi các hoạt động.

NSLookup có một số lựa chọn mở rộng. Một vài lựa chọn cơ bản liệt kê dưới đây sẽ cho bạn biết sơ về cách làm việc của NSLookup.

Để chạy NSLookup trong chế độ tương tác, gõ vào `nslookup` trong chế độ dòng lệnh.

Như trên **hình 8.7**, NSLookup đáp ứng với tên và địa chỉ IP của máy chủ DNS mà NSLookup đang hiện tại sử dụng, lấy ví dụ

```
Default Server: dnsserver.Lastingimpressions.com
Address: 192.59.66.200
>
```

Ký tự (>) là dấu nhắc của NSLookup.

NSLookup có khoảng 15 thông số mà bạn có thể thay đổi để ảnh hưởng tới cách làm việc của NSLookup. Một vài thông số thường được sử dụng được liệt kê dưới đây:

`?`; và `help`— Những lệnh này sử dụng để xem danh sách các lệnh của NSLookup

`server`— Lệnh này xác định máy chủ DNS để truy vấn.

`ls`— Lệnh này dùng để liệt kê danh sách các tên trong miền (thể hiện ở phần giữa của **hình 8.7**).

`ls -a`—Lệnh này liệt kê danh sách các tên hợp pháp và bí danh trong một miền, trong **hình 8.7**.

`ls -d`—Lệnh này liệt kê danh sách các mẫu tin tài nguyên (thể hiện ở gần phần gần cuối của **hình 8.7**).

`set all`—Lệnh này hiển thị các giá trị thông số hiện tại.



```
Command Prompt - nslookup
> webserver.lastingimpressions.com
Server: dnsserver.LastingImpressions.com
Address: 192.59.66.200

webserver.lastingimpressions.com      internet address = 192.59.66.225
> dnsserver.lastingimpressions.com
Server: dnsserver.LastingImpressions.com
Address: 192.59.66.200

dnsserver.lastingimpressions.com      internet address = 192.59.66.200
> ls lastingimpressions.com
[dnsserver.LastingImpressions.com]
lastingimpressions.com.      NS      server = dnsserver.lastingimpressions
dnsserver                    A      192.59.66.200
webserver                    A      192.59.66.225
> ls -a lastingimpressions.com
[dnsserver.LastingImpressions.com]
www                          CNAME  webserver.lastingimpressions.com
> ls -d lastingimpressions.com
[dnsserver.LastingImpressions.com]
graphics/11fig07.gif
> ls -a lastingimpressions.com
[dnsserver.LastingImpressions.com]
lastingimpressions.com.      SOA    dnsserver.lastingimpressions.com BobW
.com. (3 3600 600 86400 3600)
lastingimpressions.com.      NS     dnsserver.lastingimpressions.com
dnsserver                    A      192.59.66.200
webserver                    A      192.59.66.225
```

Hình 8-7 Đáp ứng NSLookup

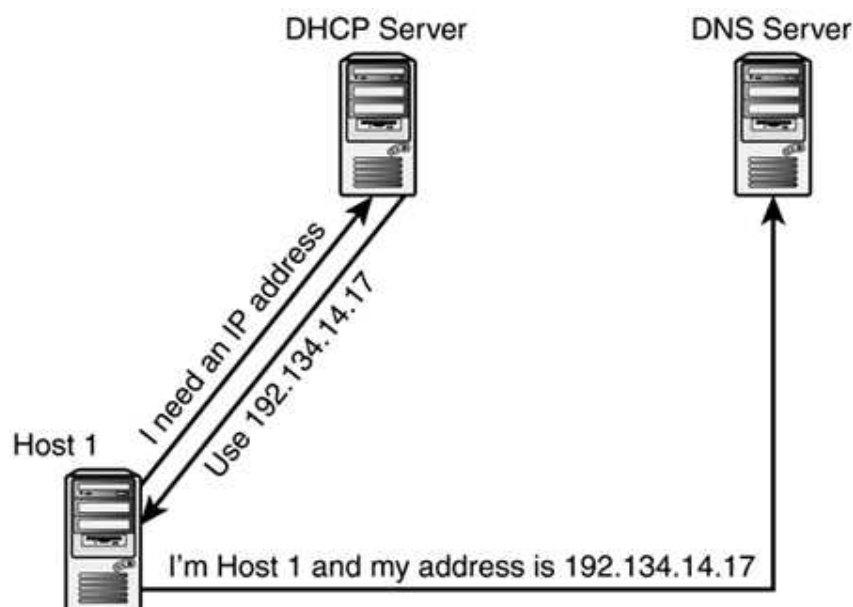
NSLookup không giới hạn trong việc xem thông tin từ máy chủ DNS của bạn; bạn có thể xem thông tin từ bất cứ server nào. Nếu bạn là một nhà cung cấp dịch vụ Internet(ISP), bạn nên dành các địa chỉ IP cho ít nhất hai máy chủ DNS.

NSLookup có thể sử dụng địa chỉ IP khác hoặc là tên miền khác. Bạn có thể chuyển tới máy chủ DNS khác bằng lệnh `server` theo sau bởi địa chỉ IP hoặc FQDN. Lấy ví dụ, để kết nối NSLookup vào server gốc E, bạn có thể nhập `server 192.203.230.10`. Sau đó gần như bạn có thể nhập bất cứ tên miền nào, ví dụ như là `sampublishing.com`, và xem địa chỉ IP được đăng ký cho tên miền đó. Nhưng chắc rằng hầu hết các máy chủ DNS thương mại và các server gốc sẽ từ chối lệnh `ls`, bởi vì chúng có thể tạo ra lưu lượng khổng lồ hoặc rò rỉ thông tin an toàn.

8.6 DNS động

DNS, như đã được mô tả phía trước, nó được thiết kế cho trường hợp có sự kết hợp cố định (hoặc bán cố định) giữa tên host và địa chỉ IP. Trong các mạng ngày nay (bạn sẽ xem trong các chương kế tiếp), địa chỉ IP thường được thiết kế động. Hay nói cách

khác, một địa chỉ IP mới được ấn định cho một máy tính qua giao thức cấu hình host động DHCP (Dynamic Host Configuration Protocol). Điều đó có nghĩa là nếu như máy tính đăng ký với DNS và có thể truy cập bằng tên host của nó thì máy chủ DNS phải bằng cách nào đó biết được địa chỉ mà máy tính đang sử dụng. Sự sử dụng rộng rãi cấu hình địa chỉ IP động đã bắt buộc các nhà sản xuất DNS phải đáp ứng theo yêu cầu. Một vài sự thực hiện IP (gồm BIND) đã cho phép cập nhật động các mẫu tin DNS. Trong kịch bản điển hình (**hình 8.8**), DHCP server phân phát một địa chỉ IP cho mỗi client và sau đó client cập nhật địa chỉ mới của nó cho máy chủ DNS. Chúng ta sẽ tìm hiểu thêm về DHCP trong **chương 9, "Giao thức cấu hình host động - DHCP"**



Hình 8-8 Cập nhật DNS động

8.7 Phân giải tên NetBIOS

NetBIOS là một API và là hệ thống phân giải tên do IBM phát triển đầu tiên và bây giờ đã trở lên phổ biến trong các mạng Microsoft Windows. Tên NetBIOS là tên của máy tính mà bạn ấn định cho máy tính Windows của bạn. Tên máy tính NetBIOS được sử dụng để nhận diện các máy tính trong Explorer và My Computer. NetBIOS đã được phát triển cho các mạng không sử dụng TCP/IP. Hệ thống tên NetBIOS thật ra là một bộ phận không cần thiết trong các mạng TCP/IP bởi vì tên NetBIOS có vai trò cũng giống như host name. Microsoft đang cố gắng làm giảm vai trò NetBIOS trong Windows 2000/XP và có lẽ sẽ tiếp tục phát triển phân giải tên miền TCP/IP trong tương lai. Tại thời điểm viết tài liệu này có lẽ cũng là lúc người ta cần nhắc lại hệ thống phân giải NetBIOS. Mặc dù vậy, ảnh hưởng của NetBIOS đối với hệ thống máy tính vẫn còn lớn đến nỗi các cuộc hội thảo về vấn đề phân giải tên sẽ không trọn vẹn nếu không có một sự lưu tâm nào đó đến NetBIOS.

Bởi vì NetBIOS hoạt động thông qua broadcast, người dùng trong các mạng nhỏ không phải quan tâm đến vấn đề cấu hình phân giải NetBIOS. Trong các mạng lớn, NetBIOS phức tạp hơn. Những mạng lớn sử dụng NetBIOS name servers được gọi là WINS server dùng cho việc phân giải tên NetBIOS. Bạn cũng có thể cấu hình một tập tin LM Hosts tĩnh (tương tự với tập tin hosts trong DNS) cho việc phân giải. Những phần tiếp theo sẽ tìm hiểu kỹ hơn quá trình phân giải địa chỉ NetBIOS.

8.8 Các phương pháp phân giải địa chỉ NetBIOS

Trong mạng TCP/IP, mục đích sau cùng của phân giải tên NetBIOS là cung cấp địa chỉ IP cho các tên NetBIOS. Tên NetBIOS là một tên đơn có thể dài tới 15 ký tự, như là Workstation1, HRServer, và CorpServer. NetBIOS không cho phép trùng tên trong một mạng.

Thông tin thêm

Về mặt kỹ thuật thì tên NetBIOS có 16 ký tự. Tuy nhiên, ký tự thứ 16 được dùng bởi ứng dụng nằm bên dưới, và thường thì người dùng không thể cấu hình trực tiếp. Những ký tự này sẽ nói đến trong phần sau của chương này. Tên NetBIOS, giống như tên host, ở dạng cấu trúc phẳng, bởi vì không có sự phân cấp hoặc khả năng mở rộng tên. Trong các phần tiếp theo, bạn sẽ xem xét một số cách để phân giải tên NetBIOS với địa chỉ IP tương ứng của chúng:

- Dựa trên Broadcast
 - Dựa trên LM Hosts
 - Dựa trên WINS
-

8.8.1 Phương pháp phân giải dựa trên Broadcast

Một trong những cách phân giải được thực hiện qua broadcast. Broadcast xảy ra khi một máy tính thông tin tới mọi máy tính khác trong phân đoạn mạng của nó, khi nó cần biết địa chỉ của một máy tính cụ thể. Mọi máy trong phân đoạn sẽ lắng nghe broadcast, nhưng chỉ một máy xác định trong lệnh broadcast là phản hồi lại yêu cầu này. Phương pháp phân giải tên này gọi là phân giải B-Node, nó làm việc tốt trong môi trường mạng LAN, nhưng không làm việc được trong các mạng mở rộng ra khỏi mạng LAN, bởi vì router sẽ chặn lại các broadcast này.

Thông tin thêm

Broadcast có thể gây ra lưu lượng trên mạng lớn, do đó nó có thể gây ra tắc nghẽn trên mạng. Routers có thể giới hạn sự tắc nghẽn đó bằng cách không chuyển tiếp các broadcast tới phần còn lại của mạng. Tiến trình phân giải tên bằng broadcast thì đơn giản và không yêu cầu cấu hình thêm nào để có thể sử dụng. Chỉ đơn giản cài đặt một card mạng và phần mềm mạng TCP/IP trên hệ điều hành Window để cho phép sử dụng broadcast xác định các máy khác thông qua việc sử dụng phân giải NetBIOS.

8.8.2 Phân giải tên dùng các tập tin LMHosts

Hệ thống Windows có thể phân giải tên NetBIOS sang địa chỉ IP sử dụng tập tin LMHosts. Tập tin LMHost tương tự với tập tin hosts (mô tả trong phần trên của chương này). Một tập tin LMHosts liên kết tên NetBIOS với địa chỉ IP. Địa chỉ IP được liệt kê ở cột bên trái của tập tin, tương ứng với tên của máy tính ở phía phải cách nhau ít nhất một khoảng trắng; các chú thích có thể đặt trong tập tin bằng cách đặt chúng sau dấu #. LMHosts yêu cầu ánh xạ tĩnh địa chỉ IP với tên NetBIOS. Trên mỗi máy tính khác nhau có riêng một tập tin LMHosts. Bạn phải cấu hình bằng tay tập tin LMHosts này. Nếu một máy tính mới được thêm vào mạng, các máy tính khác sẽ không thể tìm ra nó thông qua tập tin LMHosts cho đến khi một mục cho máy tính đó được bổ sung bằng tay vào mỗi tập tin LMHosts.

Trên một mạng chỉ gồm một phân đoạn, một tập tin LMHosts thường không cần thiết, bởi vì máy tính trên mạng đó có thể phân giải tên NetBIOS thông qua broadcast. (Trong một số trường hợp, LMHosts có thể được sử dụng để làm tăng tính hiệu quả trong các hệ thống không broadcast.) Trên các mạng lớn bao gồm nhiều hơn một phân đoạn, broadcast không thể dùng để phân giải tên vượt qua phía bên kia của router. Trong trường hợp này, máy tính phải thực hiện chức năng phân giải tên NetBIOS sử dụng hoặc là LMHosts hoặc là WINS server (mô tả trong phần sau). Trong một vài trường hợp, LMHosts rất hữu ích để chỉ ra lối đi tới bộ điều khiển domain nằm trên phân đoạn mạng khác nhau. (Bộ điều khiển tên miền là cần thiết cho việc chứng thực trong môi trường Windows hoạt động dựa trên domain.)

Trong hệ thống Windows, tập tin LMHosts được bao gồm trong Microsoft TCP/IP. Microsoft cũng bao gồm các tập tin LMHosts mẫu có tên `LMHosts.sam`. Bạn có thể chỉnh sửa tập tin `LMHosts.sam`, nhưng phải bỏ phần mở rộng `.sam` để tập tin có thể thực hiện được.

Thông tin thêm

LM trong LMHosts xuất phát từ Microsoft's LAN Manager, một sản phẩm kèm theo Windows NT.

Sau đây là một ví dụ cơ bản của tập tin LMHosts:

```
192.59.66.205  marketserv  #tập tin server for marketing department
192.59.66.206  marketapp   #application server for marketing
192.59.66.207  bobscomputer #bob's workstation
```

Những tên NetBIOS thường xuyên được phân giải sẽ lưu trong cache. Cache là một phần của bộ nhớ máy tính lưu trữ những dữ liệu thường xuyên được yêu cầu và

sẵn sàng để truy cập. Bất cứ khi nào một người dùng cố gắng định vị một máy tính cụ thể, hệ thống luôn luôn tra cứu trong cache trước khi tìm kiếm trong tập tin LMHosts. Nếu không tìm thấy một sự so trùng nào, các mẫu tin trong LMHosts có thể được duyệt để đáp ứng yêu cầu. Tiến trình này có thể tốn nhiều thời gian khi có nhiều mẫu tin trong LMHosts, do đó để tăng tốc xử lý bạn nên cho các mẫu tin thường xuyên sử dụng nạp vào bộ nhớ cache trước bằng cách thêm vào từ khóa `#PRE` (xem *hình 8.9*). Tập tin LMHosts được duyệt qua toàn bộ các dòng này một lần khi mạng khởi động, do đó để hiệu quả thì các dòng có từ khóa `#PRE` thường được đặt vào phần cuối của LMHosts. Các dòng này chỉ cần đọc duy nhất một lần nên việc đặt nó ở phần cuối của tập tin sẽ làm giảm đi khả năng duyệt qua chúng nhiều lần.

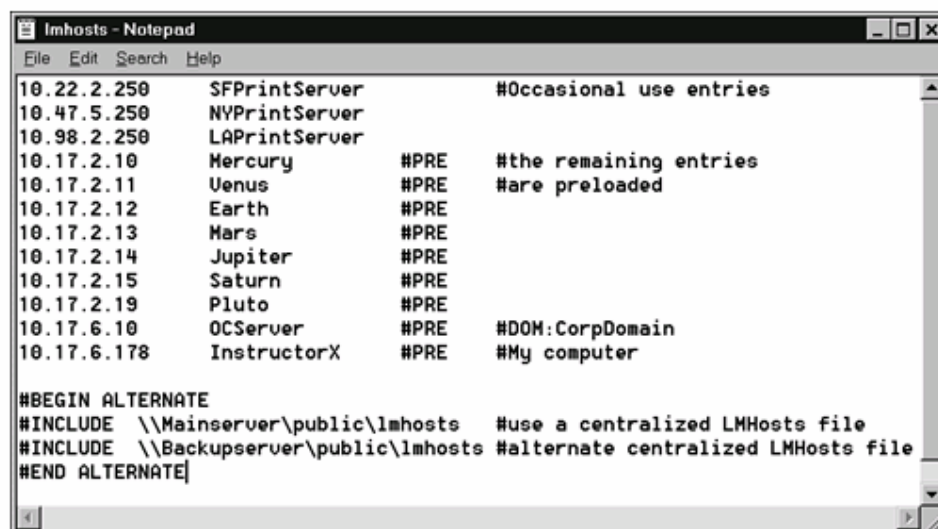
Thông tin thêm

Bạn có thể sử dụng tiện ích NBTStat để xem và thao tác trên cache của NetBIOS. Để xem nội dung trong cache, gõ `nbtstat -c` tại chế độ dòng lệnh.

Việc duy trì các tập tin tĩnh như host và LMHosts thì rất khó bởi các tập tin này nằm trong các máy tính độc lập và không có sự tập trung. Tập tin LMHosts giải quyết vấn đề trên bằng cách sử dụng từ khóa `#INCLUDE`, theo sau bởi đường dẫn đến các tập tin LMHosts trên các máy khác. Với từ khóa này, tập tin LMHosts cục bộ có thể thêm vào vị trí của tập tin LMHosts trên server được sử dụng bởi các máy cục bộ. Điều này cho phép các chỉnh sửa được thực hiện trên tập tin LMHosts của server, với các thay đổi từ phía người dùng.

Nếu có nhiều mục `#INCLUDE`, chúng cần đặt giữa hai từ khóa `#BEGIN ALTERNATE` và `#END ALTERNATE`, thể hiện trong *hình 8.9*.

Như đã đề cập trong phần trước, LMHosts có thể sử dụng để xác định vị trí bộ phận điều khiển miền trên phân đoạn khác của mạng. Từ khóa `#DOM` cho biết mẫu tin thể hiện bộ phận điều khiển tên miền.



```
lmhosts - Notepad
File Edit Search Help
10.22.2.250 SFPrintServer #Occasional use entries
10.47.5.250 NYPrintServer
10.98.2.250 LAPrintServer
10.17.2.10 Mercury #PRE #the remaining entries
10.17.2.11 Venus #PRE #are preloaded
10.17.2.12 Earth #PRE
10.17.2.13 Mars #PRE
10.17.2.14 Jupiter #PRE
10.17.2.15 Saturn #PRE
10.17.2.19 Pluto #PRE
10.17.6.10 OCServer #PRE #DOM:CorpDomain
10.17.6.178 InstructorX #PRE #My computer

#BEGIN ALTERNATE
#INCLUDE \\Mainserver\public\lmhosts #use a centralized LMHosts file
#INCLUDE \\Backupserver\public\lmhosts #alternate centralized LMHosts file
#END ALTERNATE
```

Hình 8-9 Nội dung của tập tin LMHosts

8.8.3 Phân giải tên: Dịch vụ phân giải tên Internet trên Windows (WINS)

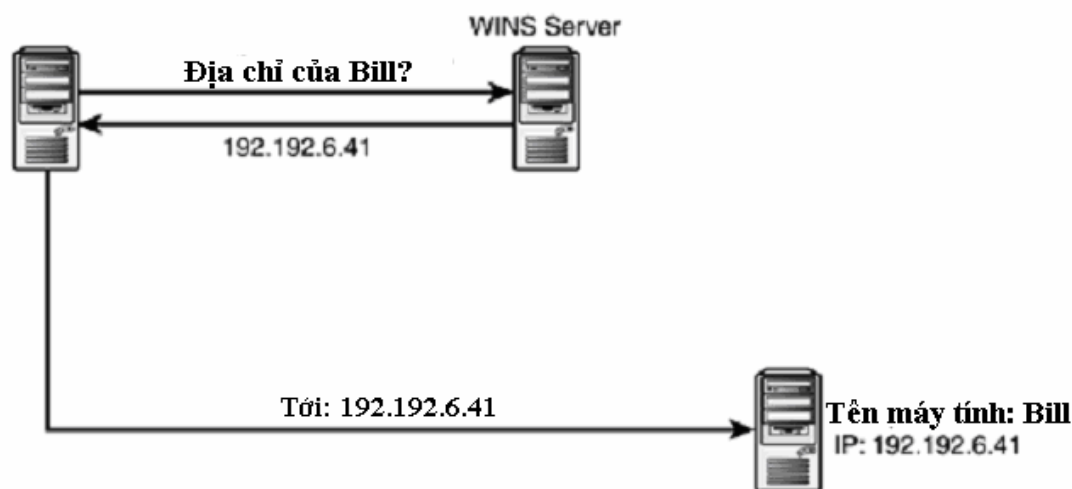
WINS được tạo ra nhằm giải quyết các thiếu sót trong LMHosts giống như DNS được tạo ra để khắc phục hạn chế của các tập tin hosts. Khi một client muốn có địa chỉ IP của một máy tính, nó truy vấn server WINS để lấy thông tin.

Thông tin thêm

WINS được Microsoft phát triển và thông thường được gọi là NBNS (NetBIOS Name Server). NetBIOS name server mô tả trong RFCs 1001 và 1002.

WINS duy trì một cơ sở dữ liệu về các tên NetBIOS được đăng ký cho nhiều loại đối tượng khác nhau, bao gồm người dùng, máy tính dịch vụ chạy trên máy tính đó và nhóm làm việc. Tuy nhiên, thay vì các mẫu tin trong cơ sở dữ liệu này có trong các tập tin văn bản được soạn thảo bằng tay, thì trong WINS giống như trong DNS, các máy tính client đăng ký động tên và địa chỉ IP của nó với server WINS khi nó khởi động.

WINS server nhận và đáp ứng lại các yêu cầu phân giải tên NetBIOS (xem **hình 8.10**). Nếu một WINS server trong **hình 8.10** trông có vẻ giống như máy chủ DNS trong **hình 8.2**, đó là bởi vì WINS server thực hiện phân giải tên NetBIOS giống như máy chủ DNS phân giải tên miền. Tuy nhiên, không gian tên miền phẳng NetBIOS không tiện lợi bằng kỹ thuật phân giải phân cấp trong DNS.



Hình 8-10 Phân giải tên NetBIOS-WINS

Thông tin thêm

Microsoft đã giới thiệu một hình thức tích hợp giữa DNS/WINS với Windows NT 4, mô hình này cung cấp việc phân giải tên miền DNS trong các mạng lớn kết hợp với phân giải NetBIOS tự động. Sự tích hợp hơn nữa giữa DNS với NetBIOS trong môi trường thư mục tích cực Windows 2000 làm cho tính chất này trở lên không cần thiết.

Để cấu hình máy tính Windows sử dụng WINS, bạn nhập vào địa chỉ IP của một (hoặc hai) WINS server trong thẻ WINS Address Property hoặc hộp thoại TCP/IP Properties. Sau khi hoàn tất và máy tính đã được khởi động lại, thì nó sẽ trở thành WINS client.

Khi một máy client WINS khởi động sau khi cấu hình sử dụng WINS, các tiến trình xảy ra tiếp theo như sau:

Khởi động dịch vụ - Khi máy tính khởi động lại, nhiều loại dịch vụ khác nhau được khởi động, một vài dịch vụ cần biết các máy tính khác.

Yêu cầu đăng ký - Để có thể biết các máy tính khác trên mạng, dịch vụ này phải tự đăng ký. Một WINS client đóng gói tên NetBIOS và địa chỉ máy tính trong yêu cầu đăng ký tên, và yêu cầu đăng ký được gửi cho server WINS. Ngay khi nhận được yêu cầu đăng ký, WINS kiểm tra trong cơ sở dữ liệu để xem tên này đã đăng ký hay chưa.

Nếu tên đó chưa có, WINS thêm một cặp tên NetBIOS và địa chỉ IP vào cơ sở dữ liệu và gửi lại một đáp ứng đăng ký xác nhận yêu cầu đã đăng ký thành công. Nếu tên NetBIOS yêu cầu đã tồn tại trong cơ sở dữ liệu của WINS, WINS kiểm tra máy tính đã đăng ký hiện hành bằng cách gửi một thông điệp cho địa chỉ IP đã đăng ký. Nếu máy tính được đăng ký hiện hành đáp ứng lại, thì nó sẽ gửi một bản tin không xác nhận NAK (Negative Acknowledgement) cho máy tính đang cố gắng đăng ký tên. Nếu

máy tính đăng ký hiện hành không đáp lại, WINS cho phép thực hiện đăng ký và ghi đè lên đăng ký trước.

Hợp đồng thuê— Giả sử máy tính thành công trong việc đăng ký tên NetBIOS và dịch vụ với WINS, những tên này được xem như đã được thuê. Thực ra, nó có nghĩa là máy tính được phép sử dụng tên NetBIOS trong một khoảng thời gian—thường là 6 ngày—. Client thông thường làm mới lại hợp đồng thuê trong khoảng thời gian bằng 50% tổng thời gian thuê, hoặc trong trường hợp này là 3 ngày.

Trong phần trước, chúng ta đã đề cập đến ký tự thứ 16 của tên NetBIOS không được cấu hình bởi người dùng. Trong quá trình đăng ký WINS, server WINS sẽ nối thêm ký tự thứ 16 vào tên, ký tự nào là dựa trên loại dịch vụ mà máy tính đang cố gắng đăng ký trước khi đặt nó vào cơ sở dữ liệu. Giữa các tên máy tính, tên nhóm máy tính, và tên các dịch vụ, thông thường mỗi máy tính có 5 đến 10 mẫu tin đăng ký trong cơ sở dữ liệu WINS.

Một ví dụ khác của tiến trình phân giải tên WINS, giả sử một người dùng trên một máy tính sử dụng một tiện ích, ví dụ như Network Neighborhood để kết nối với một máy tính khác trên mạng. Khi có một yêu cầu truy vấn tên, bao gồm cả tên NetBIOS mong muốn, yêu cầu được xây dựng bởi chương trình ứng dụng và được gửi cho server WINS. Khi WINS nhận được yêu cầu, nó truy vấn cơ sở dữ liệu để tìm đăng ký. Nếu tên yêu cầu tìm thấy, WINS trả về địa chỉ IP tương ứng. Sau khi máy tính client có địa chỉ IP của máy yêu cầu, client bây giờ có thể kết nối trực tiếp. Một tính chất tốt của WINS là nó làm việc với cả hai mạng cục bộ và máy ở xa và có thể tích hợp với DNS.

8.9 Kiểm tra phân giải tên NetBIOS

Bạn có thể kiểm tra phân giải tên NetBIOS bằng cách dựa trên các tiện ích sử dụng NetBIOS. Một trong những cách là kiểm tra bằng lệnh Net view, nó cho phép bạn xem tên các điểm dùng chung trên server. (Nhớ rằng điểm dùng chung là thư mục nơi máy tính client có thể kết nối với máy tính khác để xem hoặc trao đổi tập tin.) Để thực hiện kiểm tra này, chọn máy tính có một hoặc nhiều điểm chia sẻ. Tại chế độ dòng lệnh, gõ

```
net view // tên máy tính
```

Với tên máy tính là tên của máy tính bạn chọn. Nếu `net view` có khả năng phân giải tên máy tính sang địa chỉ IP, bạn sẽ thấy tên các điểm dùng chung liệt kê trong lệnh đầu tiên và đáp ứng. Bạn cũng có thể sử dụng lệnh Ping để kiểm tra phân giải tên NetBIOS. Trong hầu hết các hệ thống Windows nếu phân giải tên NetBIOS làm việc tốt, bạn có thể Ping máy tính bằng tên NetBIOS. Ví dụ, nếu máy tính có tên là Shirley, bạn có thể sử dụng lệnh sau

```
ping Shirley
```

và nhận được đáp ứng.

8.10 Những dịch vụ phân giải tên khác

DNS và NetBIOS là những dịch vụ tên phổ biến trên mạng TCP/IP, nhưng chúng không phải là phương pháp duy nhất. Dịch vụ thông tin mạng(Network Information Service _NIS) là dịch vụ thông tin phát triển bởi Sun Microsystems cung cấp dịch vụ phân giải host-sang-IP. NIS phổ biến trên mạng Solaris(và các mạng khác trên nền tảng Unix) nhưng gần đây đang giảm sự ảnh hưởng do Sun ưa chuộng DNS hơn.

Tóm tắt

Phân giải tên cho phép sử dụng các tên dễ nhớ để đặt cho các máy tính thay cho địa chỉ IP. Chương này mô tả phân giải tên host thông qua DNS. Bạn cũng học về hệ thống phân giải tên NetBIOS sử dụng trong mạng Microsoft.

CHƯƠNG

GIAO THỨC CẤU HÌNH HOST ĐỘNG

9

DHCP

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Phân phối địa chỉ động**
- **DHCP**
- **Cấu hình DHCP**

Giao thức cấu hình host động (DHCP) cho phép máy tính nhận được cấu hình TCP/IP một cách tự động. Một DHCP server có thể cấu hình một DHCP client với địa chỉ IP address và subnet mask. DHCP client cũng có thể nhận những cấu hình khác từ DHCP, như là địa chỉ IP hoặc là gateway mặc định, máy chủ DNS, và WINS server. Trong chương này bạn sẽ học thế nào là DHCP, cơ chế làm việc của DHCP, tại sao nó quan trọng, và trong trường hợp nào nó hữu ích nhất.

Kết thúc chương này bạn sẽ có thể :

- Mô tả DHCP và những tiện ích nó mang lại
- Mô tả tiến trình liên quan đến hợp đồng DHCP client và địa chỉ IP
- Giải thích phạm vi của DHCP
- Mô tả tiến trình cấu hình DHCP server.

9.1 Trường hợp server cung cấp địa chỉ IP cho server

Mỗi máy tính như ta đã nghiên cứu trong các chương trước, phải có một địa chỉ IP để hoạt động trên mạng TCP/IP. Hệ thống địa chỉ IP đầu tiên được thiết kế cho điều kiện rất hợp lý là mỗi máy tính được cấu hình trước một địa chỉ IP. Điều kiện này được gọi là định vị IP tĩnh. Mỗi máy tính sẽ biết địa chỉ IP của nó ngay khi khởi động và có thể sử dụng mạng ngay tức khắc. Địa chỉ IP tĩnh làm việc tốt trong các mạng nhỏ và ít thay đổi, nhưng trong các mạng lớn hơn dễ có tình trạng thay đổi và cấu hình lại các thành phần trong hệ thống (như khi một máy tính mới gắn vào và ra khỏi mạng), thì địa chỉ IP tĩnh có một vài hạn chế.

Các thiếu sót chính của địa chỉ IP tĩnh:

- Thêm cấu hình - Mỗi client phải được cấu hình độc lập. Một thay đổi trong không gian địa chỉ hoặc một tham số khác nào đó (như là địa chỉ máy chủ DNS) cũng đưa đến việc client phải thay đổi lại cấu hình.
- Thêm địa chỉ - Mỗi máy tính sử dụng một địa chỉ IP ngay cả khi nó không có trên mạng.
- Giảm tính linh hoạt - Một máy tính phải cấu hình lại bằng tay khi nó được gắn vào một mạng con khác.

Để khắc phục các hạn chế này, người ta đưa ra một hệ thống đánh địa chỉ IP khác sử dụng giao thức DHCP để cấp phát địa chỉ IP theo yêu cầu. DHCP được phát triển trên một giao thức có trước là BOOTP, nó được sử dụng chủ yếu cho các máy tính khởi động không cần đĩa. (Các máy tính này nhận được hệ điều hành từ mạng khi khởi động.) DHCP đã trở nên ngày càng phổ biến trong những năm gần đây bởi vì nó giảm được số lượng địa chỉ IP cần cung cấp cho một mạng và sự phát triển của các mạng lớn và động.

9.2 Thế nào là DHCP?

DHCP là một giao thức được sử dụng để phân phối động các tham số cấu hình TCP/IP cho các máy tính. DHCP là một tiêu chuẩn được mô tả trong RFC 1531. Những RFCs khác—1534, 1541, 2131, và 2132—nhằm cung cấp cho các nhà sản xuất những sự thực hiện DHCP một cách đặt trung và nổi bật. Một DHCP server có thể cho client DHCP một số thiết lập TCP/IP, như là địa chỉ IP, subnet mask, và máy chủ DNS.

Bởi vì DHCP server thực hiện phân phối địa chỉ IP, chỉ có DHCP server mới được cấu hình địa chỉ IP. Tham số duy nhất mà bạn cần cấu hình cho client là thông số để client nhận được thông tin địa chỉ IP từ server. Phần cấu hình còn lại được thực hiện ở phía server. Nếu có sự thay đổi cấu hình TCP/IP nào đó trong mạng, người

quản trị mạng chỉ cần cập nhật lại DHCP server, mà không phải cập nhật lại các client bằng tay.

Hơn nữa, mỗi client sẽ nhận một hợp đồng thuê địa chỉ trong thời gian hạn định. Nếu client không còn sử dụng địa chỉ khi hợp đồng thuê hết hạn, địa chỉ đó có thể cấp phát cho các client khác. Điều này cho phép số lượng địa chỉ IP cần cho một mạng có thể nhỏ hơn số lượng máy có trong mạng.

DHCP đặc biệt quan trọng trong hoàn cảnh ngày nay, nhiều nhân viên mạng máy tính xách tay di chuyển giữa các văn phòng của một công ty lớn. Nếu một máy tính xách tay được cấu hình một địa chỉ IP tĩnh thì nó phải cấu hình lại mỗi lần nhân viên di chuyển và cắm máy vào mạng khác. Nếu máy tính được cấu hình để nhận được địa chỉ IP thông qua DHCP, máy tính xách tay sẽ tự động nhận toàn bộ cấu hình TCP/IP mỗi lần người dùng kết nối với mạng có một DHCP server.

9.3 Cơ chế làm việc của DHCP

Khi một client DHCP khởi động, phần mềm TCP/IP được nạp vào bộ nhớ và bắt đầu hoạt động. Tuy nhiên, bởi vì TCP/IP vẫn chưa có địa chỉ IP, nên nó chưa có khả năng nhận và gửi các gói. TCP/IP chỉ có thể truyền và lắng nghe broadcast. Khả năng có thể liên lạc bằng broadcast là nền tảng cho DHCP làm việc. Tiến trình hợp đồng địa chỉ IP từ DHCP server có thể liệt kê trong bốn bước sau đây:

1. **DHCPDISCOVER**—DHCP client khởi tạo tiến trình bằng cách quảng bá một gói tới cổng UDP 68 (sử dụng cho máy chủ BOOTP và DHCP). Gói đầu tiên này được gọi là bản tin DHCP Discover, nó sẽ yêu cầu bất cứ DHCP server nào nhận được gói thực hiện việc cấu hình. Gói DHCP discover gồm rất nhiều trường, nhưng một vùng quan trọng nhất chứa địa chỉ vật lý của DHCP client.
2. **DHCPOFFER**— Một DHCP server được cấu hình cung cấp hợp đồng địa chỉ cho mạng mà client cư trú sẽ đáp ứng lại một gói tên là DHCP offer và gửi nó dưới dạng quảng bá tới máy đưa ra DHCP discover. Thông điệp quảng bá này được gửi tới cổng UDP 67 và bao gồm địa chỉ vật lý của client, địa chỉ vật lý và địa chỉ IP của DHCP server, cũng như giá trị địa chỉ IP và subnet mask cung cấp cho DHCP client.

Thông tin thêm

Trong trường hợp DHCP client nhận được nhiều DHCP offer, giả sử như trong mạng có nhiều DHCP server với khả năng đáp ứng cho DHCP client một IP address. Trong hầu hết các trường hợp, DHCP client chấp nhận DHCP offer đến đầu tiên.

3. **DHCPREQUEST**— Client chọn một DHCP offer, xây dựng một gói DHCP request và quảng bá gói này. Gói DHCP request này bao gồm địa chỉ IP của server phát ra DHCP offer và địa chỉ vật lý của DHCP client. DHCP request này thực hiện hai công việc cơ bản. Đầu tiên nó báo cho DHCP server được chọn rằng client yêu cầu DHCP server ấn định cho nó một địa chỉ IP (và những thông tin cấu hình khác). Thứ hai, nó thông báo cho các DHCP server khác là DHCP offer của chúng không được chấp nhận.
4. **DHCPACK**— Khi DHCP server được chọn nhận được gói DHCP request, nó sẽ xây dựng gói cuối cùng của tiến trình hợp đồng. Gói tin này là DHCP ack (viết tắt của acknowledgement). DHCP ack bao gồm địa chỉ IP và subnetmask cho DHCP client. DHCP client cũng có thể được cấu hình một cách tùy chọn thêm địa chỉ IP của gateway mặc định, nhiều máy chủ DNS, và một hoặc hai WINS server. Ngoài các thông tin về địa chỉ IP, DHCP client có thể nhận thêm các thông tin cấu hình như loại NetBIOS (thay đổi tùy theo cách phân giải tên NetBIOS).

DHCP còn có 3 trường quan trọng khác dùng để chỉ ra khoảng thời gian. Một trường cho biết độ dài của hợp đồng. Hai trường thời gian khác là T1 và T2, được sử dụng khi client muốn làm tươi lại hợp đồng. Việc sử dụng của ba trường này sẽ được giải thích sau.

9.3.1 Trạm chuyển tiếp

Nếu cả hai DHCP client và DHCP server cùng nằm trong một phân đoạn mạng, tiến trình xử lý diễn ra chính xác như trong phần mô tả phía trước. Nếu DHCP client và DHCP server nằm trên các mạng khác nhau chia cắt bởi một hoặc nhiều router, tiến trình trở lên phức tạp hơn. Router thông thường không chuyển tiếp broadcast tới các mạng khác. Để DHCP có thể làm việc được, một bộ phận trung gian phải được cấu hình phục vụ cho tiến trình DHCP. Bộ phận trung gian có thể là một host khác trên cùng một mạng với DHCP client, nhưng thường là chính router. Trong trường hợp này, tiến trình thực hiện chức năng trung gian được gọi là trạm chuyển tiếp BOOTP hoặc DHCP.

Trạm chuyển tiếp được cấu hình một địa chỉ IP cố định và cũng chứa địa chỉ của DHCP server. Bởi vì trạm chuyển tiếp có một địa chỉ IP được cấu hình, chúng có thể gửi và nhận gói trực tiếp với DHCP server. Bởi vì trạm chuyển tiếp nằm cùng phía với client, nó có thể liên lạc với DHCP client thông qua broadcast.

Trạm chuyển tiếp lắng nghe broadcast trên cổng UDP 68; khi trạm chuyển tiếp nhận ra một DHCP request, nó truyền lại yêu cầu cho DHCP server. Khi trạm chuyển tiếp nhận được phản hồi từ DHCP server, phản hồi này sẽ được broadcast lại trong

phân đoạn mạng cục bộ. Để ngắn gọn những giải thích trên đây đã bỏ một vài chi tiết trong thực hiện, nhưng nó cũng thể hiện được bản chất thực hiện của trạm chuyển tiếp, muốn có thêm thông tin, bạn có thể đọc trong RFC 1542.

Thông tin thêm

Không phải router nào cũng cung cấp chức năng trạm chuyển tiếp BOOTP/DHCP. Khả năng của router được nói đến trong RFC 1542.

9.3.2 Trường thời gian DHCP

DHCP client thuê địa chỉ IP từ DHCP server trong một khoảng thời gian cố định, thời gian này được cấu hình trên DHCP server. Các giá trị thời gian T1 và T2 gửi trong bản tin DHCP ack được sử dụng trong tiến trình làm mới lại hợp đồng. Giá trị T1 báo cho Client khi nào nên thực hiện tiến trình làm mới lại hợp đồng thuê của nó. T1 thường được đặt là nửa thời gian thuê thực tế. Giả sử ví dụ sau cho hợp đồng trong khoảng thời gian 8 ngày.

Bốn ngày sau khi hợp đồng, client gửi DHCP request đề nghị làm mới lại hợp đồng thuê địa chỉ IP của nó với DHCP server. Giả sử DHCP server đang còn trên mạng, hợp đồng sẽ được làm mới lại với DHCP ack. Không giống như DHCP request và ack trong các tiến trình trước bao gồm 4 bước, hai gói này không broadcast mà là được gửi đi trực tiếp. Điều này thực hiện được bởi vì bây giờ cả hai máy tính đã có địa chỉ thực.

Nếu DHCP server không đáp lại khi DHCP client đưa ra yêu cầu tại 50% thời gian hợp đồng (4 ngày), client sẽ tiếp tục làm mới hợp đồng khi tới 75% thời gian hợp đồng (6 ngày). Nếu yêu cầu này cũng thất bại, DHCP client cố thử lại lần 3 ở thời điểm 87.5% (7 ngày). Tại thời điểm này DHCP client chấp nhận làm lại hợp đồng nếu DHCP server gửi trả lại gói. Nếu như DHCP không có khả năng làm mới lại hợp đồng trong 87.5% thời gian của hợp đồng, thời gian T2 bắt đầu có ảnh hưởng. Thời gian T2 cho phép DHCP client bắt đầu broadcast yêu cầu cho bất cứ DHCP server nào. Nếu như DHCP client không có khả năng làm mới lại hợp đồng hoặc lấy được hợp đồng mới từ một DHCP server khác trong thời gian hết hạn của hợp đồng, client phải dừng sử dụng địa chỉ IP và các hoạt động TCP/IP trên mạng.

9.4 Cấu hình DHCP

DHCP client nhận được gói thông tin cấu hình từ DHCP server. Những thông tin này bao gồm địa chỉ IP và các cấu hình khác. Bạn phải cấu hình bằng tay DHCP server với các thông tin địa chỉ TCP/IP mà không cần làm với client. Bạn cấu hình DHCP với một khối hoặc một khoảng địa chỉ IP có thể đảm bảo cho các yêu cầu hợp đồng. Mỗi

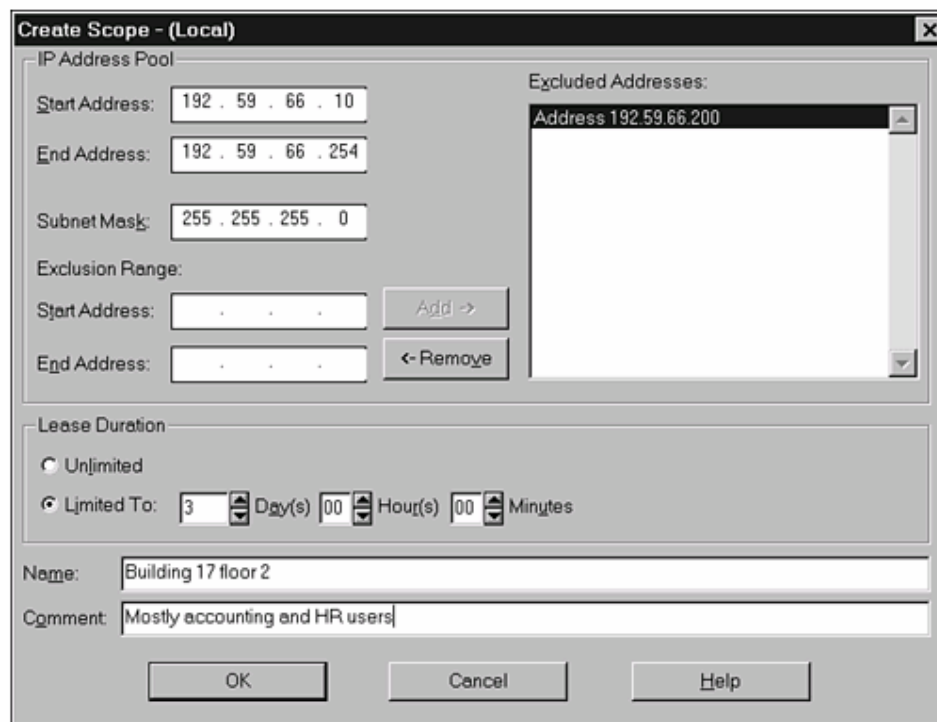
khối địa chỉ IP được gọi là phạm vi DHCP. Mỗi phạm vi DHCP bao gồm một khối địa chỉ có thể được sử dụng trên một phân đoạn mạng.

9.4.1 Cấu hình DHCP Server trên Windows

Chúng ta sẽ nghiên cứu các thông tin cần thiết để cấu hình DHCP. Windows NT Server là một ví dụ tốt cho việc cấu hình DHCP server. Phiên bản mới nhất của Windows, như Windows 2000 Server và Windows 2003, có cùng các công cụ cấu hình DHCP. Các bước sau sẽ mô tả làm sao cài đặt DHCP server. Nếu bạn đã từng cài đặt DHCP trên mạng thì bạn nên đọc thêm các thông tin kèm theo. Điều quan trọng là không chỉ Windows mới cấu hình được DHCP server. Chúng ta cũng có thể thấy các Unix/Linux cũng có các DHCP server trên mạng.

Để cấu hình DHCP server trên Windows NT, làm theo 3 bước sau:

1. Cài đặt dịch vụ DHCP.
2. Chuyển đến công cụ DHCP Manager bằng cách chọn Start, Programs, Administrative Tools, DHCP Manager. Công cụ DHCP Manager (Cục bộ) xuất hiện. Tại đây có một mục được đánh nhãn Local Machine; nếu như double-click vào mục này, một ký tự phía trái có hai giá trị + và -. Đảm bảo mục Local Machine hiển thị ký tự -, nó xác nhận mục này đã được mở rộng.
3. Chọn Scope, Create từ menu. Bạn sẽ có hộp thoại Create Scope - (Local), thể hiện trên **hình 9.1**. Trường Start Address và End Address xác nhận hai điểm đầu và kết thúc của khối địa chỉ mà bạn cho phép DHCP server điều khiển. Trong **hình 9.1**, bạn có thể nhìn thấy địa chỉ bắt đầu 192.59.66.10 và kết thúc là 192.59.66.254. Nếu bất cứ địa chỉ IP nào nằm trong dãy địa chỉ này được gán tĩnh cho một thiết bị nào đó, thì bạn phải loại chúng ra khỏi phạm vi này để chúng không gán động cho các máy tính khác. Nếu không có thể gây ra truy cập địa chỉ giữa các máy tính trong mạng. Trong ví dụ này, chính DHCP server được cấu hình tĩnh với địa chỉ IP 192.59.66.200; bạn có thể thấy địa chỉ này được loại trừ và không nằm trong phạm vi.



Hình 9-1 Hộp thoại DHCP Manager's Create Scope

Thông tin thêm

Không cần cấu hình phạm vi với tất cả các địa chỉ IP cho phép của mạng hoặc mạng con. Nếu làm như thế bạn phải đảm bảo không có sự đụng chạm với địa chỉ IP của router hoặc của các thiết bị được cấu hình địa chỉ IP tĩnh trên mạng.

4. Cấu hình trường Subnet Mask thích hợp. Nếu bạn muốn, bạn có thể thay đổi thời gian hợp đồng và tạo các mục trong trường Name và Comment. Chuỗi ký tự bạn nhập vào trong hai trường này chỉ được sử dụng cho mục đích quản trị.

Sau khi bạn hoàn thành, chọn nút OK để đóng hộp thoại Create Scope – (Local) và hiển thị hộp thoại DHCP Manager. Hộp thoại DHCP Manager xác nhận phạm vi đã được tạo thành công nhưng vẫn chưa hoạt động. Hộp thoại này sẽ hỏi bạn muốn kích hoạt nó không. Bạn có thể chọn Yes hoặc nút No. Nếu bạn muốn thêm các thông số khác như địa chỉ IP của gateway hoặc máy chủ DNS, thông thường bạn chọn không kích hoạt ...

Thông tin thêm

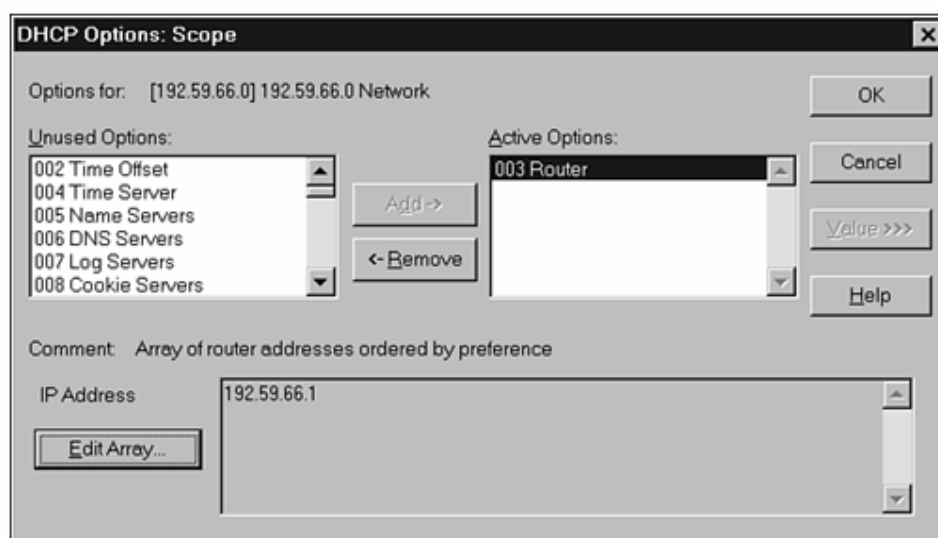
Thường hai (hoặc nhiều hơn) DHCP servers được cấu hình làm việc trên một mạng. DHCP server bổ sung cung cấp khả năng chịu lỗi cho mạng và cho phép DHCP client lấy được hợp đồng mới khi một DHCP server không hoạt động. Tuy vậy cần đảm bảo các server hoạt động độc lập và không dùng chung các thông tin liên quan đến các địa chỉ IP cho thuê. Vì lý do đó, không cấu hình nhiều DHCP server với các phạm vi địa chỉ chồng lẫn nhau. Ngược lại chắc chắn sẽ xảy ra vấn đề hai DHCP client được cấu hình cùng một địa chỉ IP dẫn đến sự

cổ cho mạng. Một vài hệ điều hành, như là Windows, sẽ thông báo cho bạn khi kiểm tra thấy trùng lặp địa chỉ.

Thông thường nếu bạn muốn DHCP server cấu hình cho DHCP client với nhiều thông số cấu hình hơn, bên cạnh địa chỉ IP và subnet mask. Trong Windows NT, DHCP Options cho phép bạn thêm vào một số các nhiệm ý cấu hình khác. Những nhiệm ý này có hai mức. Một mức cấu hình thiết lập các nhiệm ý phạm vi, chúng được dùng để cấu hình các tham số thay đổi từ phạm vi này sang các phạm vi khác. Mức cấu hình thứ hai là các nhiệm ý toàn cục được dùng để cấu hình cho các tham số, áp dụng cho tất cả các phạm vi.

Để cấu hình thông số phạm vi trong Windows NT, thực hiện các bước sau:

1. Chọn DHCP Options, Scope từ DHCP Manager. Hộp thoại DHCP Options: Scope xuất hiện.
2. Từ danh sách Unused Options, chọn nhiệm ý bạn muốn áp dụng ở mức phạm vi. Trong trường hợp này, 003 Router, được chọn và thêm vào sẽ xuất hiện trong danh sách Active Options.
3. Click vào nút Value để mở rộng hộp thoại cho nó xuất hiện như trong **hình 9.2**.



Hình 9-2 Hộp thoại Options DHCP: Scope

4. Sau khi hộp thoại được mở rộng, chọn nút Edit Array và thêm vào địa chỉ IP cho gateway. Mặc định sau khi mọi nhiệm ý mức phạm vi đã được nhập và cấu hình, bạn có thể chọn OK để đóng hộp thoại DHCP Options: Scope.

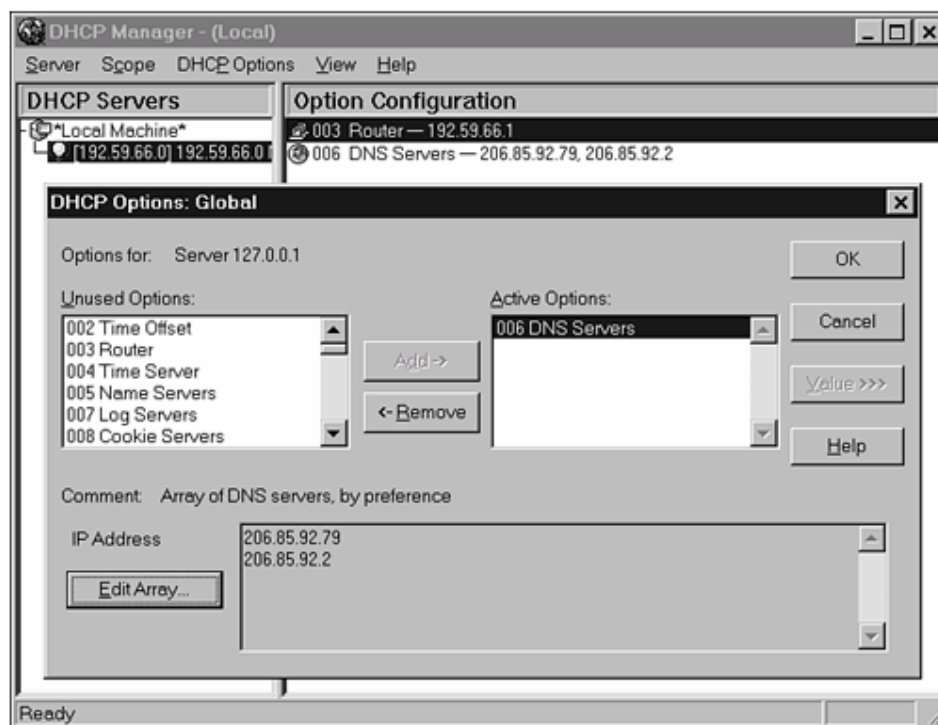
Bạn sử dụng nhiệm ý toàn cục để cấu hình các tham số không thay đổi giữa các phạm vi. Ví dụ, các máy tính trên mỗi phân đoạn mạng thường cùng sử dụng chung

các địa chỉ của các IP máy chủ DNS. Vì lý do này, các địa chỉ IP của các máy chủ DNS thường được cấu hình thông qua nhiệm ý toàn cục.

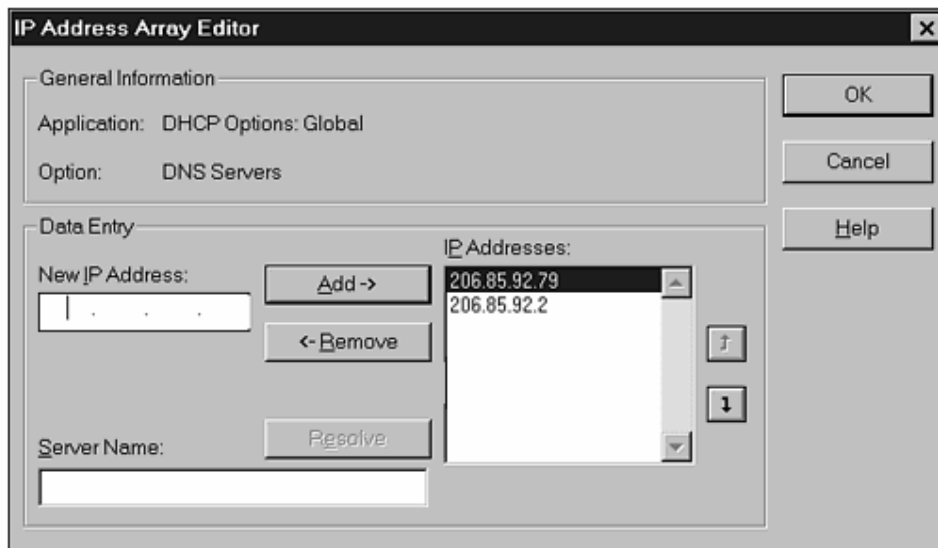
Để cấu hình các nhiệm ý toàn cục trong Windows NT, thực hiện các bước sau:

1. Chọn DHCP Options, Global từ DHCP Manager. Hộp thoại DHCP Options: Global xuất hiện.
2. Từ danh sách Unused Options, chọn nhiệm ý mà bạn muốn áp dụng ở mức toàn cục. Trong trường hợp này, 006 DNS Servers được chọn và thêm vào, và xuất hiện trong danh sách Active Options.
3. Click vào nút Value để mở rộng hộp thoại như trong **hình 9.3**.
4. Sau khi hộp thoại được mở rộng, chọn nút Edit Array. Hộp thoại IP Address Array Editor xuất hiện, như trong **hình 9.4**. IP Address Array Editor được sử dụng để nhập nhiều địa chỉ IP, trong trường hợp có nhiều máy chủ DNS.
5. Thêm vào địa chỉ IP cho máy chủ DNS. Sau khi các nhiệm ý toàn cục đã được nhập và cấu hình, bạn có thể chọn OK để đóng hộp thoại DHCP Options: Global.

Vào lúc này, bạn đã cấu hình một phạm vi DHCP với các nhiệm ý. Bạn phải kích hoạt phạm vi trước khi DHCP server có thể bắt đầu cho DHCP client trên mạng này thuê địa chỉ IP.

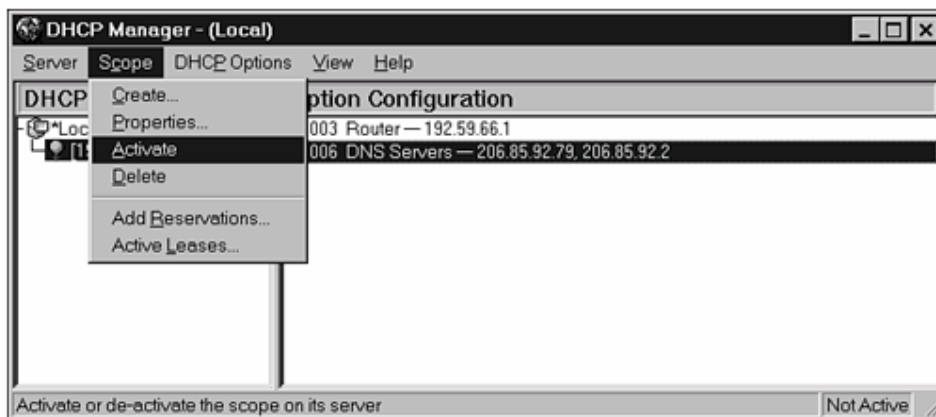


Hình 9-3 Hộp thoại DHCP Options: Global



Hình 9-4 Hộp thoại IP Address Array Editor

Để kích hoạt một phạm vi, chọn phạm vi để kích hoạt, chọn Scope, và sau đó chọn Activate từ menu, thể hiện như trong **hình 9.5**. DHCP được cấu hình và kích hoạt và bắt đầu cho các client DHCP thuê địa chỉ IP. Bạn có thể kiểm tra xem server có hoạt động thành công hay không bằng cách khởi động máy tính DHCP client và sử dụng lệnh `ipconfig` hoặc `winnicfg` với thông số Release và Renew



Hình 9-5 Phạm vi

9.4.2 Cấu hình DHCP Server trên Linux

Hệ thống Linux cung cấp dịch vụ DHCP thông qua `dhcpcd` (DHCP daemon). Các lệnh cài đặt `dhcpcd` tùy thuộc vào các nhà sản xuất. Thông tin cấu hình DHCP được lưu trong tập tin `/etc/dhcpcd.conf`.

Tập tin `/etc/dhcpcd.conf` chứa thông tin cấu hình địa chỉ IP mà DHCP daemon sẽ phân phối cho client. `/etc/dhcpcd.conf` cũng chứa các thiết lập lựa chọn

như địa chỉ broadcast, tên miền, địa chỉ máy chủ DNS, và địa chỉ của các router. Sau đây là một ví dụ của tập tin `/etc/dhcpd.conf`:

```
default-lease-time 600;
max-lease-time 7200;
option domain-name "macmillan.com";
option subnet-mask 255.255.255.0;
option broadcast-address 185.142.13.255;
subnet 185.142.13.0 netmask 255.255.255.0 {
    range 185.142.13.10 185.142.13.50;
    range 185.142.13.100 185.142.13.200;
}
```

Tóm tắt

DHCP cung cấp một cách thức đơn giản để cấu hình địa chỉ IP và những thiết lập cấu hình khác cho máy tính client. Nó rất hữu ích khi có sự thay đổi xảy ra; ví dụ, nếu bạn thay đổi ISP, bạn cần thay đổi mục máy chủ DNS. Nếu như công ty có 5000 máy cấu hình bằng tay, trải rộng trên 10 vị trí thì việc thay đổi sẽ rất tốn kém và tiêu tốn nhiều thời gian. Do đó, với một DHCP server bạn có thể thực hiện thay đổi một cách hiệu quả bằng cách đơn giản thay đổi một nhiệm ý Global / Scope. Cứ mỗi lần DHCP client cần làm mới lại địa chỉ IP, nó sẽ nhận được các địa chỉ IP của các máy chủ DNS mới. Trong chương này, bạn đã được học về cách làm việc của DHCP. Bạn cũng học về cấu hình cho các phạm vi và cách thức cấu hình và cài đặt DHCP trên server Windows NT.

CHƯƠNG 10

TRUYỀN TẬP TIN VÀ CÁC TIỆN ÍCH TRUY CẬP

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **FTP và TFTP**
- **RCP**
- **NFS**
- **SMP**

Một trong những lợi ích lớn nhất của TCP/IP là nó cung cấp môi trường rất linh động trong đó nhiều kiểu hệ thống khác nhau có thể thông tin với nhau. Không phụ thuộc vào phần cứng và hệ điều hành đang sử dụng, hai host trên mạng TCP/IP có thể liên lạc với nhau nếu chúng sử dụng cùng giao thức. Thông thường thì các host này cần sử dụng các tiện ích truy cập đặc biệt.

Truy cập và truyền tập tin thường được sử dụng nhiều nhất trong bất cứ mạng nào. TCP/IP bao gồm hai giao thức được sử dụng đặt biệt cho việc truyền và truy cập tập tin. Hầu hết các hệ điều hành đều cung cấp các tiện ích được thiết kế để tận dụng các giao thức này. Chương này nghiên cứu về ba tiện ích truyền cổ điển: Giao thức truyền tập tin FTP (File Transfer Protocol), giao thức truyền tập tin thông thường TFTP (Trivial File Transfer Protocol), và giao thức sao chép từ xa rcp (Remote Copy). Chúng ta sẽ nghiên cứu làm sao tích hợp truyền tập tin với các hệ điều hành hiện đại qua các giao thức như Network Tập tin System (NFS) và Server Message Block (SMB).

Kết thúc chương này bạn sẽ có thể :

- Giải thích mục đích và việc sử dụng FTP
- Khởi tạo phiên làm việc FTP và sử dụng các lệnh FTP cho việc xem các cấu trúc thư mục ở xa, truyền tập tin, tạo và xóa các thư mục
- Giải thích mục đích và việc sử dụng của TFTP
- Sử dụng các lệnh để truyền tập tin sử dụng TFTP
- Giải thích mục đích và việc sử dụng lệnh rpc
- Giải thích mục đích và việc sử dụng NFS và SMB.

10.1 Giao thức truyền tập tin (FTP)

Giao thức truyền tập tin – File Transfer Protocol (FTP) là một giao thức được sử dụng rộng rãi cho phép truyền tập tin giữa hai máy tính trên mạng TCP/IP. Một ứng dụng truyền tập tin (thường được gọi là ftp) sử dụng giao thức FTP để truyền tập tin. Người dùng chạy ứng dụng FTP client trên một máy, và một máy khác chạy chương trình FTP server như ftpd (FTP daemon) trên máy Unix/Linux, hoặc một dịch vụ FTP trên trên các hệ điều hành khác. Rất nhiều chương trình FTP client sử dụng chế độ dòng lệnh, ngoài ra còn có các phiên bản FTP client mới với giao diện đồ họa. FTP được sử dụng chính để truyền tập tin, mặc dù nó có thể thực hiện các chức năng khác như tạo thư mục, xóa thư mục, liệt kê các tập tin.

Trong thế giới Unix, một **daemon** là một tiến trình chạy ngầm (không thể hiện trên màn hình) và thực hiện một dịch vụ khi dịch vụ được yêu cầu. Một daemon cũng được gọi là dịch vụ trong thế giới Windows.

FTP sử dụng giao thức TCP và như vậy nó hoạt động thông qua một phiên làm việc hướng kết nối, tin cậy giữa máy tính client và server. FTP daemon tiêu chuẩn (trên server) lắng nghe các yêu cầu từ client trên cổng TCP 21. Khi một client gửi một yêu cầu, kết nối TCP được khởi tạo (xem *chương 5, "Lớp vận chuyển"*). Sau đó người dùng từ xa được FTP server chứng thực và một phiên làm việc bắt đầu. Phiên làm việc FTP trước đây dựa trên văn bản yêu cầu người dùng tương tác thông qua chế độ dòng lệnh. Đánh lệnh để bắt đầu và kết thúc phiên FTP, lướt qua cấu trúc thư mục ở xa, và tải lên hay tải về các tập tin. Các chương trình FTP client mới dựa trên GUI (giao diện người dùng đồ họa) đưa ra một giao diện đồ họa để lướt trên các thư mục và di chuyển các tập tin.

Thông tin thêm

FTP cũng được sử dụng rộng rãi trên World Wide Web, và giao thức FTP đã được tích hợp với hầu hết trình duyệt Web. Đôi khi trong khi bạn đang tải tập tin từ trình duyệt Web, bạn có thể gặp thông báo địa chỉ URL bắt đầu với ftp://.

Trong hầu hết các máy tính, bạn bắt đầu phiên làm việc FTP trong chế độ văn bản bằng cách đánh vào ftp theo sau bởi tên host hoặc địa chỉ IP của FTP server. FTP sau đó đòi bạn nhập ID và mật khẩu, chúng được FTP server sử dụng để xác định xem bạn có đủ thẩm quyền truy cập hay không và quyền hạn của bạn là gì. Ví dụ, tài khoản người dùng bạn đăng nhập có thể chỉ có quyền quyền chỉ đọc hoặc vừa đọc vừa ghi. Rất nhiều FTP server có thể cho truy cập tự do và cho phép bạn đăng nhập vào với ID là anonymous. Khi một tài khoản anonymous được sử dụng, bạn có thể nhập bất cứ mật khẩu nào. Tuy vậy, người ta thường lấy địa chỉ email để làm mật khẩu. Khi FTP server không có ý định chia sẻ cộng đồng, server sẽ cấu hình không cho phép

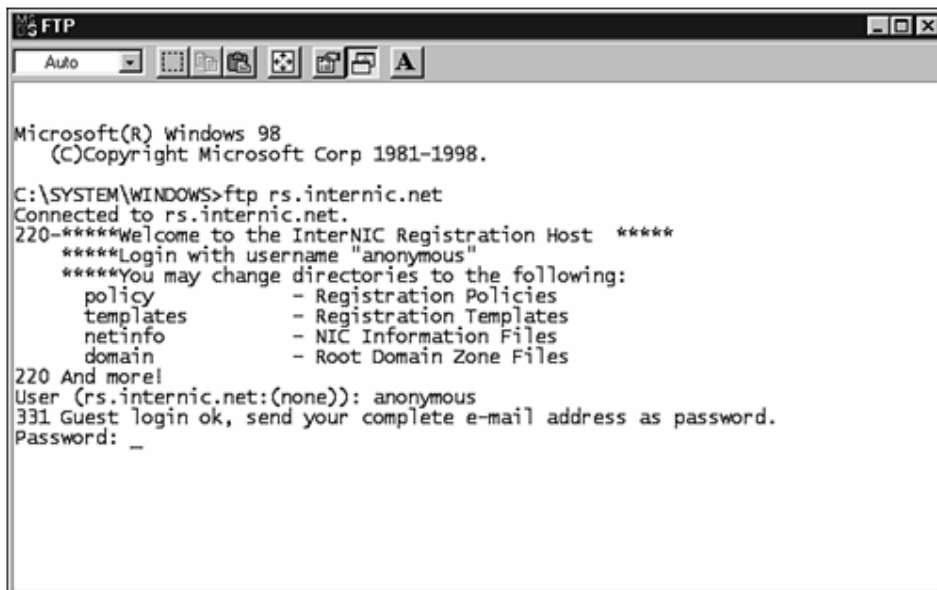
anonymous truy cập. Trong trường hợp này, bạn phải nhập ID người dùng và mật khẩu để có thể truy cập hệ thống. Nhà quản trị server FTP sẽ thiết lập và cung cấp ID người dùng và mật khẩu.

Rất nhiều FTP client cho phép bạn nhập các lệnh trên Unix hay DOS. Các lệnh thực sự tùy thuộc vào các phần mềm client đang dùng. Khi bạn chuyển tập tin sử dụng FTP, bạn phải xác định với FTP loại tập tin mà bạn muốn di chuyển; các dạng chính là dạng nhị phân hay mã ASCII. Chọn ASCII khi loại tập tin bạn muốn chuyển ở dạng văn bản đơn giản. Chọn nhị phân khi tập tin bạn muốn chuyển một tập tin chương trình, tập tin word hay các tập tin đồ họa. Chế độ chuyển tập tin mặc định là ASCII.

Có thể thấy rằng có nhiều FTP server chạy trên hệ điều hành Unix và Linux. Do trong các hệ điều hành dạng Linux có sự phân biệt giữa chữ hoa và chữ thường, nên bạn phải đánh chính xác tên tập tin. Thư mục hiện hành trên máy tính cục bộ là nơi bạn bắt đầu chạy phiên làm việc FTP, và là vị trí mặc định cho việc truyền tập tin tới hoặc đi.

Sau đây là danh sách các lệnh FTP thường dùng và phần giải thích các lệnh.

- ftp - Lệnh ftp được sử dụng để bắt đầu chương trình FTP client. Bạn có thể nhập ftp theo sau bởi địa chỉ IP hoặc tên miền. Trong **hình 10.1** một phiên FTP làm việc với rs.internic.net được bắt đầu bằng cách đánh lệnh ftp rs.internic.net. Như bạn thấy, có nhiều thông tin được trả về.



```
Microsoft(R) Windows 98
(C)Copyright Microsoft Corp 1981-1998.

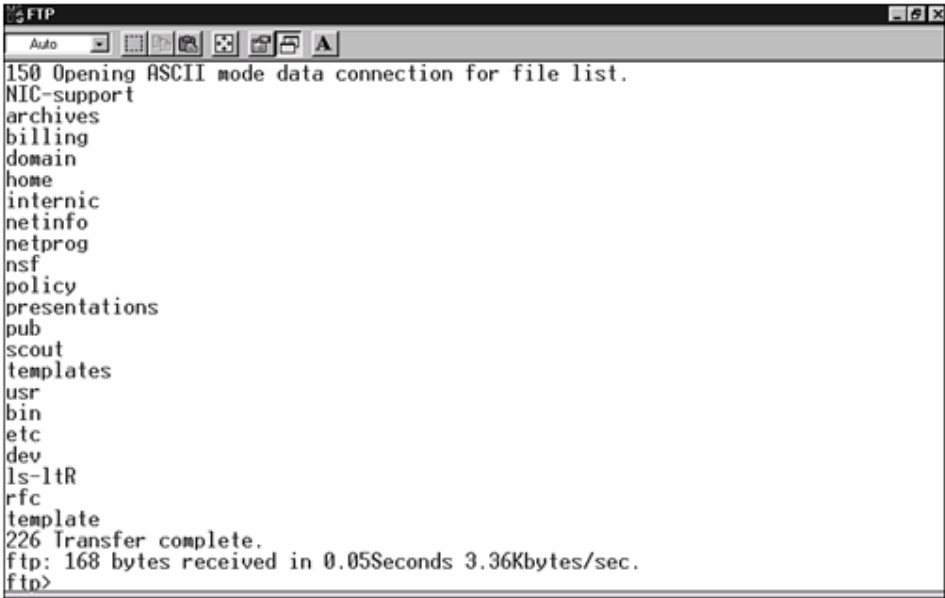
C:\SYSTEM\WINDOWS>ftp rs.internic.net
Connected to rs.internic.net.
220-*****Welcome to the InterNIC Registration Host *****
*****Login with username "anonymous"*****
*****You may change directories to the following:
policy          - Registration Policies
templates       - Registration Templates
netinfo         - NIC Information Files
domain          - Root Domain Zone Files
220 And more!
User (rs.internic.net:(none)): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password: _
```

Hình 10-1 Bắt đầu một phiên làm việc FTP

Dòng đầu tiên cho biết bạn đã kết nối. Hai dòng có 220 đứng trước và tất cả các dòng nằm giữa là một thông điệp đăng nhập được đưa ra cho tất cả các người dùng

đăng nhập. Dòng kế tiếp sẽ hỏi bạn ID người dùng; ở đây là `anonymous`. Dòng bắt đầu với `331` là một thông điệp hệ thống yêu cầu bạn nhập địa chỉ email dùng làm mật khẩu. Một con số luôn luôn đi trước một thông điệp hệ thống. Như bạn có thể nhìn thấy ở dòng cuối, mật khẩu không hiển thị khi đánh vào.

- `user` - Lệnh `user` được sử dụng để thay đổi ID người dùng và mật khẩu trong phiên làm việc hiện tại. Bạn sẽ có dấu nhắc để nhập ID người dùng và mật khẩu mới, giống như khi bạn sử dụng lệnh `ftp`. Lệnh này có tác dụng giống như thoát FTP và bắt đầu lại với một người dùng mới.
- `help` - Lệnh `help` hiển thị các lệnh ftp có giá trị trên FTP client.
- `ls` hoặc `dir` - Lệnh `ls` hoặc `ls -l` trong Unix/Linux hoặc lệnh `dir` trong Windows liệt kê các nội dung trong thư mục. Đáp ứng cho các lệnh này sẽ liệt kê danh sách các tên tập tin và thư mục trong thư mục hiện hành trên FTP server. Kết quả của lệnh `ls` thể hiện trong **hình 10.2**. Giữa hai thông điệp hệ thống (các dòng này bắt đầu bởi `150` và `226`) là nội dung thư mục hiện tại, liệt kê mọi tập tin và các thư mục con trong thư mục làm việc hiện tại. Lệnh `ls -l` thì tương tự lệnh `ls` nhưng có liệt kê thêm các thông tin bổ sung như cho phép đọc, viết và ngày tạo tập tin.



```
FTP
Auto
150 Opening ASCII mode data connection for file list.
NIC-support
archives
billing
domain
home
internic
netinfo
netprog
nsf
policy
presentations
pub
scout
templates
usr
bin
etc
dev
ls-ltr
rfc
template
226 Transfer complete.
ftp: 168 bytes received in 0.05Seconds 3.36Kbytes/sec.
ftp>
```

Hình 10-2 Lệnh `ls`

- `pwd` - Lệnh `pwd` in ra tên của thư mục làm việc hiện hành. Đây là thư mục trên máy ở xa chứ không phải trên máy cục bộ.
- `cd` - Lệnh `cd` thay đổi thư mục làm việc hiện hành trên FTP server.
- `mkdir` - Lệnh `mkdir` trong Unix/Linux tạo thư mục trên FTP server trong thư mục làm việc hiện hành. Lệnh này không cho phép trong các phiên làm việc `anonymous` FTP.
- `rmdir` - Lệnh Unix `rmdir` có thể di chuyển các thư mục trên FTP server từ thư mục hiện tại. Lệnh này không cho phép trong các phiên làm việc `anonymous` FTP.

- binary - Lệnh binary chuyển FTP client từ chế độ truyền ASCII mặc định sang chế độ truyền nhị phân. Chế độ nhị phân hữu ích khi chuyển các tập tin nhị phân như các chương trình và các tập tin đồ họa, sử dụng các lệnh get, put, mget, và mput.
- ascii - Lệnh ascii chuyển FTP client từ chế độ truyền nhị phân sang chế độ truyền ASCII.
- type - Lệnh type hiển thị chế độ hiện tại cho việc chuyển tập tin (ASCII hay Binary).
- status - Lệnh status hiển thị thông tin về các thiết lập khác nhau trên FTP client. Các thiết lập này bao gồm chế độ (nhị phân hoặc ASCII) và các thông điệp hệ thống khác.
- get - Lệnh get lấy tập tin từ FTP server tới FTP client. Sử dụng lệnh get theo sau bởi tên tập tin sẽ copy các tập tin từ FTP server tới thư mục hiện tại trên FTP client. Nếu lệnh get theo sau bởi hai tên tập tin, tên thứ hai sẽ là tên tập tin mới đặt trên client. Nếu bạn quên không nhập tên thứ hai, FTP sẽ luôn nhắc bạn.
- mget - Lệnh mget giống như lệnh get ngoại trừ nó cho phép bạn lấy được nhiều tập tin.
- put - Lệnh put truyền tập tin từ FTP client tới FTP server. Sử dụng lệnh put theo sau bởi một tên tập tin sẽ copy tập tin từ FTP client lên the FTP server. Nếu lệnh put theo sau bởi hai tên tập tin, tên thứ hai sẽ là tên tập tin mới đặt trên server. Nếu bạn quên không nhập tên thứ hai, FTP sẽ nhắc bạn.
- mput - Lệnh mput giống như lệnh put ngoại trừ nó cho phép bạn truyền được nhiều tập tin.
- open - Lệnh open cho phép bạn thiết lập một phiên làm việc mới với FTP server. Để thoát ra và khởi động lại FTP cần thiết phải có một shortcut. Lệnh open có thể sử dụng để mở một phiên làm việc với một server khác hoặc mở lại với server hiện tại.
- close - Lệnh close kết thúc một phiên làm việc hiện tại với FTP server. Chương trình FTP client vẫn mở và bạn có thể khởi động một phiên làm việc mới bằng lệnh open.
- bye hoặc quit - Lệnh này đóng phiên làm việc hiện tại và kết thúc FTP client.

Để biết thêm về giao thức FTP xem RFC 959.

10.2 Giao thức truyền tập tin bình thường (TFTP)

Giao thức truyền tập tin bình thường (TFTP) được sử dụng để truyền các tập tin giữa TFTP client và TFTP server, một máy tính chạy tftpd (TFTP daemon). Giao thức này sử dụng UDP để vận chuyển và không giống như FTP, nó không yêu cầu đăng nhập để truyền tập tin. Bởi vì TFTP không yêu cầu đăng nhập, nó có một lỗ hổng bảo mật, đặc biệt nếu TFTP server cho phép ghi.

Giao thức TFTP được thiết kế rất nhỏ đến nỗi cả nó và giao thức UDP có thể chạy trên một PROM (bộ nhớ lập trình chỉ đọc) chip. Giao thức TFTP có hạn chế khi so sánh với giao thức FTP. Giao thức TFTP chỉ cho phép đọc và ghi tập tin; nó không thể liệt kê nội dung các thư mục, tạo và di chuyển các thư mục hoặc cho phép người

dùng đăng nhập như là giao thức FTP cho phép. Giao thức TFTP chủ yếu sử dụng kết hợp với các giao thức RARP và BOOTP để khởi động các trạm làm việc không có ổ đĩa, và trong một số trường hợp, nó được dùng để tải lên mã hệ thống mới cho router hoặc cho các thiết bị mạng khác. Giao thức TFTP có thể cho phép truyền tập tin sử dụng cả khuôn dạng ASCII và các dạng nhị phân như octet, dạng thứ ba là mail nhưng không còn sử dụng nữa.

Khi người dùng nhập vào tftp trên chế độ dòng lệnh, nó sẽ khởi tạo kết nối tới server và thực hiện truyền tập tin. Khi quá trình truyền tập tin kết thúc, phiên làm việc được đóng lại và kết thúc. Cấu trúc của lệnh TFTP như dưới đây:

```
TFTP [-i] host [get | put] <tên tập tin nguồn> [<tên tập tin đích >]
```

Để biết nhiều về giao thức, xem RFC 1350.

10.3 Sao chép từ xa (Remote Copy)

Lệnh rcp có thể thay thế cho ftp; nó cho phép người dùng sao chép tập tin qua mạng. Lệnh rcp là phiên bản từ xa của lệnh cp (copy). Khi sử dụng lệnh rcp, không cần cung cấp ID người dùng và mật khẩu; nó có thể gây ra một lỗ hổng bảo mật. Tuy vậy, nó vẫn có một mức bảo mật là tên máy tính của bạn phải nằm trên một trong hai tập tin rhosts và hosts.equiv trên server. Lệnh rcp cho phép người dùng sao chép các tập tin giữa các máy cục bộ và các host-server hoặc là giữa hai máy ở xa. Cấu trúc đoạn lệnh rcp:

```
rcp [hostname1]:filename1 [hostname2]:filename2
```

- hostname1 - Thông thường là tên host hoặc là tên miền đầy đủ (FQDN) của máy tính nguồn. Sử dụng hostname nếu tập tin nguồn nằm trên máy từ xa. Xem **chương 8, "Phân giải tên,"** về thông tin của tên host và FQDN.
- filename1 - Là đường dẫn và tên tập tin của tập tin nguồn.
- hostname2 - Thông thường là tên host hoặc là tên miền đầy đủ (FQDN) của máy tính đích. Sử dụng host name nếu tập tin đích nằm trên máy từ xa.
- filename2 - Là đường dẫn và tên tập tin của tập tin đích.

Sau đây là các ví dụ sử dụng lệnh rcp.

Ví dụ này copy tập tin từ máy Unix ở xa về máy cục bộ:

```
rcp server3.corporate.earthquakes.txt earthquakes.txt
```

Ví dụ này copy tập tin từ máy cục bộ sang máy ở xa:

```
rcp earthquakes.txt server3.corporate.earthquakes.txt
```

Bạn có thể sử dụng rcp để copy các tập tin từ máy ở xa sang một máy ở xa khác. Xem *chương 11, "Các tiện ích truy cập từ xa"*, để biết thêm về rcp và các chọn lựa truy cập từ xa khác.

10.4 Tích hợp truy cập tập tin mạng

Các tiện ích như ftp và tftp là các ứng dụng độc lập nằm trên lớp Ứng dụng của giao thức TCP/IP. Các tiện ích này rất thuận tiện vào thời điểm chúng xuất hiện và hiện nay chúng vẫn được sử dụng trong một số trường hợp, nhưng các nhà sản xuất và các nhà hoạch định Internet đã tìm kiếm các giải pháp mới hiệu quả hơn. Mục đích của họ là tích hợp việc truy cập tập tin từ xa với việc truy cập tập tin cục bộ, do đó các tài nguyên ở xa và các tài nguyên cục bộ sẽ cùng xuất hiện trên một giao diện chung. (Ví dụ các tập tin có thể duyệt đều cùng xuất hiện qua giao diện Network Explorer trên Windows.)

Một phần của dịch vụ truy xuất tập tin mạng tích hợp này yêu cầu một bộ chuyển hướng (hoặc yêu cầu) trên các máy client để thông dịch các yêu cầu tài nguyên và định hướng yêu cầu trên mạng. Một phần khác của giải pháp này là giao thức truy cập tập tin, hình thành một lớp giao thức hoàn chỉnh mà thông qua nó các công cụ giao diện người dùng GUI và các ứng dụng khác có thể truy xuất mạng. Phương pháp truy cập này là một phương pháp được ưa chuộng cho các mạng cục bộ. Trong các phần sau, bạn sẽ được giới thiệu một cặp giao thức tích hợp dịch vụ truy cập tập tin mạng:

- Network File System (NFS) - Một giao thức sử dụng trên các máy Unix và Linux.
- Server Message Block (SMB) - Một giao thức sử dụng để truy cập tập tin từ xa cho các máy Windows client.

Các giao thức này thể hiện sức mạnh của lớp Ứng dụng của TCP/IP, và các thuận lợi của việc xây dựng một hệ thống mạng chung quanh chồng giao thức đã được xác định hoàn chỉnh, trong đó các giao thức lớp dưới hình thành một nền tảng cho các giao thức đặc biệt hơn ở bên trên.

Hệ thống tập tin mạng

Sun là công ty đầu tiên phát triển hệ thống tập tin mạng (NFS) và bây giờ được sử dụng trong Unix, Linux, và rất nhiều hệ thống khác. NFS cho phép người dùng truy cập (đọc, ghi, tạo, và xóa) thư mục và các tập tin nằm trên các máy ở xa cũng giống như các thư mục, tập tin này nằm trên máy cục bộ. Bởi vì NFS được thiết kế để cung cấp giao diện trong suốt giữa các hệ thống tập tin cục bộ và hệ thống tập tin ở xa, và bởi vì nó được thực hiện bên trong hệ điều hành của cả 2 máy tính (ở xa và cục bộ) nên không cần bất kỳ thay đổi nào trong chương trình ứng dụng. Các chương trình có thể truy cập các tập tin cục bộ và ở xa với NFS mà không phải biên dịch lại hoặc thay

đổi. Đối với người dùng, mọi tập tin và thư mục xuất hiện và hoạt động như là chúng chỉ tồn tại trên hệ thống tập tin cục bộ.

Phiên bản gốc của NFS sử dụng giao thức UDP cho việc vận chuyển và dùng trong mạng LAN. Tuy nhiên, các phiên bản sau cho phép sử dụng giao thức TCP; với sự bổ sung độ tin cậy của TCP cho phép mở rộng khả năng của NFS, và bây giờ nó có thể hoạt động trên WAN.

NFS được thiết kế độc lập với hệ điều hành, giao thức truyền tải, và kiến trúc vật lý của mạng. Điều này cho phép một NFS client làm việc được với bất cứ NFS server nào. Sự độc lập này có được là do sử dụng giao thức Remote Procedure Calls (RPCs) giữa máy tính client và server. RPC là một tiến trình cho phép một chương trình đang chạy trên máy này có khả năng triệu gọi một đoạn lệnh nằm trong một chương trình trên máy khác. RPC đã được phát triển rất nhiều năm và được hỗ trợ bởi nhiều hệ điều hành. Trong trường hợp của NFS, hệ điều hành trên máy client thực hiện một triệu gọi từ xa tới hệ điều hành trên server.

Trước khi các tập tin và thư mục ở xa có thể được sử dụng trên hệ thống NFS, chúng phải qua một tiến trình gọi là gắn kết. Sau khi được gắn kết, các tập tin và các thư mục ở xa xuất hiện và hoạt động như là chúng ở trên hệ thống tập tin cục bộ.

Phiên bản mới nhất của giao thức NFS là phiên bản 4, nó được mô tả trong RFC 3010. Để xem các thông tin thêm về các phiên bản trước của NFS, xem RFC 1094 cho NFS phiên bản 2, RFC 1813 cho NFS phiên bản 3. NFS thì khác nhau trong các hệ điều hành khác nhau. Bạn có thể xem tài liệu của nhà cung cấp để có thêm các thông tin về cách cấu hình NFS trên hệ điều hành của bạn.

10.5 Khối thông điệp server (SMB)

Server Message Block (SMB) là giao thức hỗ trợ các công cụ tích hợp mạng cho giao diện người dùng Windows, như là Explorer, Network Neighborhood, hoặc the Map Network Drive. SMB được thiết kế trên các giao thức khác nhau bao gồm IPX/SPX (chồng giao thức NetWare), NetBEUI (giao thức cho PC LANs), và TCP/IP. SMB nằm trên lớp NetBIOS, giao tiếp với các giao thức lớp Transport và cung cấp các dịch vụ liên quan tới định danh tài nguyên và vị trí (Xem **hình 10-3**).

SMB	Lớp ứng dụng
NetBIOS	
TCP hoặc UDP	Lớp vận tải
IP	Lớp Internet
Giao thức truy cập mạng	Giao thức truy cập mạng

Hình 10-3 SMB và chồng giao thức TCP/IP

Thông tin thêm

Ghi chú trong **hình 10-3**, cả hai SMB và NetBIOS chiếm lĩnh vị trí của lớp ứng dụng trong chồng giao thức TCP/IP. Trông có vẻ khó hiểu khi có hai giao thức cùng nằm thẳng đứng trên một lớp giao thức. Sự sắp xếp này thật ra là hợp lý khi xem nội dung hệ thống giao thức OSI. Như ta thấy trong **chương 1**, OSI chia lớp ứng dụng TCP/IP ra làm ba lớp riêng biệt. Trong trường hợp này, NetBIOS chiếm lĩnh lớp Phiên trong OSI và SMB chiếm lớp Ứng dụng và lớp Trình diện.

Microsoft đã sẵn sàng cho việc thay thế NetBIOS thông qua việc đề xướng các hệ thống khác như là hệ thống Active Directory dựa trên LDAP, xuất hiện lần đầu tiên trên Windows 2000. Tuy vậy, Active Directory vẫn chưa được sử dụng rộng rãi và NetBIOS sẽ vẫn tiếp tục được sử dụng, và chỉ có nó mới tương thích được các hệ thống khác.

Giống như các giao thức mạng khác, SMB được thiết kế theo khái niệm client (một máy tính yêu cầu dịch vụ) và server (một máy tính cung cấp dịch vụ). Mỗi phiên làm việc thường bắt đầu bằng việc trao đổi thông tin chuẩn bị, trong tiến trình này một dialect SMB được thương lượng và một client được chứng thực để đăng nhập vào server. Chi tiết của tiến trình chứng thực khác nhau tùy thuộc vào hệ điều hành và việc cấu hình, việc đăng nhập được đóng gói trong một `sesssetupX` SMB. (Một giao thức truyền đầu nằm dưới giao thức SMB và thường được gọi là SMB.)

Nếu tiến trình đăng nhập thành công, client gửi một SMB xác định tên của mạng mà nó muốn truy cập. Nếu quá trình chia sẻ truy cập thành công, client có thể đóng, mở, đọc hoặc ghi lên tài nguyên mạng, và server gửi các dữ liệu cần thiết để đáp ứng yêu cầu.

SMB thường được xem là một giao thức trên Windows, và thật ra điều quan trọng chính của SMB là sự tích hợp chặt chẽ của nó với giao diện người dùng của

Windows client. Nhưng chi tiết của giao thức NFS đã được các nhà phát triển và các hệ điều hành hỗ trợ các server liên lạc với các Windows client. Một loại server mã nguồn mở thông dụng Samba cung cấp SMB cho hệ thống Unix/Linux.

Tóm tắt

Một số các tiện ích TCP/IP cho phép người dùng chuyển tập tin hoặc truy cập các tập tin nằm ở xa như là chúng nằm trên máy cục bộ. Trong số chúng, giao thức FTP là dạng được sử dụng phổ biến nhất. Nó cho phép người dùng kết nối匿 danh với các hệ thống từ xa hoặc kết nối dùng một ID người dùng cụ thể và mật khẩu. Với quyền được cho phép thích hợp, người dùng có thể dùng lệnh ftp để copy tập tin, tạo và xóa các thư mục, xem cấu trúc thư mục trên các máy ở xa.

Giao thức TFTP cung cấp khả năng truyền tập tin cơ bản sử dụng giao thức UDP. TFTP không yêu cầu một người dùng đăng nhập và hiếm khi được sử dụng trực tiếp bởi người dùng thông thường. Giao thức TFTP sử dụng chủ yếu cho các máy trạm khởi động không cần đĩa và tải lên các mã cho các thiết bị mạng khác.

Giao thức RCP có thể thay thế cho giao thức FTP và cho phép người dùng copy các tập tin giữa hai máy. (Chúng ta sẽ nghiên cứu RCP trong **chương 11, "Các tiện ích truy cập từ xa"**)

Chương này cũng nghiên cứu về một cặp giao thức dùng trong các hệ điều hành hiện đại để tích hợp truy cập các tập tin ở xa với môi trường người dùng cục bộ: NFS, được sử dụng chính trong các mạng Unix/ Linux, và SMB, cung cấp việc truy cập tập tin và các nguồn tài nguyên khác cho Windows client.

CHƯƠNG CÁC TIỆN ÍCH

11 TRUY CẬP TỪ XA

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Telnet**
- **Công cụ Berkeley r***
- **Trusted access**

Các mạng máy tính ra đời nhằm mục đích chia sẻ tài nguyên từ xa, do đó bất cứ những gì bạn thực hiện trên một mạng đều có thể quy về định nghĩa của truy cập từ xa. Một vài tiện ích TCP/IP được xếp loại là các tiện ích truy cập từ xa. Các tiện ích truy cập từ xa phát triển trên Unix, nhưng được rất nhiều hệ điều hành cho phép làm việc. Mục đích của các tiện ích này là cung cấp cho người dùng ở xa một số khả năng mà một người dùng cục bộ có thể có. Trong chương này, chúng ta sẽ nghiên cứu về ứng dụng Telnet, và chúng ta sẽ học về tiện ích Berkeley r*—tập các tiện ích thiết kế hỗ trợ cho việc truy cập từ xa.

11.1 Telnet

Telnet là một tập các thành phần cung cấp cho các thiết bị đầu cuối truy cập đến một máy ở xa. Một phiên làm việc Telnet yêu cầu một Telnet client (hoạt động như một máy ở xa) và Telnet server (máy chấp nhận các yêu cầu kết nối và cho phép kết nối). Quan hệ này thể hiện như trên **hình 11.1**.

Telnet cũng là một giao thức - một hệ thống các luật định nghĩa các tương tác giữa Telnet server và client. Giao thức Telnet được định nghĩa trong một loạt RFCs. Bởi vì Telnet dựa trên một giao thức mở được định nghĩa hoàn hảo, nó có thể dùng trên một phạm vi lớn các hệ thống phần cứng và phần mềm. Mục đích cơ bản của Telnet là cung cấp một phương tiện sao cho các lệnh được đánh vào từ bàn phím của máy tính ở xa được đưa qua mạng tới một máy tính khác. Màn hình xuất liên quan với phiên làm việc từ máy server được đưa qua mạng tới màn hình của máy client (xem **hình 11.2**). Tác dụng của điều này cho phép người dùng từ xa có thể tương tác với server như là anh ta đang làm việc tại server này.

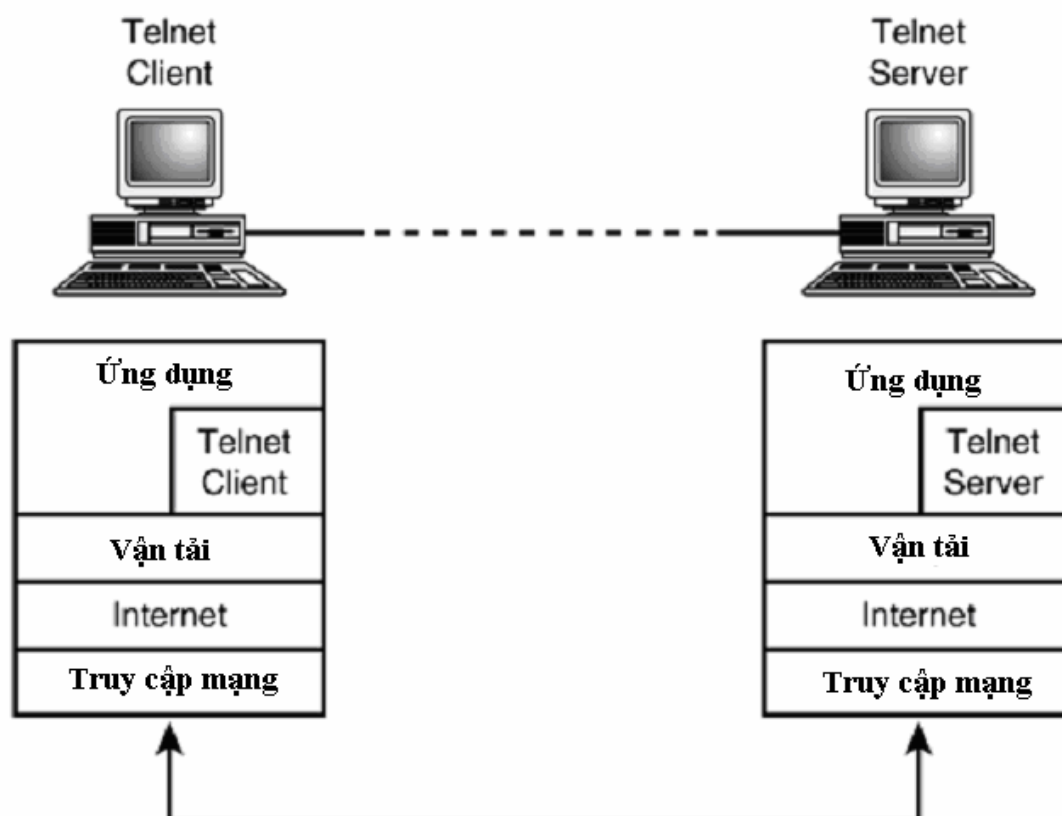
Trong hệ thống Unix, lệnh `telnet` được nhập ở chế độ dòng lệnh như sau:

```
telnet hostname
```

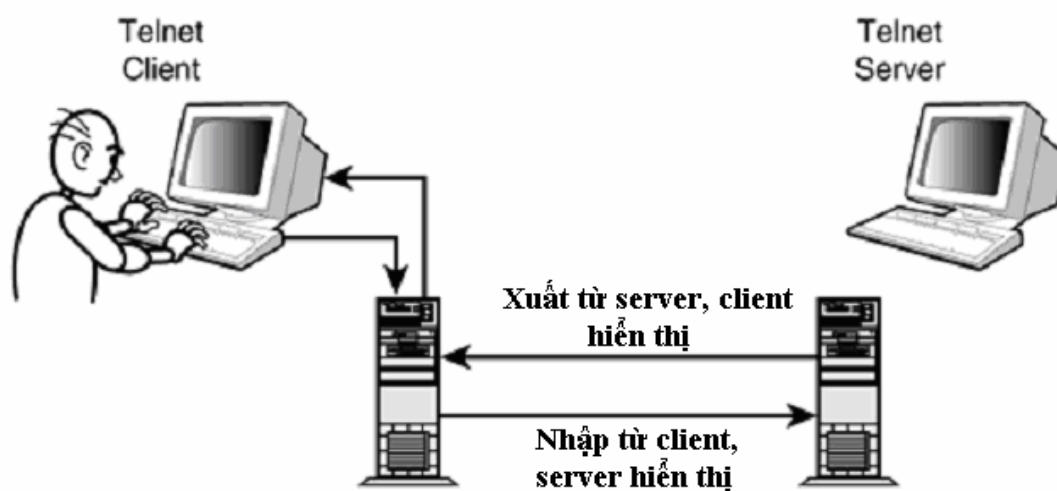
với `hostname` là tên của máy tính mà bạn muốn kết nối. (Bạn có thể nhập địa chỉ IP thay cho tên host) Lệnh này khởi động ứng dụng Telnet. Khi Telnet đang chạy, những lệnh bạn nhập vào sẽ chạy trên máy ở xa. Telnet cũng cung cấp một số lệnh đặc biệt mà bạn có thể sử dụng trong phiên làm việc Telnet như sau:

- `close` - Sử dụng lệnh này để đóng kết nối.
- `display` - Sử dụng lệnh này để hiển thị các thông tin kết nối, như là cổng hoặc các giả lập đầu cuối.
- `environ` - Sử dụng lệnh này để đặt các biến môi trường. Các biến môi trường sử dụng bởi hệ điều hành để cung cấp các thông tin riêng của người dùng hoặc các thông tin riêng của máy.
- `logout` - Sử dụng lệnh này để thoát và đóng kết nối.
- `mode` - Sử dụng lệnh này để bật tắt giữa hai chế độ chuyển tập tin giữa ASCII hoặc chế độ nhị phân.
- `open` - Sử dụng lệnh này để kết nối tới một máy tính ở xa.
- `quit` - Sử dụng lệnh này để thoát khỏi Telnet.
- `send` - Sử dụng lệnh này để gửi các chuỗi lệnh đặc biệt như chuỗi hủy bỏ, chuỗi dừng, hoặc chuỗi kết thúc tập tin.
- `set` - Sử dụng lệnh này để đặt các thông số kết nối.
- `unset` - Sử dụng lệnh này để hồi lại các tham số kết nối.

- ? - Sử dụng lệnh này để hiện thông tin trợ giúp.



Hình 11-1 Telnet server và client



Hình 11-2 Vào và ra mạng với Telnet

Trên các hệ thống có giao diện đồ họa như Microsoft Windows, một ứng dụng Telnet có thể có biểu tượng riêng của nó và chạy trên một cửa sổ, nhưng các lệnh và xử lý cũng giống như trong hệ thống chế độ văn bản.

Telnet thực sự hữu ích và là một công cụ quan trọng trên các mạng Unix. Một nhà quản trị hệ thống có thể sử dụng Telnet để thực hiện các tiến trình quản trị trên các máy ở xa. Một nhà quản trị có thể dùng một máy đơn và thông qua mạng truy cập các server để khởi động các tiến trình, xoá tập tin, tạo một thư mục mới, hoặc thống kê hệ thống. Vì một số lý do bảo mật nên có một số hạn chế trong việc sử dụng Telnet. Vấn đề nằm ở chỗ Telnet cung cấp cho những kẻ xâm nhập mạng một thứ nhiều hơn bất cứ gì chúng muốn đó là - truy cập trực tiếp vào một phiên làm việc đầu cuối trên một server ở xa. Một Telnet tiêu chuẩn hỗ trợ chứng thực mật khẩu, nhưng mật khẩu đánh vào được truyền dưới dạng văn bản không mã hoá. Bạn hầu như không bao giờ nhìn thấy Telnet sử dụng mở trên Internet mở và trên các mạng nội bộ đó là những nơi mà vấn đề bảo mật là rất quan trọng, Telnet thường được sử dụng với một số hạn chế như ai là người sử dụng và họ có thể làm gì với nó.

Thông tin thêm

Việc phát triển Mạng riêng ảo (Virtual Private Networks) đã đem đến cơ hội cho việc dùng Telnet trong mạng đã được bảo mật.

11.2 Tiện ích Berkeley

Hệ thống Berkeley (BSD) Unix, được biết đến với tên BSD Unix, là một bước phát triển lớn của UNIX. Rất nhiều cái mới đã bắt đầu với BSD Unix và bây giờ là chuẩn cho các hệ thống Unix khác, và đã được kết hợp với các hệ điều hành khác trong thế giới TCP/IP và Internet.

Một trong những đổi mới của BSD Unix là một tập nhỏ các tiện ích dòng lệnh được thiết kế cho việc truy cập từ xa trong hệ thống Unix. Tập các trình tiện ích này được gọi là các tiện ích Berkeley r* , bởi vì tên của mỗi tiện ích đều bắt đầu với r (remote). Các tiện ích Berkeley r* vẫn còn được dùng cho các hệ thống Unix, và các phiên bản của hầu hết các tiện ích r* được phân phối cho OpenVMS, Linux, Windows NT, Windows 2000, và các hệ điều hành khác. Mặc cho TCP/IP càng ngày càng phát triển rộng rãi, các tiện ích TCP/IP này vẫn không bị giảm phần quan tâm.

Một vài tiện ích Berkeley r* :

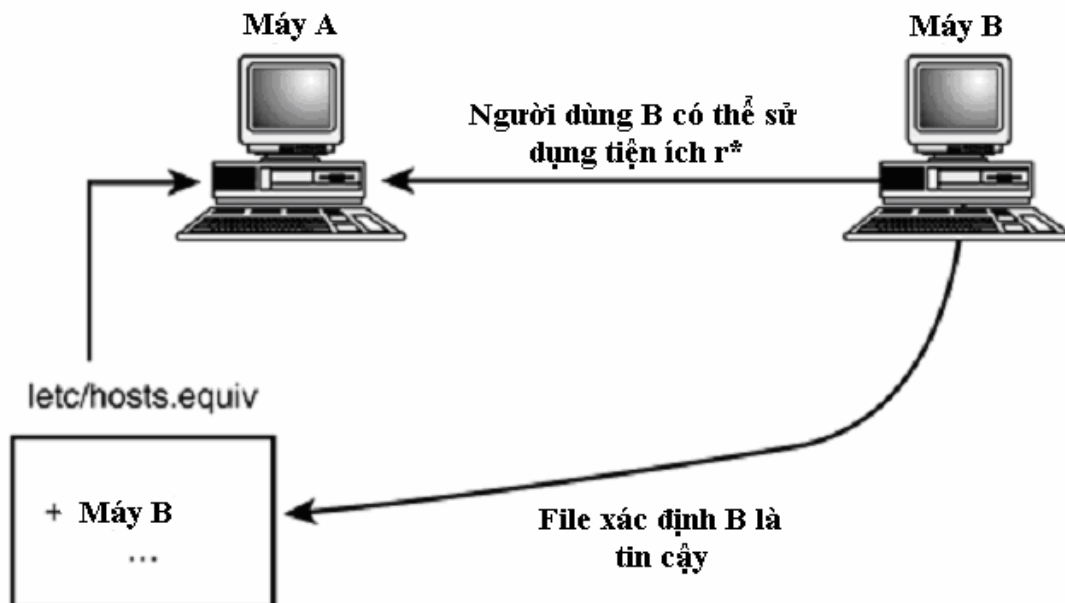
- **Rlogin**— Tiện ích này cho phép người dùng đăng nhập từ xa.
- **Rcp**— Tiện ích này cho phép việc truyền tập tin từ xa.
- **Rsh**— Tiện ích thực thi một lệnh từ xa thông qua daemon rshd.
- **Rexec**— Tiện ích thực thi một lệnh từ xa thông qua rexecd daemon.
- **Ruptime**— Tiện ích này hiển thị các thông tin hệ thống theo thời gian và số người dùng kết nối.
- **Rwho**— Tiện ích này hiển thị thông tin các người dùng đang kết nối.

Các tiện ích r^* được thiết kế vào một thời điểm phát triển ban đầu của mạng TCP/IP. Các người tạo ra các tiện ích này giả định rằng chỉ có những người tín nhiệm mới sử dụng các tiện ích này để truy cập. Ngày nay, rất nhiều nhà quản trị loại ra cái gọi là người dùng được tín nhiệm. Các tiện ích r^* được cho rằng quá nguy hiểm cho các mạng liên kết và mở ngày nay, bạn phải thật cẩn thận về cách nào và khi nào sử dụng các tiện ích này. Các tiện ích r^* đã có một số bước đầu phát triển bảo mật, đã được đo lường trong các môi trường tin cậy và hạn chế.

Thông tin thêm

Trong những năm gần đây, nhiều phiên bản bảo mật của một vài tiện ích r^* đã được phát triển để có những bảo mật cần thiết trong môi trường Internet. Ví dụ: Ssh là một ứng dụng bảo mật từ xa thay thế cho rsh và rlogin. Ssh dùng mã hoá cho việc chứng thực an toàn qua các mạng.

Các tiện ích r^* sử dụng một khái niệm là truy cập tin cậy. Truy cập tin cậy cho phép một máy tính tin vào một chứng thực của máy khác. Trong **hình 11.3**, nếu một máy A coi máy B là một máy tin cậy, người dùng có thể đăng nhập vào máy B và có thể sử dụng các tiện ích r^* để truy cập vào máy A mà không cần mật khẩu. Máy A cũng có thể chỉ định các người dùng cụ thể nào là tin cậy. Các host và các người dùng tin cậy được nhận dạng trong tập tin `/etc/hosts.equiv` của máy ở xa nơi mà người dùng muốn truy cập. Tập tin `.rhosts` trong mỗi thư mục gốc của người dùng có thể được sử dụng cho việc chứng thực tài khoản người dùng.



Hình 11-3 Tiến trình truy cập tin cậy trên Unix

Thông tin thêm

Bởi vì tập tin `/etc/hosts.equiv` và `.rhosts` cho phép truy cập các tài nguyên hệ thống, nên chúng có thể là mục tiêu tấn công chính cho các hacker. Khả năng có thể bị xâm hại của tập tin `hosts.equiv` và `.rhosts` là lý do tại sao các tiện ích `r*` không được cho là an toàn nữa.

Sau đây, chúng ta sẽ nghiên cứu một vài tiện ích Berkeley `r*`.

Rlogin

Rlogin là tiện ích đăng nhập từ xa. Bạn có thể sử dụng `rlogin` để kết nối với các Unixhost đang chạy server daemon `rlogind` (d viết tắt của daemon). Rlogin phục vụ cùng mục đích như Telnet, nhưng `rlogin` được cho là ít linh hoạt hơn. Rlogin được thiết kế đặc biệt để cung cấp truy cập cho các hệ thống Unix, trong khi Telnet sử dụng trên một tiêu chuẩn TCP/IP và có nhiều ứng dụng hơn. Rlogin cũng không cung cấp một vài đặt tính thương lượng cấu hình như Telnet.

Một tính chất đáng chú ý của `rlogin` là nó hỗ trợ đăng nhập từ xa mà không cần mật khẩu. Truy cập không mật khẩu là một tính chất chung của tất cả tiện ích `r*`, nhưng một vài người dùng cho rằng các phiên làm việc không mật khẩu hơi bất ổn hơn một vài chức năng khác hiện có của các tiện ích `r*`. Tuy nhiên, mô hình bảo mật của các tiện ích `r*` làm giới hạn truy cập tới các người dùng được tin nhiệm.

Thông tin thêm

Một điều quan trọng cần ghi nhớ là các hệ điều hành mạng như NetWare và Windows NT/2000 cũng cung cấp một số truy cập mạng không cần mật khẩu sau khi người dùng đã có một số chứng thực ban đầu. Hiện nay rất nhiều thuận lợi của các tiện ích `r*` có thể có được qua những phương pháp khác an toàn hơn.

Câu lệnh của `rlogin` như sau:

```
rlogin hostname
```

Với `hostname` là tên host của máy tính bạn muốn truy cập. Nếu không có username, username mặc định là username của người dùng trên máy cục bộ. Ngược lại, bạn có thể chỉ ra username như sau:

```
rlogin hostname -l username
```

`username` là tên người dùng bạn muốn sử dụng để đăng nhập

Server daemon `rlogind`, phải được chạy trên máy server, sau đó kiểm tra các tập tin `host.equiv` và `.rhosts` để kiểm tra thông tin về host và người dùng. Nếu quá trình chứng thực này thành công, phiên làm việc từ xa sẽ bắt đầu.

Rcp

Rcp cung cấp truy cập tập tin từ xa với hệ thống Unix. Rcp không được sử dụng rộng rãi như FTP, nhưng đôi khi nó được sử dụng để truyền tập tin trên Unix.

Rsh

Rsh cho phép bạn thực hiện một lệnh đơn trên một máy ở xa mà không cần đăng nhập vào máy ở xa. Rsh là một dạng thu gọn của shell từ xa. (Một shell là bộ giao tiếp lệnh với hệ điều hành.) `rshd` daemon chạy trên máy ở xa, chấp nhận các lệnh `rsh` kiểm tra thông tin tên host và người dùng, và thực thi câu lệnh. Rsh hữu ích khi bạn muốn nhập một lệnh và không muốn thiết lập một phiên làm việc đầu cuối với máy tính ở xa.

Khuôn dạng của lệnh `rsh` là

```
rsh -l username hostname command
```

Ở đây `hostname` là tên host của máy ở xa, `username` là tên sử dụng khi truy cập máy ở xa, và `command` là lệnh bạn muốn thực hiện.

Tên người dùng (đứng sau `-l`) là thông số tùy chọn. Nếu bạn không nhập vào tên người dùng thì nó mặc định lấy tên máy tính cục bộ và dòng lệnh như sau:

```
rsh hostname command
```

Rexec

Rexec giống như `rsh` nó ra lệnh cho máy tính ở xa thực thi một lệnh. Rexec sử dụng `rexecd` daemon.

Cấu trúc của đoạn lệnh `reexec` như sau:

```
reexec hostname -l username command
```

`hostname` là tên host của máy ở xa, `username` là tên tài khoản người dùng trên máy ở xa, và `command` là lệnh bạn muốn thực hiện. Tên người dùng (đứng sau `-l`) là thông số tùy chọn. Nếu bạn không nhập vào tên người dùng thì nó mặc định lấy tên người dùng trên máy cục bộ.

Ruptime

Ruptime hiển thị tóm tắt có bao nhiêu người dùng đăng nhập vào mỗi máy tính trên mạng. Ruptime cũng hiển thị danh sách bao lâu mỗi máy tính này hoạt động—do đó nó có tên `r-up-time`—và hiển thị thêm các thông tin về hệ thống.

Để tạo ra báo cáo ruptime bạn cần nhập vào

```
ruptime
```

Cả hai `ruptime` và `rwho` (xem trong phần tới) sử dụng `rwhod` daemon. Thật ra, mỗi máy tính trên mạng có một `rwhod` daemon thực hiện broadcast thường xuyên các báo cáo về hoạt động của người dùng. Mỗi `rwhod` daemon nhận và lưu trữ các báo cáo từ một `rwhod` daemon khác nhằm có tầm nhìn bao quát mạng về các hoạt động của người dùng.

Rwho

`Rwho` báo cáo về tất cả người dùng hiện đang đăng nhập vào các máy tính trên mạng. `Rwho` liệt kê danh sách các tên người dùng, máy tính mà mỗi người dùng đăng nhập vào, thời gian đăng nhập và thời gian thoát khỏi từ khi đăng nhập.

Cấu trúc của lệnh `rwho` rất đơn giản

```
rwho
```

Mặc định thì nó chỉ báo cáo các người dùng trong phạm vi một giờ. Để có một báo cáo về tất cả người dùng sử dụng thông số -a :

```
rwho -a
```

Giống như `ruptime`, `rwho` sử dụng `rshod` daemon.

11.3 Các hướng mới trong việc truy cập từ xa

Như các bạn đã học trong chương này, các tiện ích truy cập từ xa TCP/IP cũ như Telnet và các công cụ `r*` không an toàn trong môi trường mạng. Tiện ích `r*` biến mất khá nhanh. Telnet được dùng trong một số ứng dụng hạn chế- như là truy cập dial-up và quản trị từ xa trong mạng đã được bảo vệ - nhưng hầu hết các chuyên gia công nghệ thông tin không nghĩ sẽ sử dụng Telnet cho các mạng mở Internet. Tại thời điểm này, sự xuất hiện các công cụ quản trị với giao diện đồ họa GUI đã làm giảm địa vị thống trị của các tiện ích dựa trên văn bản như là Telnet.

Các nhà quản trị mạng bắt đầu sử dụng các công cụ truy cập từ xa dưới đây:

- Ssh (shell bảo mật) và các tiện ích shell khác có khả năng mã hoá để đảm bảo sự an toàn cao hơn.
- Công cụ Screen-sharing, như là Timbuktu của Netopia và pcAnywhere của Symantec, cho phép người dùng có khả năng xem và điều khiển các máy ở xa.
- Các công cụ quản trị từ xa thương mại với những đặt tính kết nối mạng sẵn và bảo mật.

Cũng giống như Telnet, các công cụ screen-sharing và rất nhiều các chương trình truy cập từ xa khác vẫn không đủ an toàn để sử dụng trong môi trường không được bảo vệ như Internet. Một lớp mới các công cụ đã, phát triển và đưa ra mạng riêng ảo (**VPN**). VPN đưa ra một kết nối điểm điểm được mã hóa từ người dùng đến mạng ở xa. Kết nối này đôi khi được gọi là một đường ống (tunnel) vì nó cho phép người dùng ở xa làm việc giống như đứng trong mạng nội bộ. Khi một đường ống được mở, người dùng có thể an toàn sử dụng các tiện ích.

Tóm tắt

Chương này bao gồm một số các tiện ích truy cập từ xa dựa trên TCP/IP. Bạn đã học về Telnet và các tiện ích r*. Bạn cũng có thể sử dụng các tiện ích này để thực thi các lệnh và truy cập các thông tin trên các máy ở xa.

CHƯƠNG HTTP, HTML VÀ

12 WORL WIDE WEB

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **HTTP and HTML**
- **URLs**
- **Các kỹ thuật Web tiên tiến**

World Wide Web bắt đầu như là một cơ cấu hiển thị đồ họa phổ biến Internet. Từ lúc khởi đầu, Web đã có ảnh hưởng lớn tới những nhận thức chung về Internet, và đã làm đổi mới cách chúng ta nghĩ về các giao diện ứng dụng. Chương này giới thiệu về HTTP, HTML, và Web.

Kết thúc chương này bạn sẽ có thể :

- Chỉ ra cách làm việc của World Wide Web
- Mô tả các URL và trình bày rõ ràng các URL riêng của bạn
- Xây dựng một trang Web cơ bản bằng cách sử dụng text và các thẻ HTML
- Thảo luận giao thức HTTP và mô tả cách làm việc của nó
- Liệt kê các thuận lợi của server và các client đầu cuối.

12.1 World Wide Web là gì?

Trang web mà bạn nhìn thấy qua cửa sổ của trình duyệt Web là kết quả hội thoại giữa trình duyệt và Web server. Giao thức được sử dụng cho quá trình hội thoại trên được gọi là Hypertext Transfer Protocol (HTTP). Dữ liệu từ server được chuyển tới client là một mớ lộn xộn gồm nhiều văn bản, hình ảnh, địa chỉ và các mã định dạng hình thành một tài liệu hợp nhất nhờ một ngôn ngữ định dạng linh hoạt được gọi là ngôn ngữ đánh dấu siêu văn bản HTML

Về mặt khái niệm HTML tương tự một định dạng xử lý văn bản. Thật ra, cách tốt nhất để bắt đầu tìm hiểu về HTML là xem xét đến cách thức các tài liệu xử lý văn bản được hình thành như thế nào. Các chuyên gia đã luôn thừa nhận sự cần thiết của việc lưu trữ và chuyển giao thông tin được viết bằng ngôn ngữ của con người (tiếng Anh, tiếng Nga hoặc tiếng Pháp). Do đó, các chiến lược nhanh chóng được đưa ra nhằm lưu trữ và thể hiện hệ thống ký tự chữ cái và số một cách hiệu quả. Ở Mỹ, người ta dùng chuẩn ASCII để mã hóa mỗi ký tự và số (và nhiều ký hiệu văn bản) thành một mẫu bit. Các tập tin văn bản ASCII được dùng xuyên suốt thế giới tính toán trong các tập tin cấu hình, các tài liệu trợ giúp trực tuyến, và các thông điệp thư điện tử. Các tập tin văn bản vẫn là một đặc trưng quan trọng trong các hệ điều hành Unix/Linux. Ở khía cạnh nào đó, công nghệ máy tính phát triển nhanh chóng đã bắt đầu kết hợp sự phát triển nhanh chóng của công nghệ xử lý văn bản. Đối với các tài liệu in ấn chuyên nghiệp, các nhà sản xuất thiết bị cần có một cách thức để đưa sự định dạng in ấn vào trong các tập tin văn bản. Người ta có thể tạo một tiêu đề nhỏ đầu dòng cho định dạng in đậm, thay đổi lề văn bản hoặc thay đổi một font chữ khác hay không? Các nhà sản xuất đã phát triển các hệ thống số (nhiều hệ thống thuộc sở hữu riêng) để mã hóa thông tin định dạng thành một tài liệu dạng văn bản. Một vài hệ thống này dùng mã ASCII. Một số khác sử dụng các bộ đánh số khác để biểu thị thông tin định dạng.

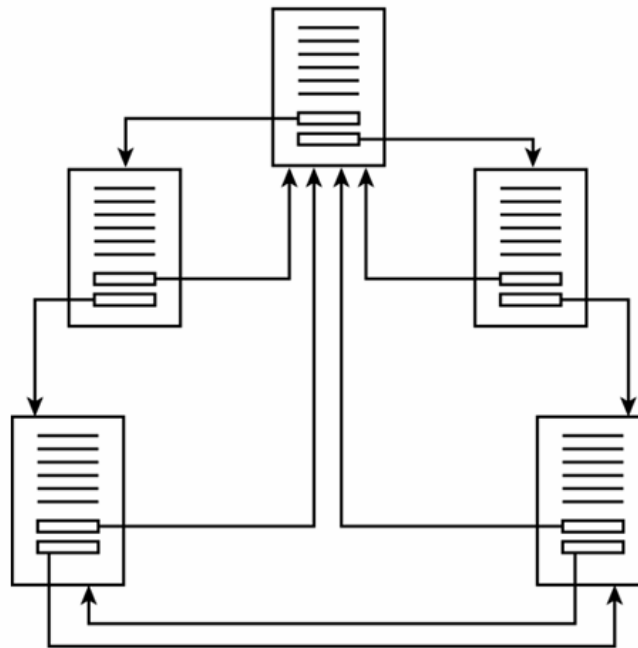
Thông tin thêm

Dĩ nhiên, các hệ thống mã định dạng này chỉ hoạt động được nếu ứng dụng tạo ra tài liệu và các ứng dụng đọc tài liệu cùng thống nhất về cách mã hoá.

Các hệ thống xử lý từ này ngày càng trở nên tinh vi. Vài hệ thống phát triển khả năng tham khảo đến một tập tin khác, ví dụ một hình vẽ, mà sau đó sẽ xuất hiện trong văn bản khi tài liệu này được thể hiện trên màn hình hoặc được in ra trên giấy.

Các nhà sáng tạo ra HTML muốn phát triển một hệ thống độc lập với nhà sản xuất và phổ biến để mã hóa thông tin định dạng. Họ muốn không chỉ có các mã sắp xếp chữ mà còn phải có các hình ảnh và thông tin về cách trình bày. Và họ đã bổ sung thêm một phương pháp mới mà đã trở thành một đặt trưng quan trọng và mạnh của định dạng mới này, đó là liên kết siêu văn bản (hypertext link).

Một liên kết là một đoạn của văn bản, hoặc chỉ là một miền của màn hình, mà làm cho trình duyệt mở một trang mới hoặc di chuyển tới một phần khác của trang. Các liên kết cho phép người đọc xem thông tin trực tuyến. Người đọc có thể chọn hoặc không chọn liên kết tới một trang khác với thông tin bổ sung. Tài liệu HTML có thể được tập hợp thành các hệ thống hợp nhất bao gồm các trang và các liên kết (xem **hình 12.1**). Một người xem có thể tìm một đường dẫn khác tới dữ liệu, phụ thuộc cách người xem đi theo các liên kết. Liên kết có thể chỉ đến một tài liệu HTML khác trong cùng một thư mục, trên một thư mục khác, hoặc ngay cả một tài liệu trên máy tính khác. Liên kết có thể dẫn đến một Website hoàn toàn khác trên một máy tính khác.



Hình 12-1 Một Web site là một hệ thống hợp nhất giữa trang và các liên kết

Bên trong mã HTML, liên kết là một dạng địa chỉ đặt biệt được gọi định vị tài nguyên đồng dạng (URL). Hầu hết các dạng của URL được kết hợp với Web như ví dụ sau:

<http://www.dobro.com>

URL là giao thức sử dụng để truy cập một tài nguyên và tên DNS của Web server. Ví dụ này dễ dàng cho bất cứ ai đã từng làm việc với một trình duyệt Web. Người ta cũng thường thấy một đường dẫn và tên tập tin được gắn vào URL:

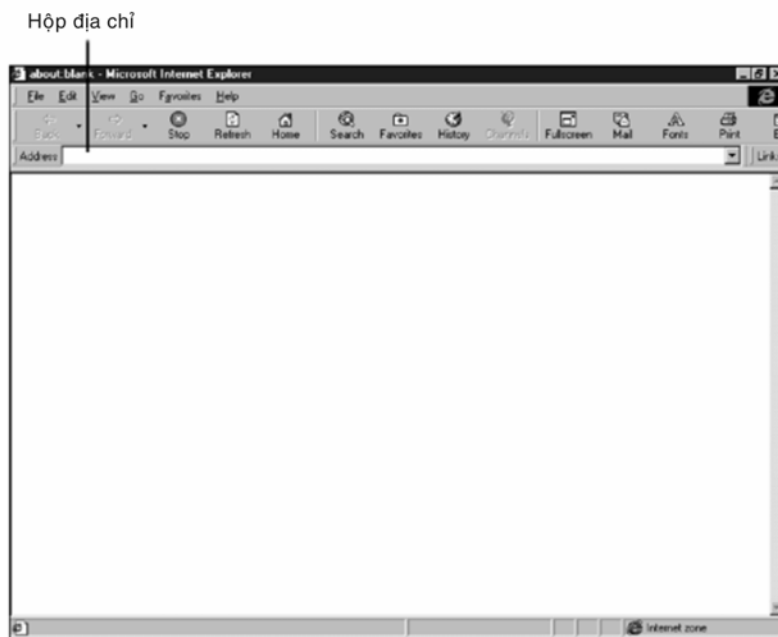
<http://www.dobro.com/techniques/repair/fix.html>

URL thậm chí có thể truyền một nhóm của các tham số bổ sung. Bạn thỉnh thoảng thấy một URL dài và phức tạp với các tham số bổ sung trong hộp địa chỉ của cửa sổ trình duyệt sau khi bạn truy cập một trang Web thông qua một trong các cơ chế tìm kiếm trên Internet. Bạn sẽ nghiên cứu nhiều về dạng tổng quan của các URL trong phần tiếp theo.

Thông tin thêm

Bạn có lẽ đã chú ý đến URL của một site điển hình (như là www.whitehouse.gov) bao gồm chỉ là một tên miền DNS và dường như không tham chiếu đến một tên tập tin. Nếu tên tập tin không được định rõ, trình duyệt tự động mở một tên tập tin mặc định được định nghĩa bởi Web server.

Một trình duyệt Web lướt qua các trang web các URL. Bạn truy cập một trang Web bằng cách nhập URL của trang đó trong hộp địa chỉ của cửa sổ trình duyệt (xem **hình 12.2**). Khi bạn kích một liên kết, trình duyệt mở trang Web được định rõ trong liên kết theo URL của liên kết đó.



Hình 12-2 Nhập URL trong hộp địa chỉ của trình duyệt window

Tóm lại một tài liệu HTML bao gồm tổ hợp nào đó của các mục sau:

- Văn bản
- Hình ảnh
- Các mã định dạng văn bản(phôn chữ và trình bày thông tin)
- Tham chiếu đến các tập tin thứ cấp chẳng hạn như các tập tin hình ảnh

- Các liên kết đến các tài liệu HTML khác hoặc các vị trí khác trong tài liệu hiện tại

Để mở một Web site, người sử dụng nhập URL của Web site trong cửa sổ trình duyệt Web. Trình duyệt bắt đầu kết nối tới Web server được định rõ trong URL. Server gửi dữ liệu HTML qua mạng tới trình duyệt Web. Trình duyệt Web tập hợp lại dữ liệu HTML, hình ảnh trang web thể hiện trong cửa sổ trình duyệt. Các phần tiếp theo sau đây sẽ thảo luận quy trình này một cách chi tiết hơn. Dĩ nhiên, quy trình này gần đây có sự phức tạp hơn do có một số đặc tính mới như HTML có kịch bản và động. ta cũng sẽ nghiên cứu về các đặc tính mới này.

12.2 Khảo sát kỹ hơn về URL

Ngày nay các URL thì quá phổ biến đến nỗi chúng xuất hiện trong các chương trình quảng cáo trên TV và trên các túi bọc nilon mà không cần phải giải thích gì thêm. Nhưng các URL trang chủ mà bạn thấy trên các phương tiện thông tin đại chúng chỉ là một tập nhỏ của nhiều chọn lựa có trong dạng thức linh hoạt này.

Không phải tất cả URL có liên quan đến HTTP. Trong thực tế, dạng URL được phát minh ra như là một phương thức chung cho nhiều giao thức Internet khác nhau. Phần giao thức của URL được xem như là một lược đồ. Lược đồ nhận dạng một giao thức và vì thế nó giải thích phần còn lại của URL cho máy tính. Định dạng chung cho một URL được mô tả trong RFC 1738, như

`<scheme>:<scheme-specific-part>`

Bảng 12.1 thể hiện một vài chọn lựa lược đồ được định nghĩa trong RFC 1738. Các lược đồ khác cũng được miêu tả. trong thực tế nhiều lược đồ mới đã được bổ sung trong các RFC sau này.

Bảng 12-1 Lược đồ URL

Lược đồ	Mô tả
ftp	Giao thức truyền Tập tin
http	Giao thức truyền siêu văn bản
gopher	Giao thức Gopher
mailto	Thư điện tử
News	Tin Usenet
nntp	Tin Usenet với truy cập NNTP
telnet	Phiên tương tác (xem Chương 11 , “ <i>Các tiện ích truy cập từ xa</i> ”)

Lược đồ	Mô tả
waiss	Các server thông tin vùng rộng
file	Các tên tập trên host cụ thể

Như thuật ngữ `<protocol-specific-part>` dạng chung của URL biểu thị trong phần sau, cấu trúc của URL có thể khác nhau, phụ thuộc vào lược đồ của URL. Máy tính trước tiên đọc lược đồ, và lược đồ giải thích cho máy tính cách để dịch phần còn lại của URL.

Phần này tập trung vào HTTP, đoạn này tập trung chính các dạng HTTP của URL. Nhưng cần chú ý rằng, bạn cũng sẽ bắt gặp các lược đồ khác khi bạn duyệt Web. Lược đồ ftp là biến thể phổ biến khác. Nhiều trình Web hiện đại có khả năng nhận ra luân phiên các lược đồ như ftp và trả lời tới URL phù hợp.

Dạng chung cho một HTTP URL mới đây

```
http://<host>[:<port>]/<path>[;<parameters>][?<search>]
```

`<host>` là tên máy chủ DNS (ví dụ như `www.dobro.com`), và `<path>` là đường dẫn tới tài liệu HTML hoặc tài nguyên khác. Các sự lựa chọn khác thì không phổ biến và không ít quen thuộc với user thông thường. Các lựa chọn này bao gồm

- `<port>`— Số cổng của daemon hoặc dịch vụ của trình duyệt đang kết nối. (Xem *chương 5, "Lớp vận chuyển,"* để biết thêm thông tin về số cổng.) Số cổng dành riêng cho dịch vụ HTTP là cổng TCP 80. Nếu phần số cổng không chỉ rõ, thì cổng 80 được sử dụng mặc định.
- `<parameters>`— Các tham số lựa chọn được cung cấp bởi client. Người dùng hầu như không bao giờ nhập các tham số để truy cập một Web site. Tuy nhiên, đôi khi các thông số được chuyển đến server thông qua các kịch bản.
- `<search>`— Cho phép client gửi một truy vấn tới người dùng. Người dùng hầu hết không bao giờ nhập một truy vấn vào trong URL bằng tay. Kiểm tra hộp URL từ trình duyệt của bạn khi bạn chọn một sự tìm kiếm qua một trong các cơ chế tìm kiếm trên Internet. Bạn có thể thấy một chuỗi truy vấn được chuyển tới server tìm kiếm qua URL.

Thông tin thêm

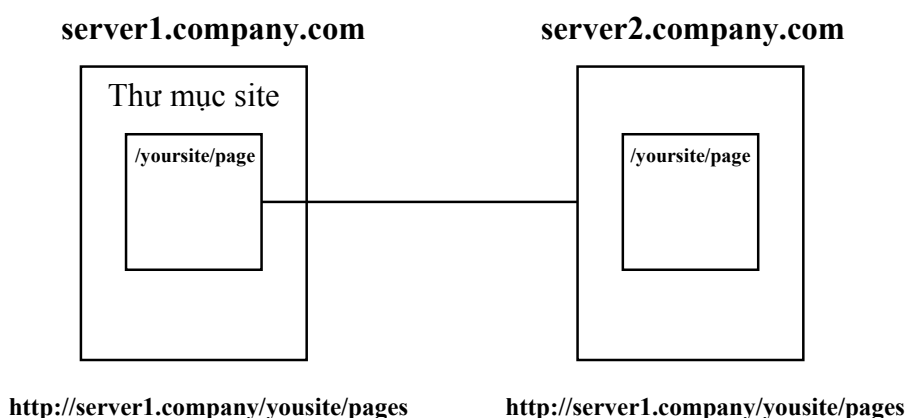
Các URL phức tạp bao gồm các cổng, các tham số, và các truy vấn thỉnh thoảng được sử dụng để sửa đổi định cấu hình cho bản thân Web server. Web server cần có các sự mở rộng cần thiết và tập lệnh để xử lý yêu cầu cấu hình.

Nếu một kết nối đã thiết lập rồi, thì không cần thiết sử dụng toàn bộ URL để nhận dạng tài nguyên. HTTP và RFC 1738 cho phép sử dụng một URL tương đối. URL tương đối cho phép tham khảo từ trang hiện hành hoặc từ một vị trí mặc định (<BASE>) định nghĩa trong tài liệu. Ví dụ, nếu bạn hiện đang ở trang chủ tham khảo đến tập tin fix.html tại vị trí URL `http://www.dobro.com`, URL tương đối của

`http://www.dobro.com/techniques/repair/fix.html`

là `techniques/repair/fix.html`.

URL tương đối có vẻ như một cách thức dễ gây nhầm lẫn mà chỉ để tiết kiệm một vài bit và vài ký tự nhập vào, nhưng nó tạo các thuận lợi trong việc xây dựng và phát triển Web site. Như trong **hình 12.3**, nếu Web chủ sử dụng các URL tương đối cho các liên kết nội bộ trong một Web site, toàn bộ cấu trúc thư mục cho site có thể được copy tới một server khác mà không phá vỡ tính toàn vẹn của các liên kết.



Hình 12-3 Các URL tương đối tạo khả năng di động cho Website

12.3 HTML

HTML là vùng tải tin được truyền thông qua các quá trình xử lý của HTTP. Như bạn đã nghiên cứu trong phần trước, một tài liệu HTML bao gồm văn bản, mã định dạng, các tham chiếu tới các tập tin khác, và các liên kết. Khi bạn duyệt qua nội dung của một tài liệu HTML sử dụng một ứng dụng xử lý văn bản như Notepad của Windows hoặc vi của Unix, bạn sẽ thấy tài liệu này thực ra là một tập tin văn bản đơn thuần. Tập tin này chứa bất kỳ văn bản nào sẽ xuất hiện trong trang Web, và nó cũng bao gồm một số các mã HTML đặc biệt được gọi là các thẻ. Các thẻ là các lệnh cho trình duyệt. Các thẻ không được xuất hiện trên trang Web, nhưng chúng tác động vào cách hiển thị của dữ liệu và cách trang Web ứng xử. Các thẻ HTML cung cấp tất cả loại định dạng, các

tham khảo tập tin, và các liên kết kết hợp với một trang Web. Một vài thẻ HTML quan trọng thể hiện trong bản sau.

Bảng 12-2 Một vài thẻ HTML quan trọng

Thẻ	Mô tả
<HTML>	Đánh dấu đoạn bắt đầu và kết thúc của nội dung đoạn HTML trong tập tin.
<HEAD>	Đánh dấu phần bắt đầu và kết thúc của phần tiêu đề.
<BODY>	Đánh dấu phần bắt đầu và kết thúc của phần thân, mô tả đoạn văn sẽ xuất hiện trong cửa sổ trình duyệt..
<H1>, <H2>, <H3>, <H4>, <H5>, và <H6>	Đánh dấu phần bắt đầu và kết thúc của một đề mục nhỏ. Mỗi thẻ heading trình bày một mức đề mục khác nhau. <H1> là mức cao nhất.
	Đánh dấu phần đầu và kết thúc của đoạn văn bản có nét đậm.
<U>	Đánh dấu phần bắt đầu và kết thúc của một đoạn văn bản được gạch dưới.
<I>	Đánh dấu phần bắt đầu và kết thúc của một đoạn văn bản có nét nghiêng.
	Đánh dấu phần bắt đầu và kết thúc của một đoạn của văn bản với các đặt tính font chữ đặc biệt. Xem bảng 12.3 một vài thuộc tính font có sẵn.
<A>	Đánh dấu phần bắt đầu và kết thúc của một liên kết siêu văn bản. Liên kết đích URL xuất hiện bên trong thẻ <A> đầu tiên với một giá trị cho thuộc tính HREF (được mô tả trong phần sau).
	Chỉ ra một tập tin hình ảnh sẽ xuất hiện trong văn bản. URL của tập tin xuất hiện trong thẻ là một giá trị cho thuộc tính SRC.

Các thẻ áp dụng cho một khối của văn bản. Thẻ xuất hiện ở phần đầu và phần kết thúc của khối. Thẻ kết thúc của khối có dấu gạch chéo (/) để báo hiệu đây là một kết thúc. Ví dụ:

```
<H1>Dewey Defeats Truman</H1>
```

Một tài liệu HTML bắt đầu với một khai báo <!DOCTYPE>. !DOCTYPE định nghĩa phiên bản của HTML được sử dụng trong tài liệu. Với HTML 4.0, lệnh !DOCTYPE là:

```
<!DOCTYPE HTML PUBLIC "-//W3C/DTD HTML 4.0//EN">
```

Hầu hết các trình duyệt không đòi hỏi khai báo !DOCTYPE (các trang web sử dụng các phần mở rộng đặc biệt này của trình duyệt có thể dư ra một kiểu tài liệu khác), và nhiều hướng dẫn HTML thậm chí không đề cập đến !DOCTYPE.

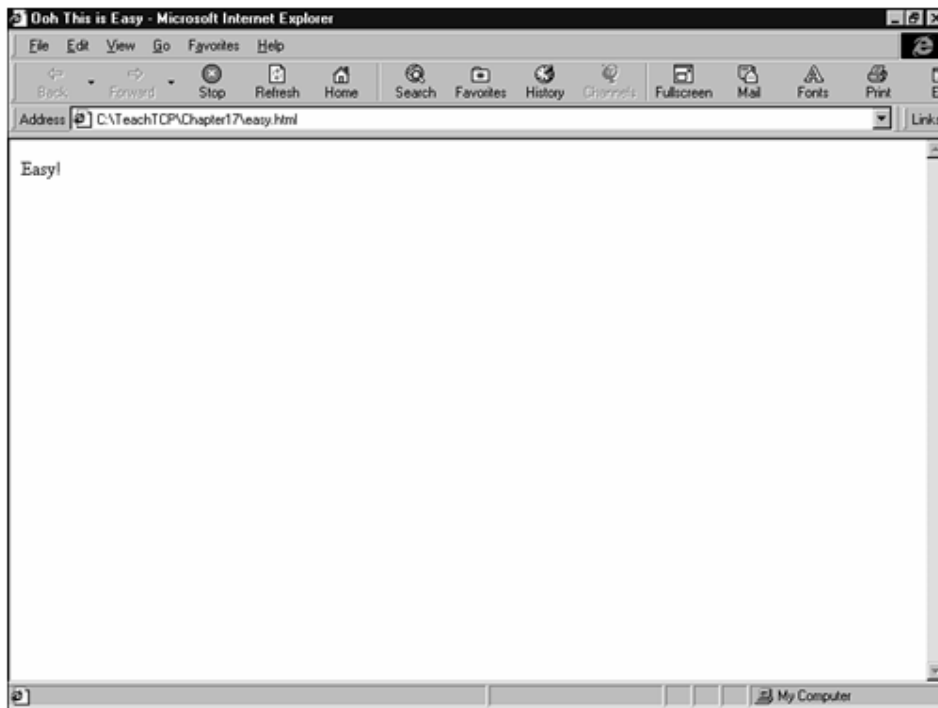
Sau phát biểu !DOCTYPE là thẻ <HTML>. Những phần còn lại của tài liệu thì được kèm giữa thẻ <HTML> và thẻ </HTML> ở phần kết thúc của tập tin. Bên trong các thẻ bắt đầu và kết thúc <HTML>, tài liệu được tách ra làm hai phần sau:

- Đoạn đầu (kẹp giữa các thẻ <HEAD> và </HEAD>) bao gồm thông tin về tài liệu. Thông tin trong phần đầu này không được thể hiện trên trang Web thẻ <TITLE> (nằm giữa 2 thẻ HEAD) chỉ ra một nhan đề sẽ xuất hiện trong thanh nhan đề của cửa sổ trình duyệt: <TITLE>. <TITLE> là một thành phần bắt buộc. Các thành phần khác của phần <HEAD> là tùy chọn. Ví dụ thẻ <STYLE> (thông tin về loại tài liệu) là tùy chọn
- Phần thân kẹp giữa 2 thẻ <BODY> và </BODY> là văn bản thực sự xuất hiện trên trang Web và bất cứ HTML nào có liên quan đến văn bản đó.

Ví dụ về tài liệu HTML đơn giản:

```
<!DOCTYPE HTML PUBLIC "-//W3C/DTD HTML 4.0//EN">
<HTML>
<HEAD>
<TITLE> Ooh This is Easy </TITLE>
</HEAD>
<BODY>
Easy!
</BODY>
<HTML>
```

Nếu ta lưu tập tin HTML này dưới dạng tập tin văn bản và sau đó mở tập tin này với một trình duyệt Web, Easy! sẽ xuất hiện trong cửa sổ trình duyệt. Thanh nhan đề sẽ có nhan đề “Ooh This is Easy” (Xem **hình 12.4**).



Hình 12-4 Một ví dụ về trang Web đơn giản

Bạn có thể bổ sung thêm vào trang Web với phần văn bản thêm vào và định dạng trong phần body. Ví dụ sau thêm thẻ <H1> và <H2> cho headings, thẻ <P> cho một đoạn, thẻ cho chữ có nét đậm, thẻ <I> cho kiểu chữ nghiêng, và thẻ thông tin font cho kiểu chữ. Chú ý thẻ bao gồm một thuộc tính. Thuộc tính là các tham số kèm bên trong thẻ cung cấp thông tin thêm. Xem *bảng 12-3* cho các thuộc tính khác nhau.

```
<!DOCTYPE HTML PUBLIC "-//W3C/DTD HTML 4.0//EN">
<HTML>
<HEAD>
<TITLE> Ooh This is Easy </TITLE>
</HEAD>
<BODY>
<H1>The Easy and Hard of HTML</H1>
<P><U>Webster's Dictionary</U> defines HTML as <I>"a small snail
found originally in the Archipelago of Parakeets." I borrow from this
theme in my consideration of HTML.</P><H2>HTML is Easy</H2>
<P>HTML is easy to learn and use because everyone reacts to it
energetically. You can walk into a bar and start speaking HTML, and
the man beside you will <B>happily</B> tell you his many
accomplishments.</P>
<H2>HTML is Hard</H2>
```



```

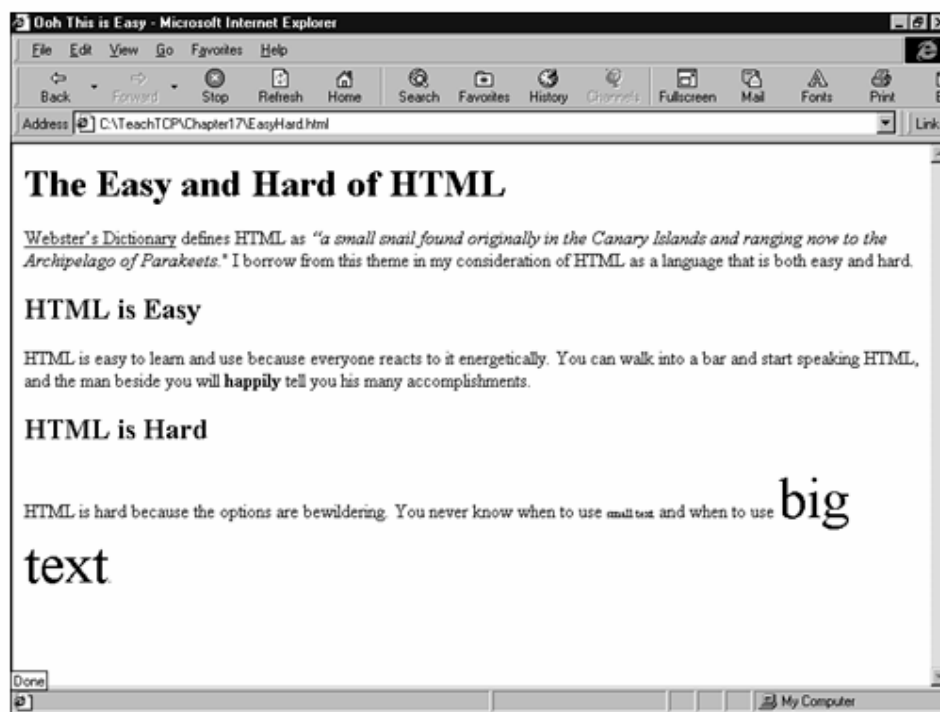
<P>HTML is hard because the options are bewildering. You never know
when to use <FONT SIZE=1>small text</FONT> and when to use <FONT
SIZE=7>big text</FONT>.</P>

</BODY>

</HTML>

```

Ví dụ thể hiện trong trình duyệt như *hình 12.5*.



Hình 12-5 Mở rộng ví dụ easy!

**Bảng 12-3 Các thuộc tính thẻ **

<i>Attribute</i>	<i>Description</i>
SIZE	Thiết lập kích cỡ font chữ. Giá trị biến đổi từ 1 đến 7: .
LANG	Mã ngôn ngữ chỉ rõ ngôn ngữ được sử dụng trong văn bản.
FACE	Thiết lập loại font chữ: .
COLOR	Màu của chữ trong văn bản: .

Như ta đã nghiên cứu trong phần trước, liên kết siêu văn bản là một thành phần vô cùng quan trọng cho việc thiết kế Web. Một liên kết là một tham chiếu đến một tài liệu khác hoặc một phần khác của tài liệu hiện hành. Nếu user kích lên đoạn được tô sáng của liên kết trên văn bản, trình duyệt ngay lập tức mở tài liệu được tham chiếu trong liên kết. Kết quả là người dùng lướt đi nhịp nhàng qua một khu vườn vô tận với những nội dung mang nhiều thông tin và đầy màu sắc.

Thông tin thêm

Một liên kết xuất hiện trong tập tin HTML dưới dạng là một thẻ. Dạng ngắn gọn nhất của một liên kết sử dụng thẻ <A> với URL của đích liên kết là một giá trị cho thuộc tính HREF. Cho ví dụ, trong ví dụ trước, nếu ta muốn các từ "Archipelago of Parakeets" xuất hiện như một siêu văn bản với một liên kết tới một Web site về quần đảo, thì ta đóng các từ này bên trong các thẻ <A> như sau:

```
originally in the <A HREF=http://www.ArchipelagoParakeets.com> Archipelago of  
Parakeets </A>. I borrow from this theme
```

Định dạng HTML linh hoạt này bao gồm nhiều tùy chọn bổ sung mà ta không thể đề cập hết trong giới thiệu vắn tắt này. Bạn có thể đặt một liên kết bên trong một bức hình. Bạn có thể tạo ra các trang có phong cách riêng của mình bằng các thẻ đặc biệt cho các kiểu đoạn văn được định dạng trước. Bạn có thể cấu trúc trang Web với các bảng biểu, các cột, các khuôn dạng và các khung. Hoặc bạn có thể thêm các nút vô tuyến, các hộp kiểm tra và các trình đơn kéo xuống. Vào thời kỳ đầu của HTML, các nhà thiết kế sử dụng các trình soạn thảo văn bản để viết mã HTML trực tiếp vào tài liệu của họ (như trong ví dụ trước). Hiện nay các nhà thiết kế Web chuyên nghiệp làm việc với các ứng dụng phát triển web đặc biệt, như Dreamweaver hoặc FrontPage. Các ứng dụng này giúp cho các nhà thiết kế không phải bận tâm về các chi tiết của HTML và cho phép họ thấy trước được các trang web mà sẽ xuất hiện trước người dùng trong quá trình thiết kế.

12.4 HTTP

Như đã đề cập trong phần trước, các web server và các trình duyệt thông tin với nhau nhờ giao thức truyền siêu văn bản HTTP (Hypertext Transfer Protocol). Phiên bản HTTP (1.1) được mô tả trong RFC 2616. Mục đích của HTTP là hỗ trợ cho việc chuyển các tài liệu HTML. HTTP là một giao thức mức ứng dụng. Các ứng dụng server và client HTTP sử dụng giao thức chuyển vận TCP để thiết lập một kết nối.

HTTP có các nhiệm vụ sau :

- Thiết lập một kết nối giữa trình duyệt (client) và server.
- Thỏa hiệp các thiết lập và thiết lập các thông số cho phiên làm việc.
- Chuyển có thứ tự nội dung HTML.
- Đóng kết nối với server.

Mặc dù bản chất của thông tin web là cực kỳ phức tạp. Nhưng hầu hết sự phức tạp này đều liên quan đến cách thức server xây dựng nội dung HTML và trình duyệt làm cái gì với nội dung nó nhận được. Quá trình chuyển nội dung thực sự qua các HTTP thì tương đối trật tự.

Khi bạn đánh một URL vào cửa sổ trình duyệt, đầu tiên trình duyệt sẽ kiểm tra lược đồ của URL để xác định giao thức sử dụng (Trong phần trước chúng ta đã biết các trình duyệt Web cũng hỗ trợ cho một số giao thức khác bên cạnh HTTP). Nếu trình duyệt xác định URL này tham chiếu tới một tài nguyên trên một site HTTP, nó lấy phần tên DNS trong URL và bắt đầu tiến trình phân giải tên. Máy tính client gửi một yêu cầu tìm kiếm DNS tới một server phân giải tên và nhận về địa chỉ của Web server. Sau đó trình duyệt dùng địa chỉ này để khởi tạo một kết nối tới web server.

Thông tin thêm

Trong những phiên bản cũ của HTTP (trước phiên bản 1.1) Client và server phải mở một kết nối mới cho mỗi mục được chuyển. Các phiên bản HTTP gần đây đã cho phép client và server duy trì một kết nối thường trực.

Sau khi kết nối TCP đã được thiết lập, trình duyệt dùng lệnh GET của HTTP để yêu cầu trang Web trên server. Lệnh GET chứa URL của trang web mà trình duyệt đang yêu cầu và phiên bản của HTTP mà trình duyệt muốn sử dụng cho phiên giao dịch này. Bởi vì kết nối với server đã được thiết lập nên trình duyệt có thể gửi URL tương đối trong lệnh GET (thay vì URL đầy đủ)

```
GET /watergate/tapes/transcriptHTTP/1.1
```

Server nhận yêu cầu này và gửi lại tài liệu được yêu cầu. Cùng với tài liệu là một tiêu đề chứa nhiều thông số phức tạp. Các thông số này có dạng sau

Keyword:value

Bảng 12.4 liệt kê vài vùng trong tiêu đề HTTP. Tất cả các vùng đều là tùy chọn và bất cứ vùng nào mà trình duyệt không hiểu sẽ không được xét đến.

Vùng	Dạng giá trị	Miêu tả
Content-Length	Số nguyên	Kích thước của nội dung tính theo đơn vị octet
Content-Encoding	x-compress x-gzip	Giá trị biểu thị kiểu mã hóa kết hợp với bản tin
Date	Định nghĩa trong RFC 850	Ngày (tính theo GMT) đối tượng được tạo ra
Last-modified date	Định nghĩa trong RFC 850	Ngày (tính theo GMT) đối tượng được thay đổi gần đây nhất
Content-Language	Mã ngôn ngữ theo ISO 3316	Ngôn ngữ dùng trong đối tượng

Bảng 12-4 Các ví dụ về các vùng tiêu đề HTTP

Thông tin thêm

Định dạng vùng tiêu đề dùng với HTML được mượn từ định dạng tiêu đề email đặc tả trong RFC 822.

Vùng `Content-Length` đặc biệt quan trọng trong môi trường Internet ngày nay. Trong phiên bản trước của HTTP(1.0), mỗi chu kỳ yêu cầu/đáp ứng đòi hỏi phải có một kết nối TCP mới. Client mở một kết nối và đưa ra một yêu cầu. Server đáp ứng yêu cầu và sau đó đóng kết nối. Do server đã đóng kết nối TCP nên client sẽ biết khi nào server dừng việc gửi dữ liệu. Do sự đóng mở liên tục các kết nối, nên tiến trình này làm tăng phí tổn cho mạng. Các phiên bản gần đây của HTTP (1.1 và sau đó) cho phép Client và Server duy trì kết nối lâu hơn. Như vậy Client cần một cách thức nào đó để biết khi nào một đáp ứng từ server kết thúc. Vùng `Content-Length` cho biết chiều dài của đối tượng HTML trong đáp ứng. Nếu server không biết chiều dài của đối tượng mà nó gửi đi (tình huống thường xảy ra trong HTML động) thì nó sẽ gửi vùng tiêu đề `Connection:close` để thông báo cho trình duyệt biết nó sẽ chỉ ra kết thúc của dữ liệu bằng động tác đóng kết nối.

HTTP cũng có một tiến trình thương lượng để server và trình duyệt đồng ý với nhau về các thông số thiết lập chung cho các tùy chọn ưa thích và định dạng nào đó.

12.5 Các kỹ thuật HTML tiên tiến

Web đã phát triển trong bối cảnh tập tin HTML là một tập tin văn bản tĩnh và đơn giản được xử lý giống nhau đối với tất cả các yêu cầu. Nhưng trong những năm gần đây bối cảnh này đã trở nên phức tạp do các tiến bộ trong công nghệ Web. Các website hiện nay thường tạo ra nội dung web ở thời điểm nhận được yêu cầu của client. Các kỹ thuật HTML động cho phép tổ chức nội dung theo những sở thích và yêu cầu cụ thể của người dùng. HTML động cũng làm đơn giản công việc thiết kế web (so với các rào cản lập trình trong quá khứ) do web server có thể đáp ứng không giới hạn các tổ hợp đầu ra thông qua một template đơn.

Trong thời gian này, một bối cảnh khác đang diễn ra trong thế giới web đó là chạy chương trình ở phía client (client-side programming). Trong trường hợp này, các lệnh của chương trình được chuyển tới client cùng với dữ liệu HTML, và các lệnh này thực thi trên máy tính client trong khi người dùng xem trang web.

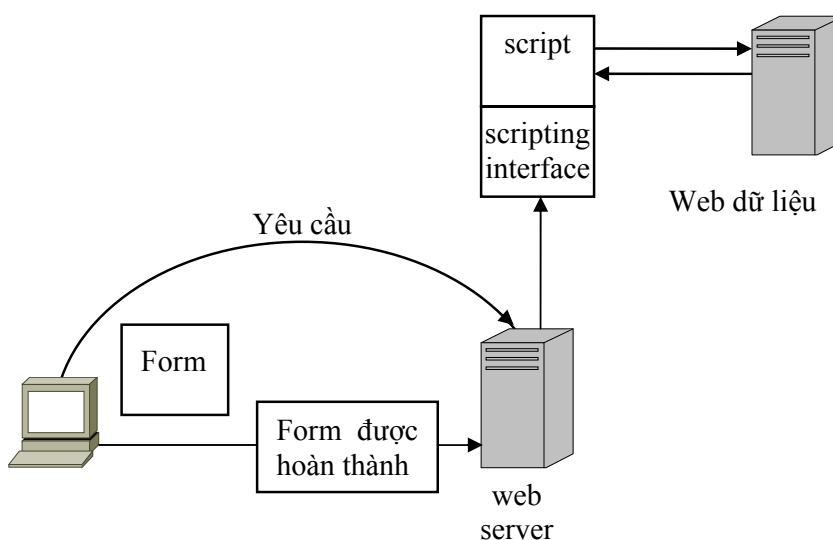
Bạn sẽ nghiên cứu về kỹ thuật HTML server-side và client-side trong phần sau.

12.5.1 Kỹ thuật HTML phía Server

Qua sự tìm hiểu về mã HTML trong phần trước, bạn có lẽ nhận thấy không có gì khó khăn hoặc phức tạp để đưa các thẻ HTML vào tập tin văn bản. Thực ra, khá đơn giản

để thực hiện một chương trình hoặc kịch bản để tập hợp nội dung HTML. Kỹ thuật động này cho phép một website tương tác với người dùng. Server có thể hình thành trang web đáp ứng lại dữ liệu nhập của người dùng. Việc lập kịch bản ở phía server cũng cho phép server chấp nhận thông tin đầu vào từ client và xử lý thông tin này ở hậu cảnh. Một kịch bản ở phía server thông thường được trình bày trong **hình 12.6**. Tiến trình xảy ra như sau :

1. Người dùng duyệt tới một trang web có một mẫu đơn dùng đăng ký mua một sản phẩm hoặc để nhập thông tin của khách thăm viếng.
2. Server tạo ra một mẫu đơn dựa vào các chọn lựa của người dùng và phát mẫu này tới trình duyệt.
3. Người dùng nhập các thông tin cần thiết vào mẫu đơn và trình duyệt phát mẫu đơn này trở lại server (tiến trình ngược với tiến trình thông thường. Trình duyệt gọi nội dung theo yêu cầu của server).
4. Server chấp nhận dữ liệu từ trình duyệt đưa đến và sử dụng một giao diện lập trình để chuyển dữ liệu này tới các chương trình xử lý thông tin người dùng. Nếu người dùng đang mua một sản phẩm, thì các chương trình hậu cảnh này có thể kiểm tra thông tin thẻ tín dụng hoặc gửi một phiếu chuyển hàng tới hộp thư. Nếu người dùng đang bổ sung tên anh ta vào danh sách gửi thư hoặc đang tham gia vào một site trực tuyến hạn chế thì có thể một chương trình sẽ bổ sung thông tin người dùng vào một cơ sở dữ liệu.



Hình 12-6 Một mô hình server-side scripting

Một trong những phương thức phổ biến hơn để giao tiếp một chương trình hoặc kịch bản với một trang Web là hệ giao tiếp cổng chung (CGI-Common Gateway Interface). CGI được phát triển để nhận thông tin đầu vào dưới dạng mẫu đơn từ một người dùng Web, xử lý thông tin nhập này, sau đó tạo ngõ ra theo dạng HTML. Các kịch bản CGI thông thường được viết theo ngôn ngữ Perl, nhưng CGI cũng tương thích với nhiều ngôn ngữ khác, bao gồm C.

Khi điều khiển chuyển qua giao diện CGI tới chương trình, chương trình có thể đảm nhận bất kỳ công việc nhiệm vụ đặc thù nào được thực hiện thông qua phần mềm. bạn có thể sử dụng một script CGI để xử lý một lệnh, trả lời một truy vấn, hoặc hình thành một cảnh trang Web tùy thích.

CGI chỉ là một trong nhiều phương thức dùng chung cho sự tích hợp việc xử lý ở đầu cuối server với một trang Web. Các phương thức khác:

- NSAPI - (Netscape Server Application Programming Interface), một giao diện chương trình được thiết kế cho Web server của Netscape.
- ISAPI - (Internet Server Application Programming Interface), một giao diện chương trình thiết kế cho Web server của Microsoft.
- Active Server Pages - Một môi trường lập kịch bản phía server được phát triển bởi Microsoft.
- Allaire ColdFusion - Một gói phần mềm phát triển ứng dụng cho các Web site động. ColdFusion chú trọng vào kết nối cơ sở dữ liệu.

Một trong những sử dụng quan trọng nhất của khả năng xử lý ở phía server (server-end) đó là web server có thể tương tác với một hệ thống cơ sở dữ liệu. Thông qua đặc tính này, trang web có thể hoạt động như một xử lý giao dịch và giao diện truy vấn từ xa. Vài ứng dụng Web server đã bắt đầu có đặc tính giao tiếp cơ sở dữ liệu có sẵn trong ứng dụng. Các website thương mại khổng lồ thì hầu như luôn luôn tích hợp với các hệ thống cơ sở dữ liệu được thiết kế tốt và khổng lồ tương xứng.

Một ứng dụng khác đang thay nổi lên sử dụng công nghệ xử lý server-end đó là công cụ quản lý và cấu hình mạng. Trong trường hợp này, một tập các tiện ích quản lý được đưa ra và giám sát thông qua một giao tiếp dựa trên web. Một số thiết bị mạng, như các router hoặc các thiết bị NAT có các server web nhỏ gắn liền bên trong thiết bị cho phép nhà quản trị truy xuất các thiết bị thông qua một trình duyệt để cấu hình và quản lý chính bản thân thiết bị. Các hệ thống quản lý dựa trên web to lớn hơn giám sát toàn bộ mạng cũng đã có trên thị trường mạng.

Cách đây một vài năm, khả năng và sự hữu ích của giao diện lập trình trên Web dường như không có giới hạn. Các kỹ thuật này vẫn là một phần không thể thiếu của Internet ngày nay, nhưng các nhà chuyên môn đã bắt đầu nhận thấy rằng các loại cộng

cụ kiểu này có thể gây ra các vấn đề bảo mật nếu chúng không được thực hiện một cách cẩn thận. Tùy theo mỗi thiết kế của chúng những chương trình này thực chất mời các user từ xa thực thi một chương trình trên máy chủ. Kẻ thù có thể gia tăng khai thác các công cụ này tìm kiếm để có được lối vào hệ thống bảo mật của Web server.

12.5.2 Kỹ thuật HTML phía Client

Xử lý phía client (client-side) cũng đã phát triển và làm thay đổi suy nghĩ về Web. Các trình duyệt ngày nay có khả năng thực thi đoạn mã được chuyển trực tiếp từ Web server đến máy tính của client. Xử lý client-side làm giảm tải xử lý trên server và thường cũng làm giảm tổng số lượng thông tin phải truyền qua mạng. Các Java applet (và các công nghệ tương tự khác) là phương tiện để tạo ra các hiệu ứng thú vị trên trang web khi bạn truy xuất vào website nào đó như các quả banh nảy lên xuống và các chú khi đang cười và đi đi lại lại trong cửa sổ trình duyệt. Các công nghệ này cũng chú ý đến một mặt quan trọng hơn. Ví dụ, bạn có thể sử dụng các kịch bản client-side để kiểm tra tính toàn vẹn của mẫu nhập liệu.

Cách đây một vài năm, nhiều người đã tin rằng tương lai của công việc tính toán là trong một môi trường hoạt động dựa hoàn toàn trên Java, còn ở client khi khởi động sẽ tải về đoạn mã thực hiện trên client. Khái niệm này gần đây dường như đã nguội lạnh, nhưng ý tưởng này một lần nữa đã nhấn mạnh vào tiềm năng rõ ràng của các kỹ thuật xử lý client-side.

12.6 XML

Ngay khi các người dùng, nhà cung cấp, và nhà thiết kế Web trở nên quen thuộc với HTML, họ đã bắt đầu đòi hỏi nhiều hơn. Sự phát triển của công nghệ lập trình phía server và phía client, và sự phát triển của kiến trúc các dịch vụ Web, làm cho nhiều chuyên gia tự hỏi mở rộng hệ thống các thẻ cứng nhắc của HTML. Mục đích của họ là vượt qua khái niệm về một ngôn ngữ đánh dấu như một phương tiện định dạng cho văn bản và hình ảnh và dùng ngôn ngữ đơn giản như là phương tiện cho việc truyền dữ liệu. Kết quả của suy nghĩ tranh luận này là một ngôn ngữ đánh dấu mới được gọi là ngôn ngữ đánh dấu mở rộng XML (Extensible Markup Language).

Như ta đã tìm hiểu ở các nội dung trước trong chương này, ý nghĩa và phạm vi ngữ cảnh của dữ liệu HTML bị giới hạn trong những gì mà bạn có thể biểu diễn qua một tập các thẻ HTML đã được định nghĩa trước (tham khảo **bảng 12.2**). nếu dữ liệu kèm trong thẻ <A>, nó được hiểu là một liên kết. XML, thì khác, nó cho phép các user định nghĩa các thành phần riêng của họ. Dữ liệu có thể biểu hiện bất kỳ thứ gì mà ta muốn chúng biểu hiện, và ta có thể sáng chế ra thẻ để đánh dấu dữ liệu. Ví dụ, nếu bạn

theo môn thể thao đua ngựa, bạn có thể tạo một tập tin XML với thông tin về chú ngựa mà bạn thích. Tập tin này bao gồm các mục như sau:

```
<horses>
  <horse_name="winky" breed="Thoroughbred">
    <sex="male" />
    <age="3" />
  </horse>
  <horse_name="Goddess" breed="Arabian">
    <sex="female" />
    <age="3" />
  </horse>
  <horse_name="Gecko" breed="Uncertain">
    <sex="male" />
    <age="14" />
  </horse>
</horses>
```

Định dạng XML nhìn hơi giống HTML, nhưng chắc chắn nó không phải là HTML. Bạn có thể sử dụng bất kỳ thẻ nào bạn muốn sử dụng trong XML, bởi vì không phải bạn đang chuẩn bị dữ liệu cho ứng dụng được định nghĩa trước một cách cứng nhắc và đặt biệt nào giống như một trình duyệt Web. Ý tưởng ở chỗ là bất cứ ai tạo ra cấu trúc trước cho một tập tin thì sau đó cũng tạo ra một ứng dụng mà có thể đọc tập tin này và hiểu ý nghĩa của dữ liệu.

XML là một công cụ cực kỳ mạnh để chuyển dữ liệu giữa các ứng dụng. Một kịch bản hoặc ứng dụng dễ dàng tạo XML ở ngõ ra hoặc đọc XML tại ngõ vào. Ngay cả khi một trình duyệt không thể đọc trực tiếp XML, XML vẫn được sử dụng rộng rãi trên Web. Trong vài trường hợp, dữ liệu XML tạo ra trên server side và sau đó được chuyển đổi thành dạng HTML sẵn sàng hiển thị trước khi nó được chuyển tới trình duyệt. Một kỹ thuật công nghệ khác cung cấp một tập tin kèm theo được gọi là Cascading Style Sheet (CSS), tập tin này cho biết cách để hiểu và hiển thị dữ liệu XML. Tuy nhiên XML thì không giới hạn đối với Web. Các lập trình viên ngày nay sử dụng XML trong các tình huống khác yêu cầu một định dạng thuận tiện và đơn giản trong việc gán giá trị cho các thuộc tính.

Ngày nay XML vượt xa Web thông thường mà chỉ là định dạng cho việc lưu trữ và truyền dữ liệu. Miễn là ứng dụng viết dữ liệu XML và ứng dụng đọc dữ liệu phải thỏa thuận về ý nghĩa của các thành phần, dữ liệu chuyển một cách dễ dàng và tiết kiệm giữa các ứng dụng.

Thông tin thêm

XML thường được mô tả như là một “ngôn ngữ đánh dấu cho việc tạo các ngôn ngữ đánh dấu”

12.7 Các công nghệ Web mới

Web ngày càng phức tạp do các lập trình viên và nhà cung cấp xây dựng nhiều biến dạng mới và tốt hơn. Trong vài năm gần đây, Web trở nên tin cậy cho các dịch vụ khách hàng và các ứng dụng có mục đích đặc biệt.

Thực ra, khái niệm dữ liệu ứng dụng được chuyển giao qua HTTP phát triển nhanh hơn chính bản thân Web và ngày nay nó là công cụ đơn giản cho sự phát triển phần mềm. Trong những phần sau ta sẽ tìm hiểu về một vài sự phát triển gần đây của thế giới Web.

- Web đa phương tiện
- Các giao tác Web
- Peer-to-peer

Khi đọc các phần sau, ta sẽ thấy nổi lên một điều đó là web hoạt động như là một giao diện đơn giản và thuận tiện cho các ứng dụng khác.

12.7.1 Web đa phương tiện

World Wide Web ngày càng trở nên giống truyền hình. Bây giờ người ta thường tìm video và audio trên trang Web. Thậm chí bạn có thể xem các chương trình trực tiếp qua web miễn sao máy tính của bạn là 1 radio hoặc tivi. Một vài công nghệ luồng dữ liệu tiên tiến hơn thì rất khác so với các công nghệ HTML thông thường mà ta đã nghiên cứu trong chương này. Tuy nhiên, các dạng gắn kết thông tin đa phương tiện khác thì không khác gì so với các dạng khác của HTML.

Như ta đã nghiên cứu trong Chương này, một thẻ <A> với thuộc tính HREF là một tham chiếu tới một tài nguyên khác. Trong các ví dụ trước, tài nguyên đó là một trang Web. Tuy nhiên, tham chiếu này có thể chỉ đến bất kỳ loại tập tin nào miễn là trình duyệt biết cách dịch nội dung tập tin. Các trình duyệt hiện đại có thể xử lý nhiều loại định dạng tập tin khác nhau. Phần đuôi của tên tập tin (chẳng hạn .doc, .gif, hoặc .avi) sẽ cho trình duyệt (hoặc hệ điều hành) biết ứng dụng nào sử dụng để mở tập tin. Nếu máy tính có phần mềm cần thiết để mở tập tin video hoặc audio, và nếu trình duyệt hoặc hệ điều hành được cấu hình để có thể nhận ra phần đuôi mở rộng tập tin,

thì trang Web có thể tham chiếu đến tập tin thông qua một liên kết thông thường, và trình duyệt sẽ thực thi tập tin khi kích vào liên kết.

Một vài định dạng tập tin video phổ biến và các phần mở rộng của chúng như sau:

- .AVI (Audio Visual Interleave)— Một định dạng âm thanh/hình ảnh được phát triển bởi Microsoft
- .MPEG (Motion Picture Experts Group)— Dạng tập tin video số có chất lượng cao và thông dụng.
- .MOV (QuickTime)— Định dạng QuickTime do Apple phát triển đầu tiên cho các hệ thống Macintosh, như có thể được sử dụng rộng rãi trên các hệ thống khác

Khi ta cài đặt phần mềm lên máy tính client (ví dụ khi ta cài chương trình QuickTime), người cài đặt ứng dụng đăng ký các phần mở rộng của tập tin mà máy tính có thể dùng để mở các ứng dụng.

Dĩ nhiên, ở đây còn nhiều quá trình như ghi, mã hoá, và xem một tập tin multimedia. Tuy nhiên, các chi tiết này không thực sự thuộc trách nhiệm của HTTP hoặc TCP/IP. Cho đến bây giờ mạng mới liên quan đến quá trình này, qua mạng server đơn giản tải về một tập tin multimedia tới client khi user kích vào liên kết.

Thông tin thêm

Sự kiện trình duyệt thỉnh thoảng sử dụng các ứng dụng khác để mở và thực thi các tập tin cho thấy toàn bộ hệ thống cộng sinh HTTP (HTTP, HTML, Web server, trình duyệt Web) về cơ bản là một phương thức phân phối, tương tự như các lớp dưới TCP/IP.

Kỹ thuật truyền dữ liệu đa phương tiện qua một liên kết gắn kết này chỉ thực hiện với các đoạn ngắn thông tin có kích thước và thời gian giới hạn. Bên cạnh đó cũng có các công nghệ khác hỗ trợ cho dạng dữ liệu đa phương tiện xử lý theo dạng luồng hướng thời gian thực. Các công nghệ này đòi hỏi một loại server đặc biệt. Ví dụ các server xử lý luồng video thời gian thực gồm Windows Media Server và QuickTime Streaming Server. Bạn có thể hình dung rằng, video dạng xử lý theo luồng có thể yêu cầu số lượng lớn băng thông mạng, phụ thuộc vào chất lượng hình ảnh mà ta muốn truyền.

12.7.2 Các giao dịch Web

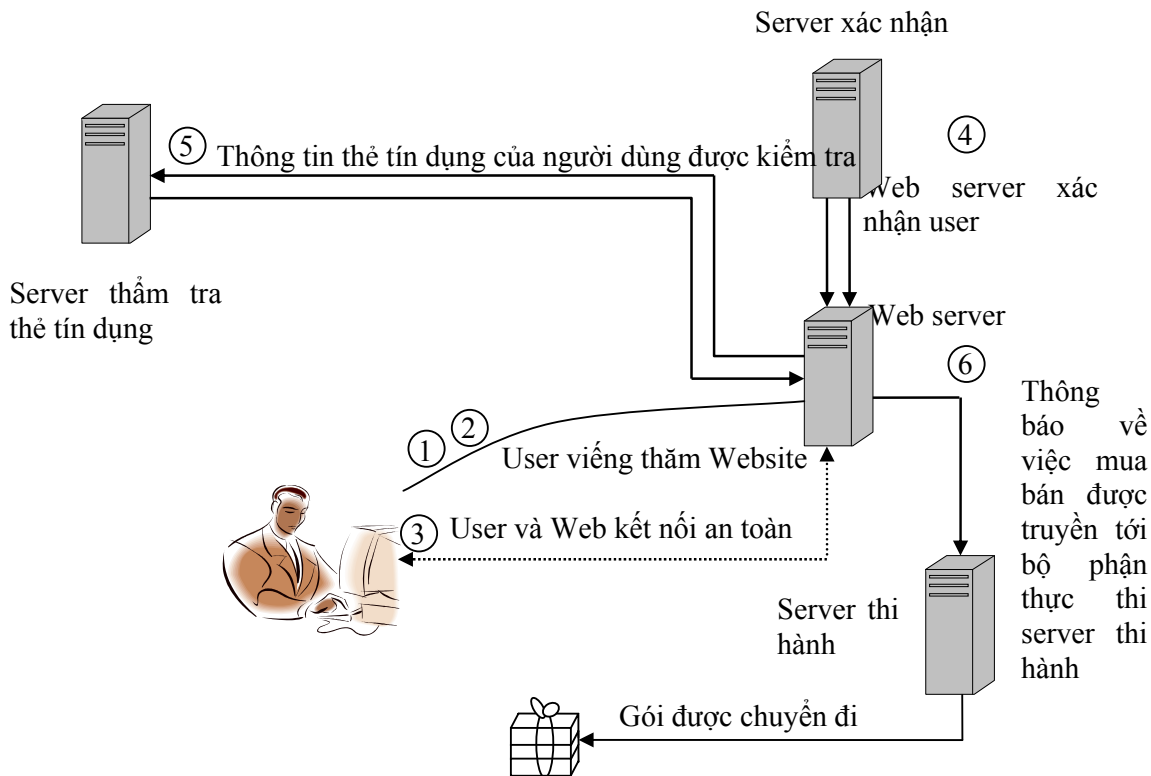
Trước đây khi các nhà cung cấp và các nhà quảng cáo bắt đầu nhận biết Web là cách quảng cáo tốt nhất. Nhiều Web site trông giống như là các quảng cáo phức tạp và dài. Web thật sự là phương tiện thuận tiện và tiết kiệm. Thay vì gửi hàng ngàn danh mục

trực tiếp bằng thư, nhà sản xuất có thể chỉ đơn giản đưa danh mục lên trang Web và khách hàng tìm ra danh mục này thông qua tìm kiếm và các liên kết.

Công việc kinh doanh qua Web đã không thật sự được bắt đầu cho đến khi các nhà cung cấp giải quyết vấn đề bảo mật liên quan đến việc gửi thông tin thẻ tín dụng qua Internet mở. Trong thực tế, việc bán hàng qua Internet có thể không thực hiện được nếu không có các kỹ thuật kết nối mạng an toàn. Hầu hết các trình duyệt ngày nay có khả năng mở ra kênh thông tin an toàn đến server. Với kênh thông tin an toàn này kẻ gian không thể lắng nghe mật khẩu thông tin thẻ tín dụng.

Các thao tác Web đặc trưng thể hiện trong **hình 12.7**. Các quá trình thực hiện như sau:

1. Web server cung cấp một khả năng truy cập danh mục trực tuyến từ trang Web. Một user duyệt qua các sản phẩm từ một vị trí từ xa qua Internet.
2. User quyết định mua một sản phẩm và kích vào liên kết “Mua hàng này” trên trang Web.
3. Server và trình duyệt thiết lập một kết nối an toàn. Tại thời điểm này trình duyệt hiển thị thông báo “Ngay lúc này bạn đang vào vùng an toàn” Các trình duyệt khác có nhiều phương thức khác nhau thông báo một kết nối an toàn. Ví dụ Netscape Navigator, hiển thị một chìa khoá vàng.
4. Sau khi đã thiết lập kết nối, luôn có một vài dạng xác nhận theo sau. Trên hầu hết các site giao dịch, người mua thiết lập vài dạng tài khoản người dùng với nhà cung cấp. Một phần vì lý do an toàn và một phần do thuận tiện (user có thể theo dõi trạng thái mua bán). Thông tin tài khoản người dùng cũng cho phép nhà cung cấp theo dõi hành vi của người dùng, thông tin nhân khẩu của người dùng và lịch sử mua bán. Bước đăng nhập này yêu cầu web server liên hệ với server cơ sở dữ liệu hoặc là để thiết lập một tài khoản mới hoặc để kiểm tra sự ủy nhiệm đăng nhập tới một tài khoản đang tồn tại.
5. Sau khi user được đăng nhập, server thẩm định lại thông tin thẻ tín dụng và đăng ký giao dịch với nhà quản lý thẻ tín dụng. Thường thì nhà quản lý thẻ tín dụng này là một dịch vụ thương mại liên kết với công ty thẻ tín dụng.
6. Nếu giao tác được chấp nhận, thông báo về việc mua bán và thông tin thư tín được chuyển đến bộ phận thực hiện của nhà cung cấp, ứng dụng giao tác đính kèm các chi tiết cuối cùng của việc xác nhận mua bán với người dùng và cập nhật tiểu sử tài khoản người dùng.



Hình 12-7 Một mô hình giao dịch Web đặc trưng

Các nhà cung cấp hệ điều hành như Sun và Microsoft cung cấp các ứng dụng giao dịch Server để giúp đỡ công việc quan trọng là xử lý đơn đặt hàng qua Internet. Bởi vì các giao dịch Web có tính chuyên môn cao, và do chúng đòi hỏi một giao diện với các ứng dụng đang tồn tại trên mạng của các nhà cung cấp. Các kết cấu ứng dụng chặn hạn như Sun ONE, WebSphere, và .NET cung cấp các công cụ đặc biệt hỗ trợ cho việc cấu trúc một cơ sở hạ tầng giao dịch.

Thông tin thêm

Trong **hình 12.7**, lưu ý Web server đặt trước một firewall. Trong các mạng thương mại qui mô lớn, việc cấu hình firewall có lẽ phức tạp hơn, với một firewall khác đặt trước Web server ngăn chặn lưu lượng nào đó nhưng vẫn để lưu lượng Web đi qua. Ngoài ra đối với các website lớn có thể có một tập hợp các web server cùng chia tải, nhóm các server như vậy thường được gọi là cụm hay nông trại server.

Lưu ý rằng các kết nối từ Web server đến server back-end có khả năng không qua hoặc qua firewall: Việc cấu hình firewall có thể cung cấp các ngoại lệ đặc biệt cho một host tin cậy có địa chỉ IP cụ thể thiết lập một kết nối thông qua một cổng đặc biệt. Một cách khác cho kết nối tới server back end là có thể thông qua một đường dành riêng không đi qua mạng chính.

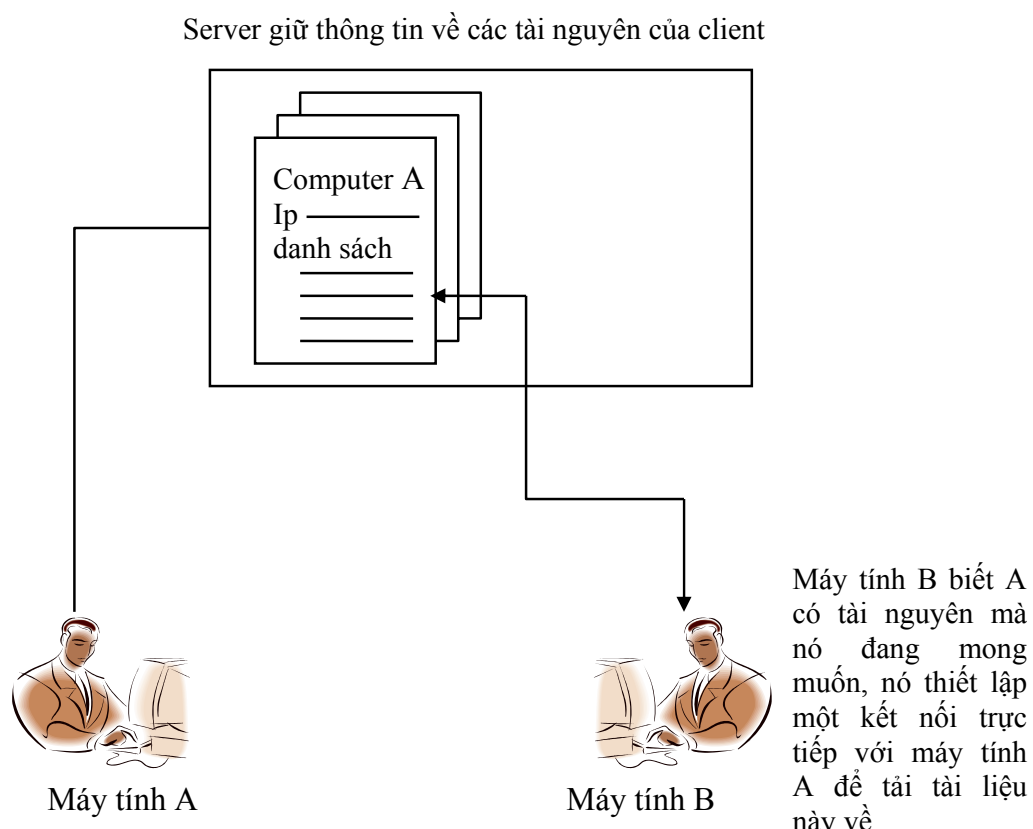
12.7.3 Peer-to-Peer

Một công nghệ chia sẻ thông tin mới nổi lên thông qua các cộng đồng chia sẻ âm nhạc trên Internet được gọi là peer-to-peer (P2P). Thuật ngữ peer-to-peer thật sự là được vay mượn từ việc cấu hình trên mạng LAN, trong đó các dịch vụ được tổ chức phân bố và mỗi máy tính có thể vừa là một client vừa là một server.. Peer-to-peer cho phép các máy tính thông qua Internet chia sẻ dữ liệu giữa các thành viên trong các cộng đồng chia sẻ thông tin. Nói cách khác, dữ liệu không đến từ một Web server đơn theo các yêu cầu từ một nhóm các client. Thay vào đó, dữ liệu cư trú trên các PC thông thường ở khắp nơi trong cộng đồng này.

Internet được tạo ra với một mục tiêu là tính đa dạng, và xét về mặt lý thuyết bất kỳ một máy tính nào có kết nối Internet có thể thiết lập kết nối với bất kỳ một máy tính tương thích nào khác có kết nối Internet ở bất kỳ đâu trên thế giới. Tuy nhiên, ta nên xem xét các ý sau:

- Các PC thông thường thì không phải luôn luôn được mở
- Hầu hết các máy tính được kết nối tới Internet không có một địa chỉ IP cố định, mà chỉ là một địa chỉ động thông qua DHCP (xem **Chương 9, "Giáo thức cấu hình host động - DHCP"**). Do đó, một máy tính không thể biết cách nào liên hệ với một máy tính khác bởi vì nó không có địa chỉ IP hoặc tên miền cố định.

Các nhà thiết kế kỹ thuật peer-to-peer đã biết ảo tưởng của họ về một cộng đồng chia sẻ âm nhạc đa dạng sẽ không thực hiện được nếu các vấn đề trên không được giải quyết. Giải pháp của họ là sử dụng một server trung tâm để phân phối thông tin kết nối cho các client sử dụng để thiết lập các kết nối với nhau. Như bạn thấy trong **hình 12.8**, người dùng A đăng nhập vào Internet. Phần mềm client trên PC của người dùng này đăng ký với server về sự hiện diện của người dùng. Server giữ một mẫu tin về địa chỉ IP của client này và các tập tin mà client muốn chia sẻ với cộng đồng. Khi người dùng B kết nối đến server này và tìm thấy tập tin mong muốn trên máy tính của người dùng A. Server cung cấp thông tin cần thiết cho người dùng B liên hệ với người dùng A. B liên hệ với A, thiết lập một kết nối trực tiếp và tải tập tin này về.



Hình 12-8 Một máy tính đăng ký dịch vụ peer-to-peer với địa chỉ và danh sách tài nguyên của nó. Các máy tính khác truy cập các tài nguyên này thông qua một kết nối trực tiếp

Phần tốt nhất về các cộng đồng peer-to-peer là các chi tiết về yêu cầu địa chỉ IP và thiết lập kết nối được điều khiển bên trong phần mềm. Người dùng đứng trong giao diện người dùng của ứng dụng peer-to-peer và không cần biết bất kỳ thứ gì về hoạt động mạng.

Tóm tắt

Phần này mô tả về các công việc xử lý đằng sau dịch vụ Internet nổi tiếng như World Wide Web. Bạn được nghiên cứu về các hoạt động Web, về URL và được giới thiệu ngắn gọn về tài liệu HTML. Phần này cũng mô tả giao thức HTTP tạo điều kiện thuận lợi cho việc phân phối nội dung của HTML từ server tới client. Cuối cùng nghiên cứu về kỹ thuật lập kịch bản server-end and client-end và cách chúng tăng cường sức mạnh cho một Web site.

CHƯƠNG

13

EMAIL

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Email (thư điện tử)**
- **SMTP**
- **Spam**

Nếu bạn không phải là một chuyên gia tin học thì cũng nhận thấy rằng thư điện tử đang trở thành một công cụ cực kỳ thông dụng cho thời giới hiện đại. Hiện tại cả hai mối quan hệ nghề nghiệp và cá nhân đều dựa vào thư điện tử để có thông tin nhanh và tin cậy khi liên lạc trên khoảng cách xa. Trong chương này sẽ giới thiệu một vài khái niệm thư điện tử quan trọng và trình bày cách mà dịch vụ thư điện tử vận hành trên mạng TCP/IP

Kết thúc chương này bạn sẽ có thể :

- Mô tả các thành phần của thông điệp thư điện tử.
- Thảo luận các tiến trình phân phát thư điện tử.
- Mô tả cách hoạt động của một phiên truyền dẫn SMTP.
- Thảo luận các giao thức nhận thư điện tử như POP3 và IMAP4.
- Thảo luận vai trò của người sử dụng thư điện tử.

13.1 Thư điện tử là gì?

Một thông điệp thư điện tử là một lá thư điện tử được soạn trên một máy tính và truyền qua mạng đến một máy tính khác (máy tính này có thể ở cạnh bên hay có thể bên kia thế giới). Thư điện tử được phát triển khá sớm. Hầu như ngay từ khi các máy tính được liên kết với nhau để tạo thành mạng, các kỹ sư máy tính đã tự hỏi liệu con người cũng giống như máy móc có thể liên lạc với nhau thông qua những liên kết mạng đó hay không?.

Hệ thống thư điện tử Internet hiện nay có từ thời mạng ARPAnet. Hầu hết nền tảng thư điện tử của Internet được cung cấp từ một cặp tài liệu được xuất bản năm 1982: RFC 821 (Giao thức truyền thư đơn giản) và RFC 822 (Tiêu chuẩn dành cho định dạng của các thông điệp văn bản mạng ARPA). Các định dạng thư điện tử được đề nghị khác đã phát triển kể từ sau đó (chẳng hạn hệ thống X.400, cũng như một vài định dạng riêng). Nhưng tính đơn giản và linh hoạt của thư điện tử dựa trên SMTP đã làm cho nó trở nên nổi trội và trở thành tiêu chuẩn dựa trên thực tế (de-facto) cho Internet. Thư điện tử được phát minh trong những ngày giao diện người dùng là văn bản, và mục đích chính của thư điện tử là truyền tải văn bản. Định dạng thông điệp thư điện tử được thiết kế để truyền tải văn bản một cách hiệu quả. Các đặc tả thư điện tử ban đầu không đề cập đến việc gửi các tập tin nhị phân. Một trong những nguyên nhân chính cho tính hiệu quả của thư điện tử là văn bản ASCII thì nhẹ và đơn giản cho quá trình truyền tải. Nhưng cuối cùng văn bản ASCII cũng có sự giới hạn. Trong những năm 1990, định dạng thư điện tử được mở rộng để bổ sung thêm các thành phần đính kèm nhị phân. Một thành phần đính kèm có thể là bất kỳ một dạng tập tin nào, miễn sao không vượt quá kích thước lớn nhất được cho phép bởi ứng dụng thư điện tử. Các thành phần đính kèm này được mã hóa theo định dạng phần mở rộng thư điện tử đa mục đích MIME (Multipurpose Internet Mail Extensions). Ngày nay, người dùng thường đính kèm các tập tin đồ họa, các tập tin bảng tính hay xử lý văn bản vào các thông điệp thư điện tử của họ.

13.2 Thư điện tử có dạng như thế nào?

Ứng dụng đọc thư điện tử cấu trúc một thông điệp thành dạng cần thiết để truyền. Nếu mạng của bạn sử dụng một hệ thống giao thức khác (hay một hệ thống thư điện tử khác), thông điệp có thể chuyển qua một hay nhiều gateway thư, gateway thư này chuyển đổi thông điệp thành định dạng Internet được mô tả trong chương này. Một thông điệp gửi qua mạng Internet bao gồm hai thành phần:

- Tiêu đề (header)
- Thân thông điệp (body).

Giống như thân của thông điệp, tiêu đề được truyền bằng văn bản mã ASCII. Tiêu đề bao gồm một chuỗi các tên vùng từ khóa được theo sau bởi một hay nhiều giá trị được phân cách bằng các dấu phẩy. Hầu hết các vùng tiêu đề thư điện tử đều quen thuộc đối với bất cứ ai dùng thư điện tử. Một vài vùng quan trọng được trình bày trong *bảng 13.1*.

Bảng 13-1 Một số vùng quan trọng trong tiêu đề thư điện tử

Vùng tiêu đề	Mô tả
To:	Địa chỉ thư điện tử người nhận thư.
From:	Địa chỉ thư điện tử của người gửi.
Date:	Ngày và thời gian thông điệp được gửi
Subject:	Miêu tả vắn tắt về chủ đề của thư
Cc:	Các địa chỉ thư điện tử của các người dùng khác sẽ nhận một bản sao của thông điệp.
Bcc:	Các địa chỉ thư điện tử của người dùng sẽ nhận một bản sao không nhìn thấy. Nó là một bản sao thông điệp mà những người nhận khác không biết rõ về nó. Bất kỳ địa chỉ nào được liệt kê trong vùng Bcc sẽ không xuất hiện trong tiêu đề thông điệp mà các người nhận khác nhận được.
Reply-To:	Địa chỉ thư điện tử sẽ nhận hồi đáp cho thông điệp này. Nếu trường này không được điền vào, các hồi đáp sẽ không đến địa chỉ trong trường From:

Tiếp theo tiêu đề là một dòng trống, và tiếp theo dòng trống là thân của thông điệp (văn bản thực của thư điện tử).

Người dùng thường muốn gửi nhiều thứ hơn chỉ là văn bản trong một thông điệp thư điện tử. Một số phương thức được dùng để truyền tải các tập tin nhị phân bằng thư điện tử. Hầu hết các chiến lược này sử dụng một tiện ích nào đó để chuyển đổi các bit nhị phân thành mã ASCII tương đương. Tập tin thu trông giống như văn bản mã ASCII – thực tế, nó là văn bản mã ASCII. Nhưng bạn không thể đọc được do nó là một mớ lộn xộn các ký tự tương ứng với mã nhị phân ban đầu. Tiện ích BinHex (ban đầu được phát triển dành cho Macintosh) và Uuencode (ban đầu được phát triển dành cho Unix) sử dụng phương thức này. Bạn hay người đọc thư của bạn phải có tiện ích giải mã cần thiết để chuyển đổi ngược lại thành dạng tập tin nhị phân ban đầu.

Một giải pháp chung để gửi tập tin nhị phân bằng thư điện tử là dùng định dạng MIME. MIME là một định dạng chung cho việc mở rộng khả năng của thư điện tử. Một ứng dụng thư điện tử có cho phép MIME mã hóa thông điệp thành định dạng MIME trước khi truyền đi. Khi thông điệp được tải đến người nhận, một ứng dụng thư

điện tử cho phép MIME trên máy tính của người nhận phải giải mã và khôi phục lại định dạng ban đầu.

MIME mang lại nhiều cải tiến cho thư điện tử, bao gồm:

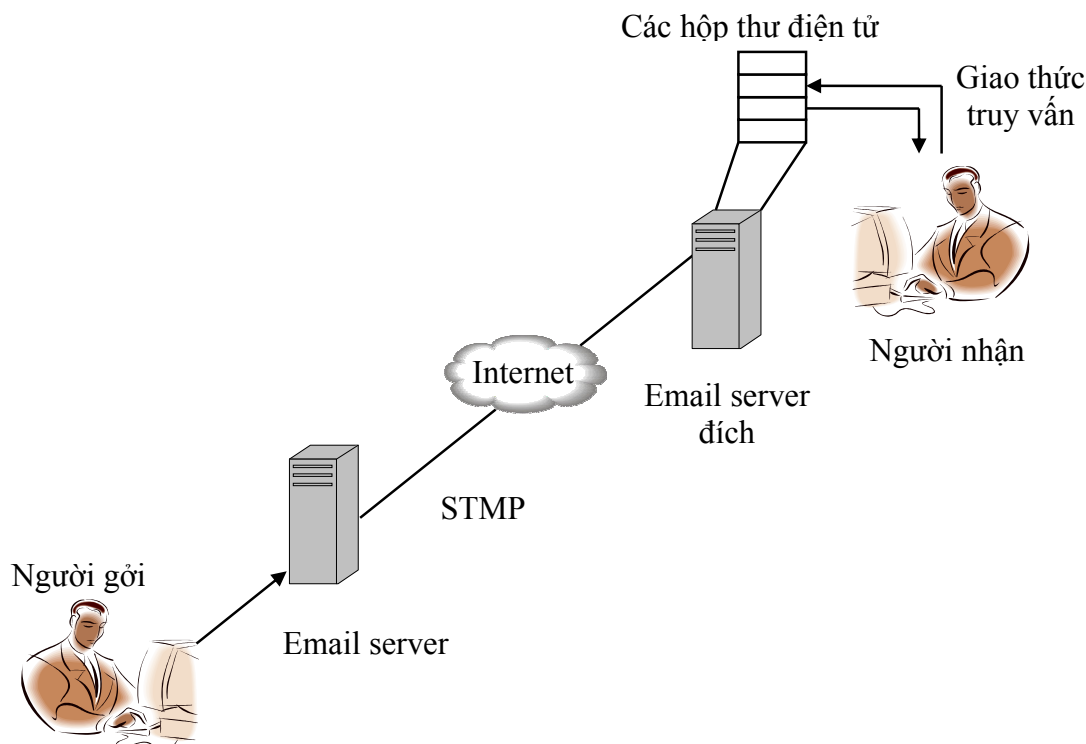
- Mở rộng các tập hợp ký tự. MIME là không bị giới hạn ở tập ASCII 128 ký tự chuẩn. Điều này có nghĩa là bạn có thể dùng nó để truyền các ký tự đặc biệt và các ký tự không có trong tiếng Anh.
- Không giới hạn chiều dài mỗi dòng và chiều dài thông điệp.
- Tiêu chuẩn mã hóa cho các thành phần đính kèm.
- Cho phép hợp nhất các hình ảnh, âm thanh, liên kết, và văn bản được định dạng trong thông điệp.

Hầu hết các ứng dụng đọc thư điện tử đều hỗ trợ MIME. Định dạng MIME được mô tả nhiều RFC bao gồm các RFC sau: 1521, 1522, 1563, và 1590.

13.3 Thư điện tử hoạt động như thế nào?

Giống như các dịch vụ Internet khác, thư điện tử được xây dựng dựa trên một tiến trình khách/ chủ. Tuy nhiên, tiến trình thư điện tử phức tạp hơn một chút. Nói một cách ngắn gọn, các máy tính ở cả hai đầu cuối của giao dịch thư điện tử hoạt động như các client, và thông điệp này được chuyển đi qua mạng bởi các server ở giữa. Một tiến trình phân phối thư điện tử được trình bày ở trong **hình 13.1**. Một client gửi một thông điệp đến một server thư điện tử. Server này đọc các địa chỉ của người nhận để chuyển thông điệp đến một server thư điện tử khác liên kết với địa chỉ đích.

Thông điệp được lưu trữ trên server thư điện tử đích trong một hộp thư điện tử (mailbox). (Một hộp thư điện tử cũng giống với một thư mục hay một hàng đợi của các thông điệp thư điện tử đến). Người dùng thỉnh thoảng đăng nhập vào server thư để kiểm tra thư. Nếu có các thông điệp đến đang đợi trong hộp thư của người dùng thì chúng sẽ được chuyển tải về máy tính của người dùng. Người dùng có thể đọc, lưu trữ, xóa, chuyển đi, hay hồi đáp thông điệp thư điện tử.



Hình 13-1 Tiến trình phân phối email

Một ứng dụng client được gọi là bộ đọc thư thực hiện các công việc chi tiết gửi thư đi hay đăng nhập vào server để tải thư đến. Hầu hết người dùng tương tác với tiến trình thư điện tử qua giao diện của một bộ đọc thư. Tiến trình gửi một thông điệp và chuyển tiếp nó giữa các server được điều khiển bởi một giao thức thư điện tử gọi là giao thức truyền thư đơn giản SMTP (Simple Mail Transfer Protocol).

Địa chỉ thư điện tử cho ta thông tin địa chỉ server cần thiết để chuyển tiếp thông điệp, RFC 822 chỉ ra định dạng của các định dạng địa chỉ thư điện tử phổ biến trên Internet.

`user@server`

Ví dụ:

`BillyBob@Klondike.net`

`SallyH@montecello.com`

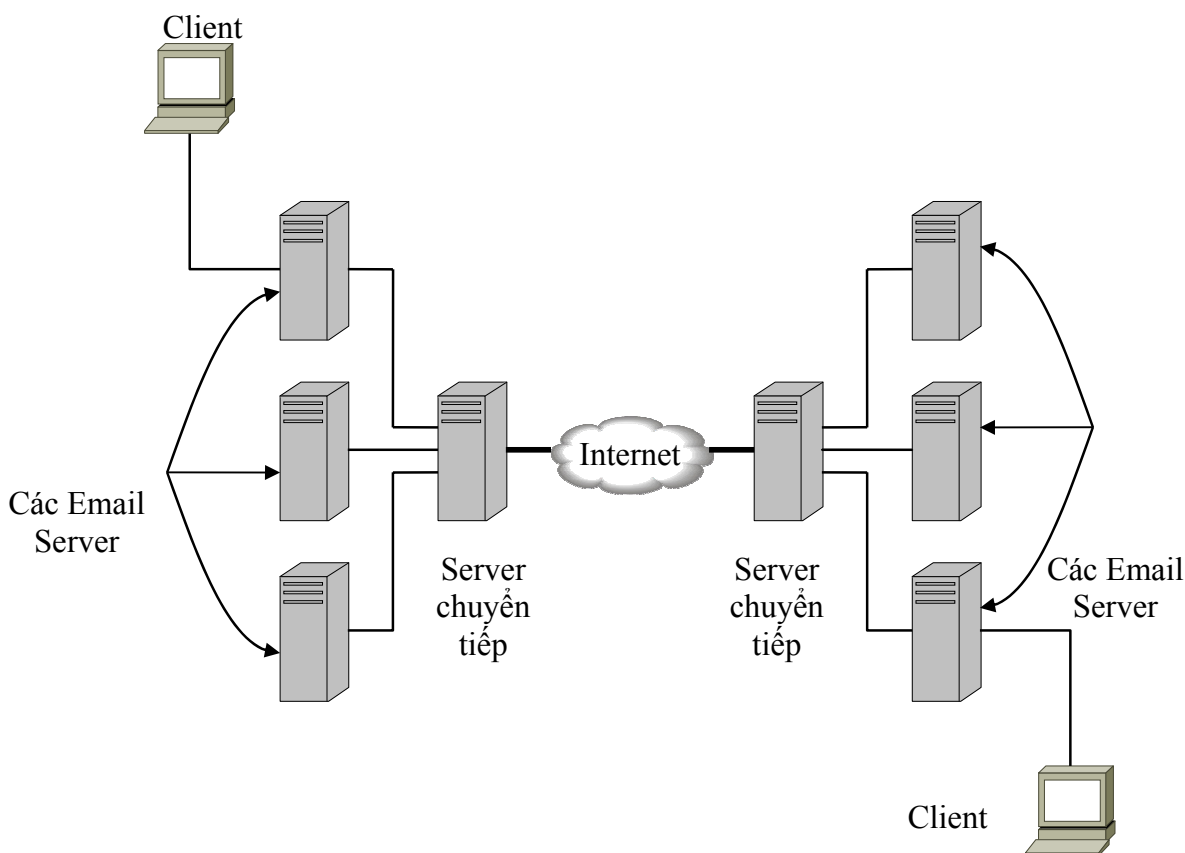
cravenprof@harvard.edu

Trong định dạng chuẩn, chuỗi văn bản sau ký hiệu @ là tên của địa chỉ server thư điện tử nói đến. Phần văn bản trước ký hiệu @ là tên của hộp thư người nhận trên server này. Trong thực tế phần văn bản phía sau @ thường đại diện cho tên miền của server thư điện tử mặc định trong miền người nhận. Các máy chủ DNS cho miền này sẽ lưu giữ mẫu tài nguyên MX liên kết một server thư điện tử với tên miền này.

Định dạng của địa chỉ thư điện tử

Khi nói về định dạng của địa chỉ thư điện tử cần có một nhận xét quan trọng về thư điện tử trên Internet: Đích của một thông điệp thư điện tử không phải là máy tính của người nhận thư mà là hộp thư của người nhận thư trên server thư điện tử. Bước cuối cùng để chuyển các thông điệp thư điện tử đang chờ từ một server thư điện tử đến một máy tính của người nhận là một tiến trình riêng biệt. Bạn sẽ tìm hiểu ở phần sau bước cuối cùng này được thực hiện như thế nào qua các giao thức truy vấn thư điện tử chẳng hạn như POP (Post Office Protocol) hay IMAP (Internet Message Access Protocol).

Một số mạng sử dụng các server thư điện tử có phân cấp để phân phối thư hiệu quả hơn. Trong tình huống này (xem **hình 13.2**), một server thư cục bộ chuyển các thông điệp đến một server thư chuyển tiếp. Server thư chuyển tiếp sau đó sẽ gửi lá thư này đến một server chuyển tiếp khác trên mạng đích, và server chuyển tiếp này gửi thông điệp này đến server cục bộ kết hợp với máy nhận.



Hình 13-2 Các server chuyển tiếp thường tăng hiệu suất của tiến trình phân phối thư

13.4 Giao thức chuyển thư đơn giản SMTP

SMTP là giao thức mà các máy chủ thư dùng để chuyển tiếp các thông điệp ngang qua một mạng TCP/IP. Máy tính client khởi phát một thông điệp thư điện tử cũng dùng SMTP để gửi thông điệp đến server cục bộ để phân phối đi.

Một người dùng không bao giờ phải làm việc với SMTP. Tiến trình liên lạc SMTP được thực hiện đằng sau hậu cảnh. Tuy nhiên, cũng quan trọng khi biết một ít về SMTP để có thể hiểu rõ các thông điệp báo lỗi cho thư điện tử không được phân phối đi. Hơn nữa, thỉnh thoảng các chương trình và các đoạn kịch bản truy cập trực tiếp SMTP để gửi các cảnh báo và báo động thư điện tử đến toàn bộ nhân viên trên mạng.

Giống như các dịch vụ ứng dụng TCP/IP khác, SMTP truyền thông trên mạng thông qua chồng giao thức TCP/IP. Các nhiệm vụ của ứng dụng thư điện tử thì đơn giản bởi vì ứng dụng này có thể dựa vào các dịch vụ xác thực và kết nối của phần mềm giao thức TCP/IP. Thông tin SMTP thực hiện thông qua một kết nối TCP đến cổng 25 của server SMTP. Cuộc đối thoại giữa client và server dùng các lệnh (và dữ liệu) tiêu chuẩn 4 ký tự từ client cùng với các mã hồi đáp 3 ký số từ server. **Bảng 13.2** trình bày một số lệnh của SMTP client. Các mã hồi đáp tương ứng của server được trình bày trong **bảng 13.3**.

Bảng 13-2 Các lệnh SMTP Client

Lệnh	Mô tả
HELO	Lời chào (Client yêu cầu một kết nối đến Server)
MAIL FROM:	Đặt trước địa chỉ mail của người gửi.
RCPT TO:	Đặt trước địa chỉ mail của người nhận.
DATA	Thông báo ý định để bắt đầu truyền tải nội dung của thông điệp.
NOOP	Yêu cầu server gửi một hồi đáp OK.
QUIT	Yêu cầu server gửi một hồi đáp OK và kết thúc phiên truyền.
RESET	Hủy bỏ giao tác.

Bảng 13-3 Một số hồi đáp của SMTP Server

Mã	Mô tả
220	<tên miền> dịch vụ sẵn sàng.
221	<tên miền> dịch vụ đóng kênh truyền.
250	Hành động được yêu cầu đã hoàn tất thành công.
251	Người dùng ở bên ngoài. Thông điệp sẽ được chuyển tiếp đến

Mã	Mô tả
	<path>.
354	Bắt đầu gửi dữ liệu. Kết thúc gửi dữ liệu bằng chuỗi <CRLF>.<CRLF> (biểu thị một dấu chấm trên một dòng).
450	Hành động yêu cầu không thực hiện bởi vì hộp thư đang bận.
500	Lỗi cú pháp: không nhận ra lệnh.
501	Lỗi cú pháp: có lỗi tham số hay đối số.
550	Hành động không thực hiện được bởi vì hộp thư không tìm thấy.
551	Người dùng ở bên ngoài. Thử gửi thông điệp đến <path>.
554	Giao tác bị lỗi.

Tiến trình này được thực hiện như sau. Như đã đề cập trong phần đầu chương, tiến trình này gửi một thông điệp từ client ban đầu đến server thư điện tử cục bộ và chuyển tiếp thông điệp này từ server cục bộ đến server đích hay tới một server khác trên đường dẫn chuyển tiếp:

1. Máy tính gửi lệnh HELO đến server. Tên của bên gửi được chứa trong một đối số.
2. Server gửi lại mã hồi đáp 250.
3. Bên gửi gửi đi lệnh MAIL FROM:.. Địa chỉ mail của bên gửi thông điệp, nó được chứa trong một đối số.
4. Server gửi lại mã hồi đáp 250.
5. Bên gửi sẽ phát ra lệnh RCPT TO:.. Địa chỉ của bên nhận thông điệp được chứa trong một đối số.
6. Nếu server chấp nhận thư cho bên nhận, server sẽ gửi ngược lại mã hồi đáp 250. Ngược lại, server gửi lại một mã biểu thị lỗi (ví dụ : mã 550 cho biết không tìm thấy hộp thư của người dùng)
7. Bên gửi gửi lệnh DATA để nói rằng nó bắt đầu gửi dữ liệu của thông điệp.
8. Server gửi lại mã hồi đáp 354 chỉ thị cho bên gửi bắt đầu truyền nội dung thông điệp.
9. Bên gửi gửi nội dung thông điệp và kết thúc bằng dấu chấm (.) trên một dòng.
10. Server gửi lại mã hồi đáp 250 báo rằng mail đã nhận được.
11. Bên gửi gửi lệnh QUIT nói rằng sự truyền tải đã chấm dứt và phiên làm việc nên được đóng.
12. Server gửi mã 221 báo kênh truyền dẫn sẽ được đóng lại.

Mạng sử dụng tiến trình truyền thông SMTP để gửi thông điệp thư điện tử đến hộp thư của người dùng trên server thư đích. Thông điệp sẽ được chứa trong hộp thư của người dùng cho đến khi người dùng đăng nhập và tải bất kỳ thư đang đợi nào. Sự tải về cuối cùng này là một tiến trình riêng biệt và cần một giao thức khác. Bạn sẽ học

thêm về các giao thức lấy thư về trong các phần sau.

13.5 Quá trình lấy thư

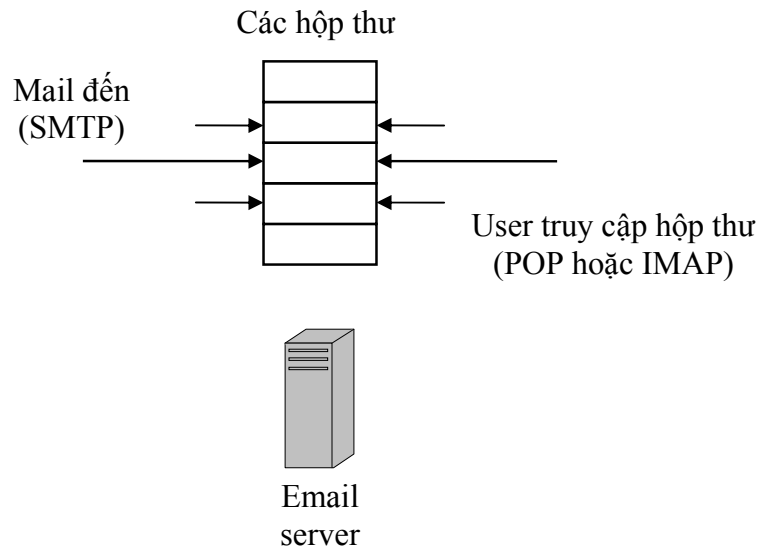
Tiến trình phân phát SMTP được mô tả trong phần trước không được thiết kế để phân phát thư điện tử đến một người dùng mà chỉ đến hộp thư của người dùng. Sau đó, người dùng phải truy cập vào hộp thư và tải thư về. Bước bổ sung này sẽ làm phức tạp tiến trình lấy thư nhưng nó có được các lợi ích sau:

- Server sẽ tiếp tục nhận thư cho người dùng thậm chí khi máy tính người dùng không tồn tại trên mạng.
- Hệ thống phân phát thư là độc lập với máy tính của người nhận thư (vị trí người nhận).

Lợi ích thứ hai là một đặc điểm mà nhiều người dùng thư quen thuộc. Đặc điểm này cho phép người dùng kiểm tra thư từ các vị trí khác nhau. Theo lý thuyết, bất kỳ máy tính nào truy cập Internet và một ứng dụng đọc thư được cấu hình để kiểm tra hộp thư của người dùng cho các thông điệp. Bạn có thể kiểm tra thư của bạn ở nhà, văn phòng hay khách sạn. Tiến trình truy cập vào hộp thư và tải thư về cần một giao thức lấy thư. Trong phần sau, bạn sẽ học POP và IMAP.

Trong thực tế, các hệ thống bảo mật mạng chẳng hạn như các bức tường lửa thỉnh thoảng ngăn chặn người dùng kiểm tra thư từ bất kỳ điểm nào trên Internet.

Server thư điện tử lưu giữ các hộp thư người dùng phải hỗ trợ cả hai dịch vụ SMTP (để nhận thư đến) và một dịch vụ giao thức lấy thư về (để user truy cập vào hộp thư). Tiến trình này được miêu tả trong **hình 13.3**. Sự tương tác với nhau này cần tính kết hợp và tính tương thích giữa dịch vụ SMTP và dịch vụ lấy thư về sao cho dữ liệu không bị mất hay xảy ra lỗi khi các dịch vụ truy cập cùng hộp thư đồng thời.



Hình 13-3 Dịch vụ SMTP và dịch vụ lấy thư phải được sắp xếp để được truy cập vào hộp thư

13.5.1 POP3

Giao thức bưu điện phiên bản 3 (POP3) là một giao thức được sử dụng rộng rãi. Nếu hiện tại bạn đang sử dụng thư Internet, bạn nên sử dụng client thư dùng POP3.

POP3 được mô tả trong RFC 1939. Client khởi động một kết nối TCP đến ứng dụng phục vụ POP3 trên server thư. Server POP3 lắng nghe các kết nối trên cổng TCP 110. Sau khi kết nối được thiết lập, ứng dụng client phải gửi thông tin tên người dùng và mật khẩu đến server thư. Nếu quá trình đăng nhập được chấp nhận, người dùng có thể truy cập vào hộp thư để tải hay xóa các thông điệp thư.

Giống như client SMTP, POP3 sử dụng một chuỗi lệnh 4 ký tự để trao đổi với server. Server hồi đáp lại chỉ bằng một số rất nhỏ các hồi đáp, chẳng hạn +OK (diễn tả lệnh được thực thi) và -ERR (diễn tả lệnh sinh ra lỗi). Các hồi đáp cũng có thể bao gồm các đối số và tham số thêm vào. Mỗi thông điệp trong hộp thư được *tham chiếu bởi một số nhận diện thông điệp*. Client gửi lệnh RETR (lấy về) đến server để tải một thông điệp. Lệnh DELE để xóa một thông điệp từ server.

Các thông điệp gửi giữa client POP3 và server là ẩn đối với người dùng. Các lệnh này được phát đi bởi ứng dụng đọc thư như là một đáp ứng cho các hành động của người dùng tác động trên giao diện người dùng đọc thư.

Một khuyết điểm của POP3 là giới hạn số chức năng thực hiện ở server. Người dùng chỉ có thể liệt kê các thông điệp trong hộp thư, xóa các thông điệp, và tải các thông điệp về. Bất kỳ thao tác nào trên nội dung thông điệp phải thực hiện ở client.

Giới hạn này có thể là nguyên nhân gây ra độ trễ và tăng lưu lượng mạng khi các thông điệp được tải về client. Một phiên bản mới hơn và tinh vi hơn là giao thức IMAP, nó được phát triển để khắc phục một vài khuyết điểm này.

13.5.2 IMAP4

Giao thức truy cập thông điệp Internet phiên bản 4 (IMAP4) là một giao thức lấy thư giống như POP3. Tuy nhiên, IMAP4 có thêm một vài đặc điểm mới không có trong POP3. Với IMAP4, bạn có thể duyệt các thư mục, di chuyển, xóa, và xem các thông điệp mà không cần sao chép các thông điệp đến máy cục bộ. IMAP4 cũng cho phép bạn lưu các thiết lập nào đó chẳng hạn khung nhìn cửa sổ client hay tìm kiếm các thông điệp trên server với một chuỗi tìm kiếm cụ thể. Bạn có thể tạo, xóa, và đặt tên hộp thư lại trên máy server.

Hầu hết các ứng dụng đọc thư gần đây hỗ trợ cả POP3 và IMAP4. Mặc dù hiện tại POP3 được sử dụng rộng rãi hơn, nhưng nhiều ưu điểm của IMAP đảm bảo các hệ thống thư sẽ tiếp tục chuyển đổi thành giao thức IMAP4.

13.6 Các bộ đọc thư điện tử

Một bộ đọc thư là một ứng dụng client chạy trên máy người dùng và trao đổi với server thư. Như đã đề cập trong phần trước, máy cục bộ không hình thành một kết nối trực tiếp với máy nhận thông điệp. Thay vì vậy, máy gửi dùng bộ đọc thư sẽ gửi một thông điệp đến một server thư. Server này gửi thông điệp này đến server ấn định cho người nhận. Người dùng kiểm tra hộp thư của họ trên server mail, và thông điệp được tải về máy của người dùng. Bước đầu tiên và bước cuối cùng trong tiến trình này (tiến trình gửi thông điệp đến server ban đầu và tải thông điệp về từ server nhận thông điệp) được thực hiện bởi một ứng dụng đọc thư.

Bộ đọc thư phải đáp ứng ba chức năng:

- Gửi các thông điệp đến một server chuyển đi dùng SMTP.
- Tập hợp các thông điệp thư đến từ một server thư dùng POP3 hoặc IMAP4.
- Có giao diện người dùng để đọc, quản lý và soạn thảo các thông điệp thư.

Bộ đọc thư phải có khả năng thực hiện cả chức năng client SMTP và client lấy thư (POP và IMAP).

Các giao thức thư điện tử được thảo luận ở trên cung cấp một lộ trình rõ ràng cho thông tin thư điện tử và vì vậy tất cả các bộ đọc thư là giống nhau. Chi tiết cách cấu hình một bộ đọc thư có thể khác nhau, nhưng nếu bạn đã quen thuộc với các tiến trình được mô tả ở đây, thì không khó để hình dung ra cách cấu hình cho nó hoạt động. Giống như các ứng dụng client mạng khác, một bộ đọc thư thông tin với mạng thông

qua chồng giao thức. Máy có bộ đọc thư phải cài đặt TCP/IP, và nó phải được cấu hình sao cho ứng dụng thư điện tử có thể vào mạng thông qua TCP/IP.

Thư điện tử từ lâu đã có khắp nơi trước những ngày vàng son của Internet, và nhiều hệ thống mạng riêng có các đặc tính truyền thông điệp tương tự. Bạn cũng có thể gửi và nhận thư trên các mạng sử dụng giao thức khác, chẳng hạn IPX/SPX hay SNA. Tuy nhiên, bạn phải có TCP/IP để gửi và nhận thư trên một mạng TCP/IP chẳng hạn Internet.

Sau khi bạn thiết lập máy tính như một client trên mạng TCP/IP, bạn cần xác định thêm một vài tham số từ một bộ phận trên mạng để cấu hình bộ đọc thư trên hệ thống của bạn. Nếu bạn là một người dùng gia đình, bạn có thể xác định thông tin này thông qua ISP của bạn. Nếu bạn là người dùng trong một công ty thì xác định thông tin này từ nhà quản trị mạng.

Bạn cần phải biết những điều sau đây:

- Tên miền đầy đủ của server thư để dùng cho mail gửi đi. Server này thường có tên máy chủ SMTP theo sau bởi tên miền (ví dụ, SMTP.rosbud.org).
- Tên máy chủ đầy đủ của POP hoặc IMAP server.
- Tên người dùng và mật khẩu của tài khoản người dùng thư trên server POP hoặc IMAP.

Cấu hình một bộ đọc thư là xác định các tham số này và nhập chúng vào ứng dụng đọc thư. Phần tiếp theo sẽ thảo luận các bộ đọc thư thông dụng.

Một số mạng có thể cần các cài đặt thêm, chẳng hạn cài đặt tham số xác thực.

13.6.1 Pine

Pine là một hệ thống thư được phát triển bởi trường đại học Washington. Nó cho phép người dùng soạn thảo và đọc thư sử dụng một giao diện đầu cuối đơn giản. Bạn có thể sử dụng Pine để soạn thảo và đọc các thông điệp thư điện tử, duy trì các sách địa chỉ, tạo và quản lý các thư mục, thêm các tập tin đính kèm với thư điện tử, thực hiện các chức năng kiểm tra chính tả, hồi đáp tin nhắn, và chuyển tiếp các thông điệp đến các máy khác.

Trong những năm gần đây, Pine bị qua mặt bởi nhiều bộ đọc thư có giao diện người dùng đồ họa GUI mới. Tuy nhiên, Pine (và các hệ thống dựa trên ký tự khác chẳng hạn Elm) vẫn được ưa thích bởi người dùng Linux và Unix vì họ thích hoặc cần một giao diện người dùng dựa trên văn bản.

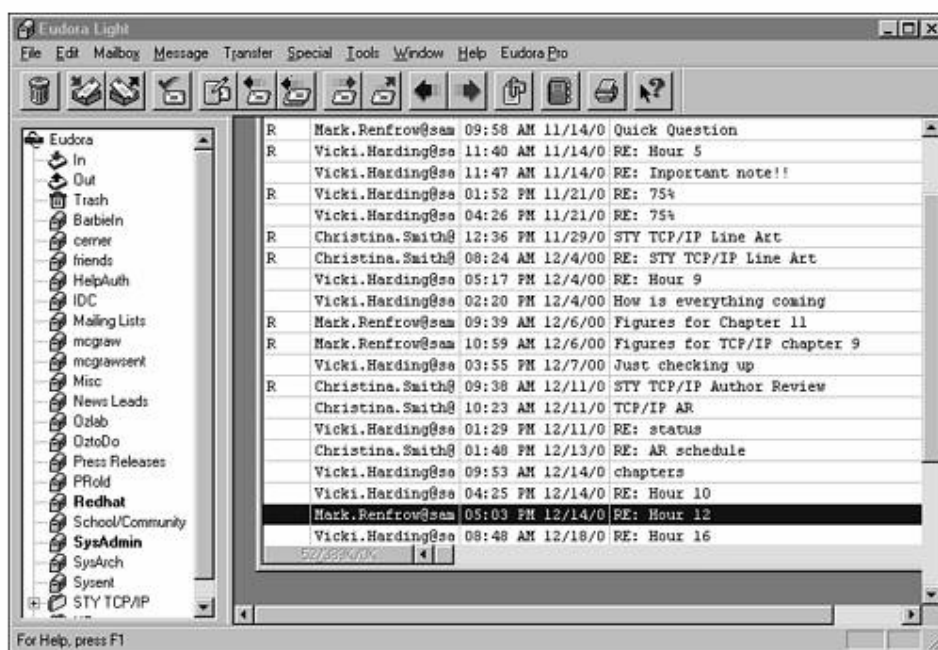
Pine được xây dựng trong nhiều hệ thống Unix và Linux. Nếu hệ thống của bạn có Pine, chỉ cần đánh pine ở dấu nhắc lệnh. Để cấu hình các tham số, chẳng hạn SMTP

server, truy cập thực đơn cài đặt (luôn bằng cách đánh chữ s).

13.6.2 Eudora

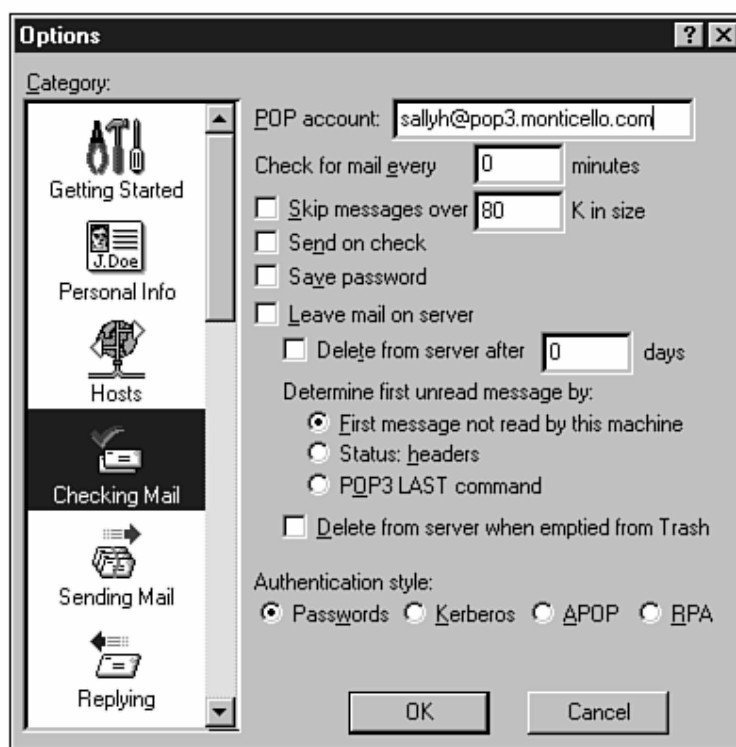
Eudora là một bộ đọc thư ổn định và nổi tiếng do tập đoàn QUALCOMM phát triển. Bởi vì Eudora là độc lập với các nhà cung cấp phần mềm lớn chẳng hạn Microsoft, bạn có thể sử dụng nó mà không cần phải lo ngại các công ty lớn này. Quan trọng hơn, các sản phẩm đối tác thứ ba như Eudora thường đơn giản hơn nhiều các sản phẩm tích hợp khổng lồ như Outlook và Netscape. Các chức năng tự động và hướng đối tượng của Outlook thực tế có thể gây ra các vấn đề an toàn nếu chúng không được cài đặt hợp lý. Và thậm chí trong trường hợp tốt nhất, các bộ ứng dụng tích hợp và lớn đôi khi đưa ra những thứ phức tạp hơn những gì mà người dùng muốn có. Cách đây một vài năm, Eudora đã có một lượng khách hàng lớn, trước khi thư điện tử trở thành một đặc tính có sẵn bên trong các máy tính chạy hệ điều hành Windows, nhưng thậm chí hiện tại, các bộ đọc thư của đối tác thứ ba chẳng hạn Eudora lại được nhiều người dùng ưa chuộng hơn.

Cửa sổ chính của Eudora Light được trình bày trong **hình 13.4**. Bạn có thể tổ chức các thông điệp thư điện tử nhận được vào trong các thư mục. Trong **hình 13.4**, các thư mục được trình bày trong cây ở bên trái. Click vào một thư mục để xem danh sách các thông điệp được lưu trong thư mục. Click đôi vào một thực thể thông điệp trong danh sách các thông điệp để đọc thông điệp. Bạn có thể sử dụng các nút nhấn khác nhau trên thanh công cụ để gửi nhận, hồi đáp một thông điệp, hay soạn thảo một thông điệp mới.



Hình 13-4 Cửa sổ chính của Eudora Light

Nhập vào các tham số cấu hình chẳng hạn server SMTP và server POP, chọn menu Tools và chọn mục Options. Hộp thoại Options sẽ đưa ra nhiều tùy chọn cấu hình (xem *hình 13.5*)

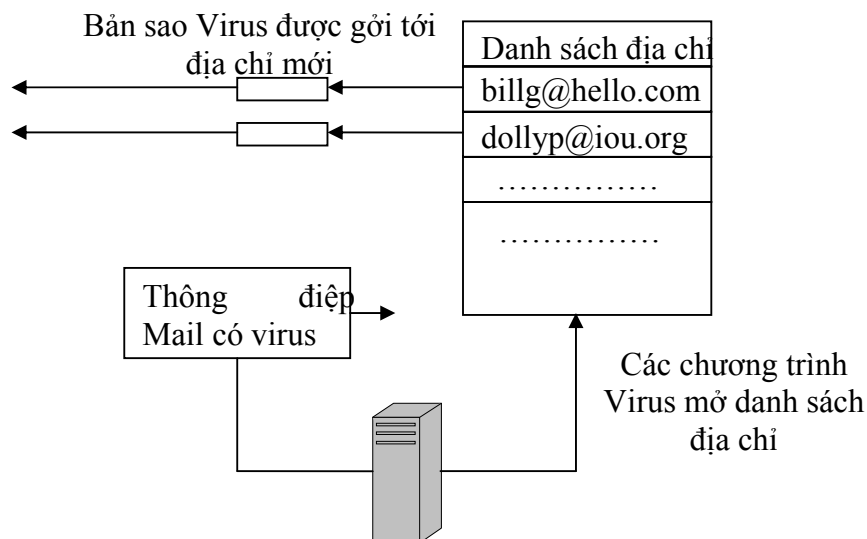


Hình 13-5 Cấu hình các tùy chọn trong Eudora Light

13.6.3 Các ứng dụng thư điện tử tích hợp

Các ứng dụng Internet tích hợp chẳng hạn như Netscape và Internet Explorer có chứa các bộ đọc thư điện tử. Bộ đọc thư điện tử của Microsoft là Outlook Express có trong nhiều hệ điều hành Windows, và một phiên bản nâng cấp chứa trong bộ Microsoft Office. Các ứng dụng đọc thư tích hợp như Outlook là giống với các bộ đọc thư khác ngoại trừ chúng được hỗ trợ một cấp độ xử lý tích hợp cao hơn. Bộ đọc thư có thể tương tác trực tiếp với các thành phần khác, đáp ứng các kịch bản hay các đặc tính trình duyệt từ một ứng dụng bảng tính hay xử lý văn bản.

Trong trường hợp của sản phẩm Microsoft, bộ đọc thư xem thành phần đính kèm đến như là một đối tượng và tùy thuộc vào sự chỉ dẫn bên trong thành phần đính kèm này, nó có thể chuyển điều khiển đến một ứng dụng khác nào đó bên trong bộ sản phẩm tích hợp này. Đặc tính tự động sẽ rất thuận tiện nếu được sử dụng hợp lý, nhưng nó cũng sinh ra một thể hệ mới của các virus macro phân phối qua các thành phần đính kèm trong thư điện tử. Một virus macro tiêu biểu có thể truy cập sổ tay địa chỉ của người dùng để học các địa chỉ mới, sau đó lá thư tự động được chuyển đến các người dùng khác trong danh sách này (xem *hình 13.6*).



Hình 13-6 Một virus thư điện tử

Sự ra đời của virus thư điện tử đưa đến một cuộc đấu tranh triền miên trong nền công nghiệp máy tính giữa các nhu cầu đối lập về sự an toàn và sự tiện lợi. Các bộ đọc thư tích hợp như Outlook có nhiều lợi ích, nhưng tất cả những thuận lợi này lại yêu cầu người dùng có một sự chú ý hơn. Các phiên bản gần đây của Outlook và các sản phẩm thư điện tử tích hợp khác có những cảnh báo và nhiều tùy chọn bảo mật để giới hạn ảnh hưởng của thư nguy hiểm.

Mặc dù người dùng bảo vệ thư khỏi virus. Nó có thể tắt một số đặc tính tự động trong Windows. Một ứng dụng chống virus tốt cũng có thể nhận biết các virus khi chúng đến.

13.7 Thư điện tử trên Web

Sự phát triển gần đây của WWW tạo ra một loại ứng dụng đọc thư điện tử mới được thiết kế gần gũi với HTML. Các server web mail không cần một bộ đọc thư. Người dùng chỉ đơn giản mở trang web thư điện tử bằng một trình duyệt Internet và truy cập thư điện tử thông qua giao diện web. Thư của người dùng vì vậy được truy cập từ bất kỳ máy tính nào được kết nối Internet. Yahoo và Hotmail là hai dịch vụ web mail thông dụng. Vì vậy các dịch vụ này thường được miễn phí hay miễn một phần bởi vì nhà cung cấp chủ yếu thu lợi từ quảng cáo để hỗ trợ cho toàn bộ cơ sở hạ tầng.

Web mail linh hoạt và dễ sử dụng. Nó là sự lựa chọn tốt cho những người dùng gia đình không biết về kỹ thuật, họ đã quen với web và không muốn phải cấu hình một ứng dụng thư điện tử nào cả. Hiện nay, một số công ty dùng Web mail trong những tình huống nhất định bởi vì bức tường lửa của họ cho phép lưu lượng HTTP và ngăn chặn SMTP. Web mail có thể nói là không an toàn. Bất kỳ ai trên mạng Internet biết

cách truy cập trang Yahoo có thể hình dung ra cách truy cập trang mail Yahoo. Nhưng điều quan trọng là phải nhớ rằng thư điện tử truyền thống cũng không an toàn, trừ khi bạn bảo vệ nó. Bất kỳ ai có tên người dùng và mật khẩu của bạn đều có thể kiểm tra thư của bạn. Các trang web mail lớn được bảo vệ bằng quá trình đăng nhập và một số sự bảo vệ khác. Nếu bạn đang quan tâm đến một dịch vụ web mail cục bộ nhỏ, thì bạn nên tìm ra một giải pháp an toàn để bảo vệ hệ thống.

Lời than phiền lớn nhất về web mail thường là hiệu suất của nó. Bởi vì hệ thống thư không hiện diện thật sự trên máy client (chỉ đơn giản là một trình duyệt web), tất cả các hoạt động tiểu tiết như soạn thảo, di chuyển, mở thư đều phải thực hiện qua ‘cổ chai’ của một kết nối mạng. Ngược lại một bộ đọc thư truyền thống tải về bất kỳ thông điệp mới nào tại thời điểm bắt đầu phiên làm việc, mọi hoạt động liên quan đến soạn thảo và lưu trữ thông điệp được thực hiện ở phía client. Mặc dù có sự kém hiệu suất trên nhưng sự cực kỳ thuận tiện của Web mail (bạn có thể kiểm tra thư ở bất kỳ nơi nào trên thới giới miễn là máy tính đó được kết nối vào Internet mà không phải cấu hình lại) – đảm bảo web mail vẫn là sự lựa chọn quan trọng của nhiều người dùng mạng.

Mục đích chính của Web mail là cung cấp cho người dùng phương tiện để gửi và nhận các thông điệp. Mặc dù web mail dường như là một khái niệm hoàn toàn mới, nó cũng không khác so với những hệ thống mail truyền thống đã được trình bày trong **hình 13.1**. Sự khác nhau là ở chỗ các phần mềm đọc và gửi thư được đặt trên server thư và máy nhận phải truy cập phần mềm đó thông qua một giao diện web. Các hệ thống web mail vẫn sử dụng SMTP để truyền các thông điệp qua mạng.

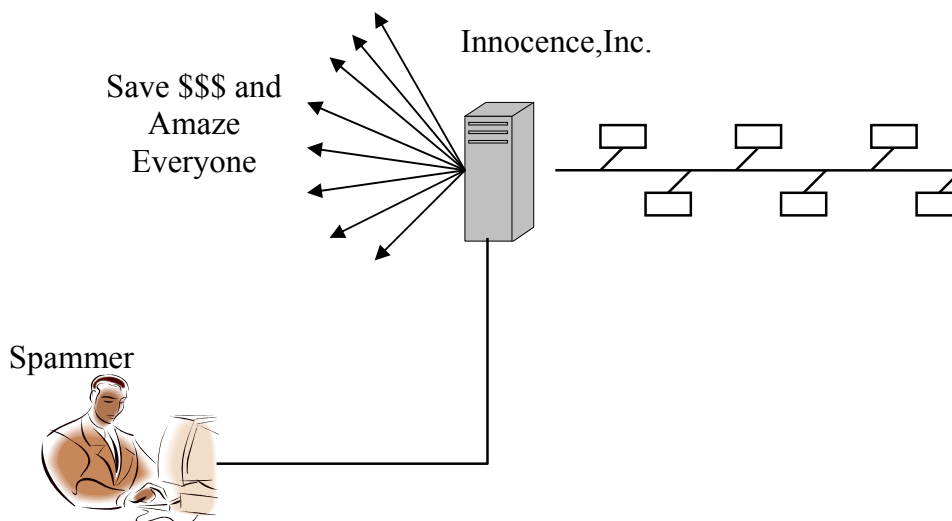
13.8 Spam

Sự phát triển gần đây trong kỹ thuật thư điện tử dẫn đến sự phát sinh ra spam. Spam là nickname của các thông điệp thư Themes-mail, chúng làm lộn xộn các hộp thư của hàng triệu người dùng Internet. Các thông điệp spam này quảng cáo về các món tiền vay ngân hàng, hỗ trợ ăn kiêng trên cơ sở các món tiền thưởng phù du, các tổ chức nhân đạo, và đa dạng các dịch vụ và sản phẩm trên. Về công nghệ, spam chỉ là thư điện tử. Các server thư định tuyến một thông điệp mà không biết thông điệp đó được phát sinh bởi chương trình tự động ghê tởm hay bởi một người thân của người nhận.

May thay, bên nhận có một số tùy chọn để nhận dạng và loại trừ spam. Một số kỹ thuật được sử dụng để chống lại spam là dựa trên các nguyên lý TCP/IP. Tuy nhiên như bạn đã thấy, các bộ tạo spam rất giỏi để tìm ra con đường đi qua được các chương ngại vật này, vì vậy không có giải pháp nào tồn tại mãi mãi. Các kỹ thuật mới hơn tập trung chủ yếu vào phân tích các văn bản của thông điệp thư.

Khi nền công nghiệp spam bắt đầu, người nhận bắt đầu nhận ra rằng nhiều lá thư spam đến từ một vài địa chỉ thư cụ thể. Những máy spam gom góp một số lượng lớn các địa chỉ thư được quan tâm để chúng liên kết với spam. Các dữ liệu này được gọi là danh sách đen. Tìm hiểu Cơ sở dữ liệu chuyển tiếp mở (Open Relay Database) tại trang <http://www.ordb.org>, đây là một ví dụ về danh sách đen của các server SMTP chuyển tiếp mở được công nghiệp Spam sử dụng). Các bức tường lửa, các server thư, hay các chương trình client có thể quét các thông điệp đến để đối chứng với một địa chỉ trong danh sách đen.

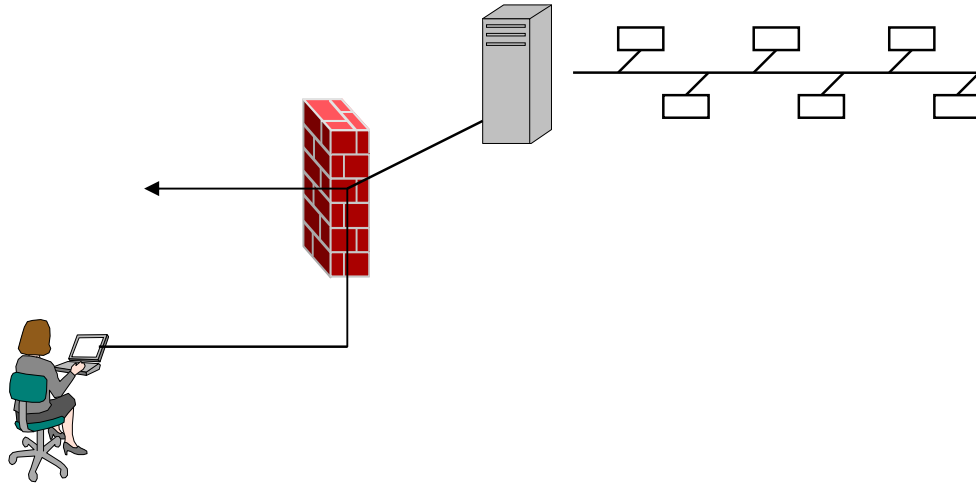
Các bộ spam thường thay đổi địa chỉ IP và tên miền để tránh danh sách đen. Một danh sách đen được xem là phương thức tốt hàng đầu để chống lại spam, nhưng nó không thích hợp để điều khiển hoàn toàn spam. Thực tế, thỉnh thoảng các bộ spam dùng các server thư của các công ty không bị nghi ngờ khác để chuyển tiếp thông điệp spam. Như đã nói ở trên, một server thư SMTP chỉ đơn giản là đợi thông điệp từ một client và chuyển tiếp nó đi. Dĩ nhiên một cách lý tưởng là chỉ có chủ của server thư mới sử dụng nó để chuyển tiếp các thông điệp, nhưng một server thư mà không được khóa một cách hợp lý có thể bị sử dụng bởi bất kỳ ai, bao gồm cả các spammer ở một vị trí khác (xem **hình 13.7**). Thỉnh thoảng các công ty hợp pháp và toàn bộ các cá nhân vô tội lại tìm thấy chính họ trong danh sách đen bởi vì các spammer đã sử dụng server của họ để chuyển tiếp thư.



Hình 13-7 Các Spammer có thể dùng server không bị nghi ngờ và không được bảo vệ để gửi các thông điệp của họ

Các công ty đã chống lại chiến thuật này bằng biện pháp riêng của họ. Bằng cách đặt server thư bên trong bức tường lửa công ty và ngăn chặn các yêu cầu SMTP đến tại bức tường lửa này (xem **hình 13.8**), một tổ chức tự bảo vệ mình tránh trở thành một điểm chuyển tiếp spam. Như trình bày trong **hình 13.8**, các client thư từ bên trong

bức tường lửa có thể sử dụng server thư để chuyển tiếp các thông điệp, nhưng các client ở bên ngoài thì không thể đến được server thư này. Kỹ thuật này thì hữu ích để điều khiển spam. Tuy nhiên, nó cũng có giới hạn. Một người dùng đang du lịch với một laptop hay đang kiểm tra thư từ một nơi nào đó bên ngoài mạng có lẽ thấy là không thể gửi thông điệp nếu không cấu hình lại client thư để chỉ đến server SMTP khác.



Hình 13-8 Đặt server SMTP đằng sau bức tường lửa và ngăn cấm các yêu cầu SMTP, bảo vệ server khỏi sự lợi dụng của spammer

Các kỹ thuật khác để chống lại spam dựa vào việc phân tích nội dung thông điệp. Các thuật ngữ hay các đoạn nào đó hay xuất hiện trong tiêu đề và thông điệp spam. Một số bộ lọc spam đã ngăn các thông điệp dựa trên tập luật. Ví dụ, một bộ lọc có thể ngăn chặn các từ thô tục hay các thuật ngữ khác liên quan đến các mô tả về sự miễn phí. Những phương pháp tinh vi hơn sử dụng các kỹ thuật xác suất thống kê để phân tích từ ngữ dùng trong thông điệp và ấn định một điểm số thể hiện mức độ của một thông điệp có thể là một spam.

Những loại phương pháp này mang lại hiệu quả trong việc phát hiện ra các thông điệp spam, nhưng thỉnh thoảng chúng cũng bị sai, các thông điệp hợp pháp lại bị ngăn cấm bởi vì nó trình bày giống như một spam. Những kỹ thuật tốt nhất cung cấp phương tiện để ‘rèn luyện’ bộ lọc, bằng cách chỉ ra cho nó thấy bất kỳ lỗi nào để nó có thể tính toán lại các khả năng và không gặp sai lầm lần thứ hai.

Tóm tắt

Nếu bạn có một tài khoản Internet, bạn có thể có kinh nghiệm trong việc gửi nhận thư điện tử. Chương này đã mô tả những gì xảy ra để một thông điệp thư điện tử sau khi nó rời khỏi máy tính của bạn. Bạn đã xem bên trong các tình huống phân phối thư đi. Bạn đã học được về SMTP và các giao thức lấy thư liên quan như POP3 và IMAP4. Chương này cũng đã thảo luận về vai trò của các ứng dụng đọc thư điện tử.

CHƯƠNG CÁC GIAO THỨC

14 QUẢN LÝ MẠNG

Trong chương này, bạn sẽ tìm hiểu các vấn đề sau :

- **Quản lý mạng**
- **SNMP**
- **RMON**

Các nhà quản trị mạng sử dụng các phần mềm và giao thức quản lý mạng để truy vấn tới các thiết bị như các router, hub, và các server đặt ở các vị trí mạng từ xa. Ví dụ các truy vấn này có thể xác định tất cả các cổng (giao tiếp) có hoạt động hay không, hoặc số lượng datagram tối đa và trung bình được xử lý trong một giây là bao nhiêu. Trong chương này thảo luận về các giao thức quan trọng được sử dụng để quản lý và giám sát các thiết bị trong các mạng TCP/IP. Chúng ta sẽ nghiên cứu về giao thức quản trị mạng đơn giản SNMP (Simple Network Management Protocol) và giám sát từ xa RMON (Remote Monitoring).

Kết thúc chương này bạn sẽ có thể :

- Mô tả được các phần mềm dùng giám sát mạng
- Thảo luận cách SNMP trao đổi thông tin giữa một tác nhân (agent) giám sát mạng và bộ giám sát mạng (server monitor)
- Giải thích một cơ sở dữ liệu thông tin quản lý (MIB) và cách sử dụng nó
- Giải thích về RMON và điểm khác của nó so với SNMP.

14.1 Giao thức quản lý mạng đơn giản SNMP

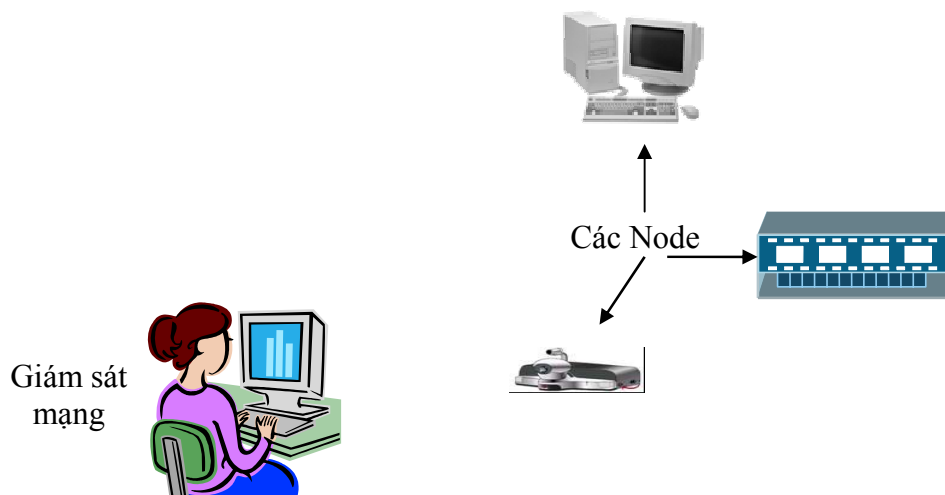
Mục đích của một giao thức mạng giúp thuận tiện trong truyền thông, và bất cứ khi nào ta có một loại thông tin cụ thể có những đặc tính phân biệt và định nghĩa được thì dường như ta có thể tìm ra một giao thức tương ứng. Giao thức quản trị mạng đơn là một giao thức được thiết kế cho việc quản lý và giám sát thiết bị từ xa trong một mạng. SNMP hỗ trợ một hệ thống cho phép một nhà quản trị mạng điều hành từ một trạm làm việc để quản lý từ xa và giám sát các máy tính, các router, và các thiết bị khác của mạng.

Hình 14.1 cho biết các thành phần cơ bản của cấu trúc SNMP:

Bộ giám sát mạng - một thiết bị giao tiếp quản lý, đôi khi được gọi là bộ quản lý (manager) hoặc hệ quản lý mạng NMS (Network Management Console), cung cấp một vị trí trung tâm quản trị các thiết bị trên mạng. Thiết bị giám sát mạng là một máy tính thông thường với phần mềm quản lý SNMP cần thiết.

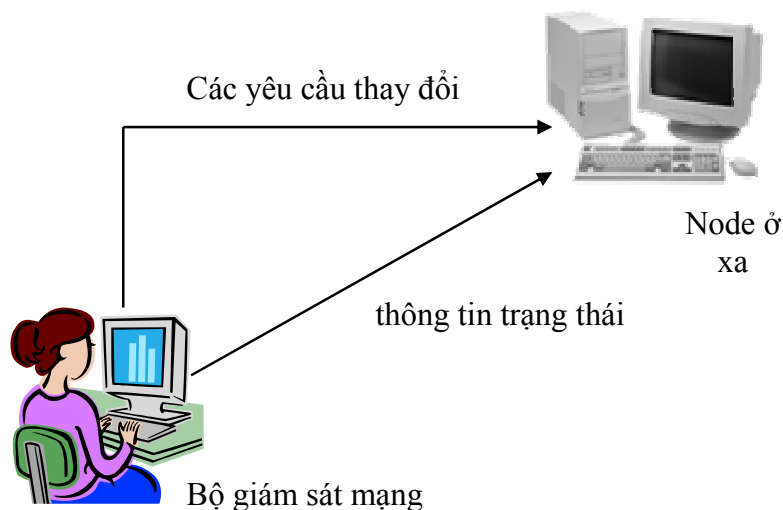
Các node - các thiết bị trên mạng.

Community - là một nhóm các node trong khung quản lý chung.



Hình 14-1 Một cộng đồng SNMP gồm có một hoặc nhiều các thiết bị giám sát và tập hợp các node

Một giao thức cung cấp một lược đồ truyền thông, nhưng tương tác thực tế xảy ra giữa các ứng dụng chạy trên các thiết bị truyền thông. Trong trường hợp của SNMP, một chương trình được gọi là một tác nhân chạy trên các node ở xa, thông tin với phần mềm quản lý đang chạy trên thiết bị giám sát mạng (xem **hình 14.2**).



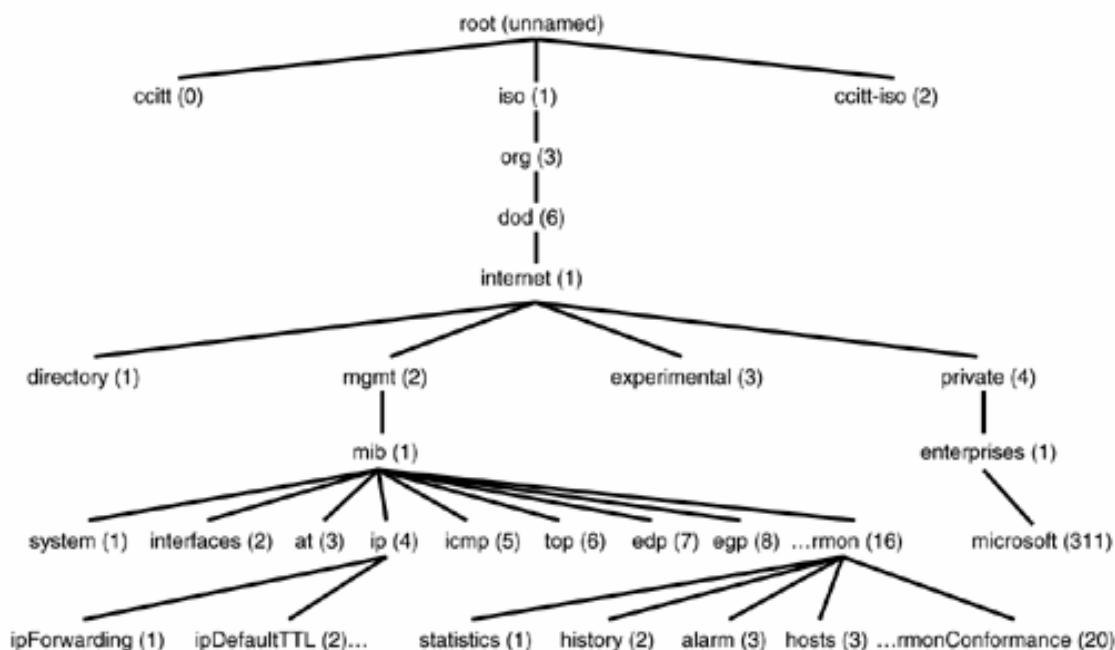
Hình 14-2 Một chương trình tác nhân đang chạy tại các node ở xa gửi thông tin tới thiết bị giám sát mạng và nhận các yêu cầu thay đổi các thiết lập cấu hình

Thiết bị giám sát và tác nhân sử dụng giao thức SNMP để thông tin với nhau. SNMP sử dụng cổng UDP 161 và 162. Các phiên bản trước kia của SNMP không yêu cầu bất kỳ dạng bảo mật nào đối với các user đăng nhập. Vấn đề bảo mật được cung cấp bởi tên community (chuỗi cộng đồng). Bạn phải biết chuỗi cộng đồng này thì mới kết nối vào hệ thống được. Trong nhiều trường hợp, bạn có thể cấu hình tác nhân chỉ nhận dữ liệu từ các địa chỉ IP định sẵn. Tuy nhiên cách bảo mật này không phù hợp với các tiêu chuẩn hiện đại. Hầu hết các phiên bản gần đây của SNMP (SNMP v3) đều quan tâm đến các vấn đề này, chúng cung cấp cơ chế xác thực, sự bí mật và hệ thống an toàn tổng thể tốt hơn cho các hệ thống.

Bạn có thể muốn biết thiết bị giám sát và tác nhân thông tin cái gì với nhau. Loại dữ liệu nào được truyền giữa thiết bị giám sát và tác nhân qua SNMP? Trong phần tiếp theo ta nghiên cứu về vấn đề này, SNMP định nghĩa một số lượng lớn các tham số quản lý. Thiết bị giám sát sử dụng các tham số của MIB này để yêu cầu thông tin từ tác nhân và thay đổi các thiết lập cấu hình.

14.2 Không gian địa chỉ SNMP

Quá trình SNMP dựa vào phần mềm giám sát và tác nhân có khả năng trao đổi thông tin liên quan với các vị trí có thể định vị riêng biệt bên trong MIP. MIP (trình bày trong **hình 14.3**) cho phép chương trình giám sát và tác nhân trao đổi thông tin chính xác và rõ ràng. Cả phần mềm giám sát và phần mềm tác nhân đều đòi hỏi các cấu trúc MIP đồng nhất, bởi vì chúng phải có khả năng nhận diện duy nhất đơn vị thông tin cụ thể.



Hình 14-3 Một phần nhỏ của MIB

MIB là một không gian địa chỉ phân cấp đảm bảo một địa chỉ duy nhất cho mỗi phần của thông tin. Chú ý: địa chỉ MIB không giống như địa chỉ mạng. Chúng không biểu thị một vị trí hoặc một thiết bị mạng thực tế. MIB thực ra là một tập hợp các tham số được tổ chức phân cấp thành một không gian địa chỉ. Sự tổ chức địa chỉ phân cấp này đảm bảo tất cả các thiết bị SNMP tham khảo tới một thiết lập cụ thể theo cùng một cách thức. Phương pháp này cũng cho phép sự phân quyền thuận tiện. Ví dụ, một nhà cung cấp cụ thể có thể định rõ các thiết lập MIB để áp dụng cho các sản phẩm của nhà cung cấp này, hoặc một tổ chức tiêu chuẩn có thể quản lý bộ phận của cây MIB dành cho các chuẩn của nó. MIB sử dụng biểu thị dấu chấm để nhận dạng mỗi địa chỉ duy nhất bên trong đối tượng MIB.

Thông tin thêm

MIB được mô tả trong nhiều RFC, bao gồm RFC 1158 và RFC 1213. Miêu tả chính thức SNMP nằm trong tiêu chuẩn RFC 1157. Phiên bản mới nhất SNMP v3, được mô tả trong tiêu chuẩn RFC 2570 và một số tiêu chuẩn RFC khác.

Hầu hết các vị trí có thể đánh địa trong cây MIB đều liên quan đến các bộ đếm. Ví dụ địa chỉ của tham số `ipForwarding`, trong **hình 14.3**, hoặc `ipInReceives` (không hiển thị), đếm số của gói IP nhận về từ lúc phần mềm kết nối mạng bắt đầu hoạt động hoặc từ lúc bộ đếm thiết lập lại gần đây nhất.

Phần lớn các vị trí có thể định vị bên trong MIP tham khảo tới các bộ đếm là các con số rành mạch. Ví dụ một bộ đếm là `ipForwarding` hoặc `ipInReceiver`, bộ

đếm này đếm số datagram IP đi về từ lúc phần mềm nối mạng khởi động hoặc từ lúc bộ đếm được thiết lập lại gần đây nhất.

Thông tin MIB có thể có nhiều dạng: số, văn bản, địa chỉ IP. Một ví dụ khác của thông tin cấu hình MIB là `ipDefaultTTL`. Thiết lập `IpDefaultTTL` lưu giữ giá trị số của tham số TTL (thời gian sống) được chèn vào trong mỗi datagram IP bắt nguồn từ một máy tính.

Cấu trúc MIP được định vị bắt đầu từ root và đi xuống theo yêu cầu cấu trúc phân cấp cho tới khi nhận diện duy nhất thiết lập mà ta muốn đọc. Ví dụ để định vị các MIB `ipDefaultTTL` và `ipInReceives`, bộ giám sát SNMP sẽ gọi các địa chỉ MIB tới tác nhân SNMP như sau:

```
.iso.org.dod.internet.mgmt.mib.ip.ipDefaultTTL
.iso.org.dod.internet.mgmt.mib.ip.ipInReceives
```

Tại mỗi vị trí trên cây MIB cũng có một địa chỉ số tương đương. Bạn có thể tham khảo tới một MIB hoặc bằng chuỗi ký tự số hoặc bằng địa chỉ số của nó. Trong thực tế, nó là dạng số mà thiết bị giám sát mạng sử dụng khi truy vấn thông tin từ tác nhân:

```
.1.3.6.1.2.1.4.2
.1.3.6.1.2.1.4.3
```

Địa chỉ MIB cung cấp một cách đặt tên chung để đảm bảo thiết bị giám sát và tác nhân có thể tham khảo một cách tin cậy đến các tham số cụ thể. Các tham số MIB này sau đó được chứa trong các lệnh (được mô tả trong phần tiếp theo).

14.3 Các lệnh SNMP

Phần mềm tác nhân giám sát mạng đáp ứng cho ba lệnh `get`, `getnext`, và `set`. Các lệnh này thi hành các chức năng sau:

- `get` - Lệnh `get` chỉ thị cho tác nhân đọc và trả về một đơn vị thông tin cụ thể từ MIB.
- `getnext` - Lệnh `getnext` chỉ thị tác nhân đọc và trả về đơn vị thông tin tiếp theo từ MIB. Lệnh này có thể được sử dụng để đọc một bảng các giá trị.
- `set` - Lệnh `set` chỉ thị tác nhân thiết lập một thông số cấu hình hoặc thiết lập lại một đối tượng chẳng hạn một giao tiếp mạng hoặc một bộ đếm cụ thể.

Thực tế phần mềm SNMP hoạt động theo nhiều cách khác nhau, phụ thuộc vào nhu cầu của người quản trị mạng. Các loại hoạt động khác nhau của SNMP được mô tả trong danh sách sau:

- Một tác nhân giám sát mạng hoạt động theo dạng truy vấn hoặc trả lời. nó có thể nhận các yêu cầu và gửi các trả lời đến trạm giám sát. Tác nhân nhận một lệnh `get` hoặc `getnext` và trả lại thông tin từ một vị trí địa chỉ.
- Mặc dù có sự lựa chọn, các tác nhân thường được cấu hình gửi các thông điệp không được yêu cầu tới trạm giám sát khi các sự kiện không bình thường xảy ra. Các thông điệp không được yêu cầu này được gọi là các thông điệp trap. Chúng được đưa ra khi các phần mềm tác nhân bắt gặp các sự kiện bất thường.

Ví dụ, phần mềm tác nhân SNMP thường hoạt động trong một chế độ, giám sát các ngưỡng được thiết lập có bị vượt quá hay không. Những mức ngưỡng này được thiết lập bằng lệnh `set`. Trong trường hợp giá trị một ngưỡng bị vượt, tác nhân nhận diện sự kiện và sau đó cấu trúc và gửi một thông điệp không được yêu cầu đến trạm giám sát mạng, trạm giám sát này sẽ nhận diện ra địa chỉ IP của máy xảy ra sự kiện cũng như mức ngưỡng nào bị vượt quá.

- Tác nhân có thể nhận các yêu cầu từ trạm giám sát để thực hiện các hành động nào đó, chẳng hạn thiết lập lại một cổng xác định trên một router hoặc thiết lập các mức ngưỡng được sử dụng phát hiện các sự kiện. Lệnh `set` được sử dụng để thiết lập các tham số cấu hình hoặc thiết lập lại bộ đếm hoặc các giao tiếp.

Ví dụ sau minh họa cho các lệnh truy vấn và trả lời dùng trong SNMP. Ví dụ này sử dụng một tiện ích chuẩn đoán được gọi là `snmputil`, tiện ích này cho phép nhà kỹ thuật mô phỏng một trạm giám sát. Thông qua tiện ích này, một nhà kỹ thuật có thể đưa ra các lệnh đến tác nhân. Trong trường hợp này, vị trí của tác nhân là một máy tính có địa chỉ IP là `192.59.66.200`, và tác nhân là một thành viên của một cộng đồng tên là `public`. Chú ý `.0` ở cuối hai lệnh đầu tiên; được sử dụng như là một hậu tố khi đọc các biến đơn giản chẳng hạn các bộ đếm.

```
D:\>snmputil get 192.59.66.200 public .1.3.6.1.2.1.4.2.0
Variable = ip.ipDefaultTTL.0
Value    = INTEGER - 128
```

```
D:\>snmputil getnext 192.59.66.200 public .1.3.6.1.2.1.4.2.0
Variable = ip.ipInReceives.0
Value    = Counter - 11898
```

Tên cộng đồng mặc định trên nhiều hệ thống là public. Quản trị trong ví dụ này nên thay đổi một tên nào đó khác. Dùng tên mặc định có nghĩa là trao cho những kẻ tấn công mạng mình một sự khởi đầu thuận lợi.

SNMP hữu ích cho các nhà quản trị mạng, nhưng nó không hoàn hảo. Nhiều thiếu sót của SNMP được miêu tả theo danh sách sau:

- Không thể thấy các lớp dưới - SNMP chỉ hoạt động tại lớp ứng dụng (Application) dựa trên UDP, nên nó không thể thấy cái gì đang xảy ra ở các lớp thấp nhất, chẳng hạn như tại lớp truy cập mạng (Network Access layer).
- Đòi hỏi một chồng giao thức hoạt động - trạm giám sát mạng và trạm tác nhân liên lạc với nhau phải có một chồng giao thức TCP/IP đầy đủ. Nếu có sự cố mạng làm cho chồng giao thức không hoạt động đúng, SNMP không thể trợ giúp để khắc phục vấn đề này.
- Có thể tạo ra lưu lượng mạng lớn - kỹ thuật truy vấn/ trả lời được sử dụng bởi SNMP có thể gây ra một khối lượng lớn lưu thông trong mạng. Mặc dù chỉ khi có các sự kiện quan trọng thì tác nhân mới gửi các thông điệp không được yêu cầu, trong thực tế các trạm giám sát mạng phát ra một khối lượng lưu thông mạng liên tục khi nó truy vấn các tác nhân về thông tin riêng biệt.
- Cung cấp quá nhiều dữ liệu nhưng ít thông tin - Với hàng ngàn vị trí địa chỉ trong MIB, bạn có thể truy vấn nhiều phần nhỏ thông tin. Tuy nhiên, nó đòi hỏi một hệ thống quản lý thật sự mạnh để phân tích các chi tiết tỉ mỉ này và có khả năng cung cấp các phân tích có hữu ích về cái gì đang xảy ra trên một máy cụ thể.
- Cung cấp quá trình kiểm tra thiết bị nhưng không kiểm tra được mạng - SNMP được thiết kế để cung cấp thông tin trên một thiết bị cụ thể. Bạn không thể thấy cái gì đang xảy ra trên phân đoạn mạng.

14.4 Giám sát từ xa (RMON)

Giám sát từ xa RMON (Remote Monitoring) là một sự mở rộng không gian địa chỉ MIB và được phát triển để cho phép thực hiện việc giám sát và duy trì các mạng LAN ở xa. Khác với SNMP, được dùng để cung cấp thông tin truy vấn từ một máy tính đơn, RMON lấy dữ liệu trực tiếp từ môi trường mạng và vì thế nó có thể nhìn thấu trọn vẹn vào bên trong mạng LAN.

MIB RMON bắt đầu từ vị trí địa chỉ .1.3.6.1.2.1.16 (trong **hình 14.3**) và hiện nay được chia thành 20 nhóm, ví dụ .1.3.6.1.2.1.16.1 đến .1.3.6.1.2.1.16.20. RMON được phát triển bởi IETF để điều chỉnh sự thiếu sót của SNMP và cung cấp tầm nhìn lớn hơn về lưu lượng mạng trên các LAN ở xa.

Có hai phiên bản của RMON: RMON 1 và RMON 2.

Thông tin thêm

Khi được sử dụng cùng chung với RMON, phần mềm tác nhân được gọi bằng thuật ngữ tham dò (probe).

- RMON 1— RMON 1 được định hướng giám sát các mạng LAN ethernet and token ring . Tất cả các nhóm trong RMON 1 có liên quan tới việc giám sát hai lớp dưới cùng, ví dụ lớp vật lý và lớp liên kết dữ liệu của mô hình OSI (tương ứng với lớp truy cập mạng (Network Access) trong mô hình TCP/IP). RMON 1 được mô tả trong RFC 1757, là bản cập nhật của RFC 1271, được công bố vào tháng 11 năm 1991.
- RMON 2— RMON 2 cung cấp các chức năng của RMON 1 và cũng đưa ra quá trình giám sát 5 lớp cao của mô hình OSI (tương ứng với lớp Internet, Transport, và Application của mô hình TCP/IP). Chi tiết kỹ thuật của RMON 2 có chứa trong RFC 2021 và 2034, các khuyến nghị này được công bố vào năm 1997.

Bởi vì RMON 2 có thể lắng nghe các giao thức lớp cao, nên nó có thể cung cấp thông tin về các giao thức mức cao, chẳng hạn như IP, TCP, và NFS.

Mục đích của RMON là bắt giữ dữ liệu lưu lượng mạng. Một tác nhân RMON (hoặc máy dò) lắng nghe trên một phân đoạn mạng và chuyển tiếp dữ liệu tới một trạm điều khiển RMON. Nếu mạng gồm nhiều phân đoạn, một tác nhân khác lắng nghe trên mỗi phân đoạn. Thông tin RMON được tập hợp lại trong các nhóm thống kê tương quan với các loại thông tin khác nhau. Sau đây là các tên nhóm RMON1:

- Statistics— Nhóm Statistics giữ thông tin thống kê theo dạng bảng cho mỗi phân đoạn mạng có máy thăm dò. Một vài bộ đếm trong nhóm này theo dõi số lượng gói, số các gói quảng bá, số các lần xung đột, số các datagram quá kích thước và kích thước thấp.
- History— Nhóm History giữ thông tin thống kê mà được biên soạn và lưu trữ định kỳ cho sự truy vấn sau này.
- Alarm— Nhóm Alarm sử dụng kết hợp với nhóm Event (được mô tả sau). Nhóm Alarm kiểm tra định kỳ những mẫu thống kê từ các biến trong máy dò và so sánh chúng với mức ngưỡng đã được cấu hình; nếu các ngưỡng bị vượt giới hạn, một sự kiện được tạo ra có thể được sử dụng để thông báo cho người quản lý mạng.

- **Hosts**— Nhóm Hosts duy trì các thống kê cho mỗi host trên phân đoạn mạng; nó biết về các host này bằng cách khảo sát địa chỉ vật lý nguồn và đích trong các datagram.
- **Host top n**— Nhóm Host Top n được sử dụng để tạo ra các báo cáo dựa trên các thống kê về số host xác định cao nhất trong một loại thông tin cụ thể. Ví dụ, một người quản lý mạng muốn biết các host nào xuất hiện trong hầu hết các datagram, hoặc các host nào gửi hầu hết các datagram có kích thước vượt quá giới hạn hoặc quá nhỏ.
- **Matrix**— Nhóm Matrix cấu trúc một bảng về các cặp địa chỉ vật lý nguồn và đích cho mỗi datagram được giám sát trên mạng. các cặp địa chỉ này xác định các cuộc trao đổi giữa hai địa chỉ.
- **Filter**— Nhóm Filter cho phép tạo ra mẫu nhị phân có thể được sử dụng để so trùng hoặc lọc các datagrams đến từ mạng.
- **Capture**— Nhóm Capture cho phép các datagrams được chọn bởi nhóm Filter được giữ lại cho việc khôi phục và kiểm tra sau này bởi người quản lý mạng.
- **Event**— Nhóm Event hoạt động kết hợp với nhóm Alarm để phát ra các cảnh báo cho người quản trị mạng khi một ngưỡng của đối tượng được giám sát vượt quá giới hạn.
- **Token Ring**— Nhóm Token Ring duy trì thông tin được thu thập dành riêng cho thủ tục điều khiển truy cập môi trường Token-Ring.

RMON 2 cung cấp các nhóm bổ sung liên quan đến việc giám sát các giao thức lớp trên của nó.

Tóm tắt

Trong chương này, ta đã tìm hiểu về giao thức SNMP, là một bộ tích hợp cung cấp việc giám sát và bảo trì tập trung cho các mạng ở xa. Ta cũng được nghiên cứu vấn đề đó, bằng cách sử dụng một thiết bị quản lý mạng trung tâm, một nhà quản lý mạng có thể được thông báo khi các sự kiện khác thường được tìm thấy và có thể xem trạng thái lưu lượng mạng được báo cáo bởi các tác nhân đang hoạt động trên các router, các hub và các server. Bằng cách sử dụng thiết bị điều khiển quản lý mạng, nhà quản lý mạng có thể thực hiện nhiều chức năng như thiết lập lại các cổng trên các router hoặc ngay cả thiết lập lại các thiết bị điều khiển từ xa.

Các thiết bị mạng mới hơn đã được nhúng thêm các đặc trưng RMON. RMON có thể làm giảm đáng kể lưu thông mạng so với SNMP và không yêu cầu có một thiết bị điều khiển quản lý mạng mạnh để dịch dữ liệu. Tuy nhiên, khi sử dụng RMON, có một số lượng xử lý đáng kể thực hiện trên tác nhân RMON hoặc máy dò, đó là quá trình thăm dò lưu thông mạng.

THUẬT NGỮ

A

ACK-Timer Bộ định thời xác nhận (**A**cknowledgement **T**imer) đảm bảo xác nhận cho một truyền dẫn TCP chỉ có hiệu lực trong một khoảng thời gian định trước.

ACK-Number Số xác nhận: Trong một kết nối [TCP](#), số xác nhận (**A**cknowledgement **N**umber) xác nhận gói dữ liệu đến bằng cách cộng thêm vào [số trình tự \(SN\)](#) số byte của phần dữ liệu Công thức tính là: ACK (trạm nhận) = SN (trạm gửi) + số byte của gói được truyền. Do vậy, số ACK cho biết trạm nhận sẽ nhận gói dữ liệu nào tiếp theo. Trong quá trình bắt tay ba bước, phải tăng SN nhận được lên 1 đơn vị để khớp với số ACK, số sau đó được gửi trở lại cho máy gửi, và sẽ trở thành số SN của máy gửi.

AND Phép toán và logic. Mỗi bit riêng biệt của địa chỉ IP đích được so sánh với bit tương ứng của mặt nạ mạng con. Nếu cả hai bit đều là 1 thì kết quả là 1. Trong các trường hợp khác, kết quả luôn là 0.

ARP Giao thức phân giải địa chỉ (**A**ddress **R**esolution **P**rotocol) nhận dạng địa chỉ MAC của máy tính đích khi đã biết địa chỉ IP.

ATM Chế độ truyền không đồng bộ (**A**synchronous **T**ransfer **M**ode) là một công nghệ chuyển mạch gói tầng liên kết dữ liệu. Trái với Frame Relay, các gói truyền trên mạng ATM có chiều dài cố định.

B

BER **BER** cho biết tỷ lệ bit lỗi (Bit Error Rate).

C

ccTLD Mọi quốc gia trên khắp thế giới đều có miền riêng trong hệ thống tên miền. Đó là tên miền mức đỉnh (country coded **T**op **L**evel **D**omain).

CIDR Định tuyến liên vùng không phân lớp (**C**lassless **I**nter-**D**omain **R**outing), là một phương pháp đánh địa chỉ mới để tối ưu việc gán địa chỉ IP cho các mạng.

- Class A** Các mạng được phân loại theo kích thước. Lớp A (**Class A**) cung cấp 126 mạng với 16.777.214 trạm trên mỗi mạng.
- Class B** Lớp B (**Class B**) cung cấp 16.384 mạng với 65.534 trạm trên mỗi mạng.
- Class C** Lớp C (**Class C**) cung cấp 2.097.152 mạng với 254 trạm trên mỗi mạng.
- Class D** Lớp D (**Class D**) được sử dụng cho các nhóm đa hướng (multicast)..
- Class E** Lớp R (**Class E**) là lớp thử nghiệm, không được thiết kế cho các mục đích sử dụng chung, nhưng được sử dụng cho các ứng dụng tương lai.
- CRC** Kiểm tra dư vòng (**Cyclical Redundancy Check**) là phương pháp được sử dụng để kiểm tra lỗi. Nó được chứa trong phần đuôi của dữ liệu tại tầng giao diện mạng. Tổng kiểm tra khung được gọi là dãy kiểm tra khung (Frame Check Sequence, FCS).
- CSMA/CD** Đa truy nhập cảm nhận sóng mang có phát hiện xung đột (**Carrier Sense Multiple Access with Collision Detection**) là phương pháp truy nhập được sử dụng trong mạng Ethernet. CSMA/CD là một tập luật xác định cách thiết bị mạng phải làm nếu có hai máy trên mạng cùng gửi dữ liệu một lúc.

D

- DF** Nếu bit không phân mảnh (**Don't Fragment**) trong phần tiêu đề IP được đặt là 1 thì không được phân mảnh gói..
- dial-up** Quay số là loại kết nối cho phép một máy khách kết nối tới nhà cung cấp dịch vụ (ISP), nơi sẽ nối họ tới Internet.
- DHCP** Giao thức cấu hình host động (**Dynamic Host Configuration Protocol**) tập trung và quản lý cấp phát các tham số cấu hình [TCP/IP](#) bằng cách tự động cấp phát [địa chỉ IP](#) cho các máy tính.
- DHCP ACK** Máy chủ gửi thông báo xác nhận DHCP (**DHCP ACK**), để thông báo cho máy khách rằng yêu cầu [thue IP](#) đã thành công. Thông báo này chứa địa chỉ IP thuê cũng như các tham số cấu hình khác. Cả máy khách và máy chủ đều lưu trữ thông tin này. Lúc này máy khách có thể truyền thông qua mạng trong thời gian thuê.
- DHCP DISCOVER** Máy khách quảng bá thông báo khám phá DHCP (**DHCP DISCOVER**) để hỏi thuê một [địa chỉ IP](#).

DHCP OFFER Lời mời chào này (được một máy chủ **DHCP** gửi tới máy khách), chứa địa chỉ phần cứng của máy khách, một Địa chỉ IP, mặt nạ mạng con, khoảng thời gian thuê và địa chỉ IP của máy chủ. Thông báo này luôn được gửi như một trả lời cho thông báo **DHCP DISCOVER**.

F

FCS **Frame Check Sequence**. Chuỗi kiểm tra khung **FCS** dùng để kiểm tra khung theo phương thức [CRC](#)

FDDI **Fiber Distributed Data Interface**. Giao thức dùng ở lớp liên kết dữ liệu. FDDI cung cấp kết nối tốc độ cao cho nhiều loại mạng

Frame Frame là đơn vị truyền dẫn ở lớp liên kết dữ liệu. Một Frame bao gồm tiêu đề được thêm vào tại lớp liên kết dữ liệu và dữ liệu đưa xuống từ lớp [IP](#).

FTP **File Transfer Protocol**. Giao thức truyền file được sử dụng để trao đổi file giữa các máy tính và để chia sẻ dữ liệu qua mạng.

G

gTLD **generic Top Level Domains** - ví dụ như arpa, com, edu, gov, mil, net, org và int là phần địa chỉ cấp trên cùng trong cấu trúc tên miền [DNS](#).

H

Header Đây là tiêu đề của một gói dữ liệu. Nó cung cấp các chức năng khác nhau phụ thuộc vào lớp ([layer](#)), tại đó tiêu đề được thêm vào.

HELO **HELO** là lệnh nhận dạng được dùng bởi client để khởi động kết nối tới server [SMTP](#)

Host-ID Địa chỉ **Host-ID** dùng để nhận dạng máy trạm, server, router hay các host [TCP/IP](#). Mỗi địa chỉ host là duy nhất trong một mạng máy tính.

HTML The **H**ypertext **M**arkup **L**anguage. Ngôn ngữ đánh dấu siêu văn bản **HTML** là ngôn ngữ chuẩn cho các trang web. HTML đưa ra các chuẩn để định dạng văn bản trên internet.

HTTP **H**ypertext **T**ransfer **P**rotocol. Giao thức truyền siêu văn bản dùng để truyền các bản tin từ server tới client sử dụng TCP/IP. Lưu lượng HTTP không được mã hóa. Giống như [HTTPS](#), [FTP](#) và [SMTP](#), HTTP là một trong những giao thức được sử dụng nhiều nhất để truy nhập internet.

HTTPS **H**ypertext **T**ransfer **P**rotocol **S**ecure là giao thức được sử dụng để thiết lập các kết nối web server an toàn với sự trợ giúp của [SSL](#) - **S**ecure **S**ocket **L**ayer. Cùng với [HTTP](#), [FTP](#) và [SMTP](#), HTTPS là một trong những giao thức được sử dụng nhiều nhất để cung cấp để truy nhập Internet.

I

IAC Không giống như các giao thức khác, dịch vụ TELNET không sử dụng tiêu đề để truyền các chức năng quản lý. Thay vì thế, nó sử dụng ký tự IAC, các octet được biên dịch thành các lệnh. Bên nhận sẽ tìm trong luồng dữ liệu tới các ký tự này, nếu ký tự IAC được phát hiện, các bit tiếp theo sẽ được dịch thành các lệnh.

ICMP Giao thức ICMP cung cấp các dự báo lỗi và đưa ra các thông báo lỗi xảy ra khi truyền dẫn

IGMP Giao thức IGMP trong [TCP/IP](#) quản lý việc truyền quảng bá, tức là từ một điểm tới đa điểm.

IP Giao thức IP thực hiện đánh địa chỉ gói dữ liệu và truyền chúng tới đúng đích.

IP address Mỗi máy tính sử dụng giao thức [TCP/IP](#) hay gọi là host TCP/IP được nhận dạng bởi một địa chỉ IP logic. Mỗi host và các thành phần mạng giao tiếp với nhau sử dụng một địa chỉ IP duy nhất. Địa chỉ này là duy nhất trên toàn cầu và tuân theo dạng chuẩn. Mỗi địa chỉ IP bao gồm hai phần [Network ID](#) và [Host ID](#).

IP address class Các địa chỉ [IP](#) được chia thành các lớp địa chỉ [A](#), [B](#), [C](#), [D](#), và [E](#).

IP datagram Đây là một gói dữ liệu [IP](#). Nó bao gồm [IP header](#) và dữ liệu.

- IP header** Đây là tiêu đề của gói [IP datagram](#). Nó cung cấp các thông tin để định tuyến và nhận dạng dữ liệu cũng như kích cỡ gói tin, thứ tự các gói và các tùy chọn của [IP](#).
- IP lease** Khi một server [DHCP](#) nhận được yêu cầu truy nhập mạng của một client, nó sẽ lấy một địa chỉ [IP](#) từ cơ sở dữ liệu và gửi tới client. Nếu client chấp nhận, địa chỉ này sẽ là của client đó trong suốt thời gian sử dụng. Chúng ta gọi đây là dịch vụ thuê địa chỉ IP. Client có thể gửi và nhận dữ liệu trong suốt thời gian thuê địa chỉ này.
- IPv4** Giao thức IPv4 là một phiên bản của giao thức IP đang được sử dụng hiện nay
- IPv6** Giao thức IPv6 là phiên bản sau của [IPv4](#). IPv6 được đưa ra để giải quyết những vấn đề liên quan đến địa chỉ mạng và cung cấp khoảng địa chỉ nhiều hơn so với phiên bản trước.
- ISDN** **I**ntegrated **S**ervices **D**igital **N**etwork. Đây là mạng số tích hợp đa dịch vụ được thiết kế cho các cuộc gọi thông thường, mạng quay số, fax và các dịch vụ khác, ví dụ như truyền hình hội nghị.
- ISP** **I**nternet **S**ervice **P**rovider. Nhà cung cấp dịch vụ internet cung cấp quyền truy nhập internet cho các cá nhân và cơ quan. Để thực hiện, ISP gán một [IP address](#) tới mỗi mạng con.

L

- Layer** Chồng giao thức [TCP/IP](#) gồm nhiều lớp.

M

- MAC** Trường thích ứng mạng bao gồm 12 ký tự dạng số hexa, địa chỉ MAC **M**edia **A**ccess **C**ontrol (Điều khiển phương tiện truyền dẫn) là một địa chỉ phần cứng quan trọng để đánh địa chỉ và gửi dữ liệu.
- MF** Nếu bit **M**ore **F**ragments (còn phân mảnh) trong mảnh dữ liệu của cờ tiêu đề IP ([IP header](#)) được thiết lập nghĩa là không phải tất cả các gói dữ liệu đã được truyền và vẫn còn các mảnh theo sau.
- MTU** **M**aximum **T**ransmission **U**nit **MTU** (Đơn vị truyền lớn nhất) chỉ ra kích thước gói lớn nhất một mạng có thể truyền.

N

NAT **Network Address Translator NAT** (Bộ biên dịch địa chỉ mạng NAT) là một router thực hiện việc dịch địa chỉ riêng thành địa chỉ chung để truyền số liệu qua Internet.

Network ID **Network ID** (Chỉ số mạng) xác định các hệ thống trong cùng đoạn mạng. Tất cả các hệ thống trong cùng một đoạn mạng phải có cùng một Network ID. Chỉ số này là duy nhất.

NLPID Trong Frame Relay (Chuyển tiếp khung), trường chỉ số giao thức tầng mạng (**Network Layer Protocol Identifier**) **NLPID** xác định giao thức tầng Internet thực hiện đóng gói dữ liệu.

O

OSPF **Open Shortest Path First** (Đường truyền ngắn nhất) là giao thức định tuyến dùng trong định tuyến động.

P

PAR Trong kết nối TCP, việc truyền dữ liệu dựa trên **PAR Positive Acknowledgement with Retransmission** (Phúc đáp tích cực có truyền lại). Nói cách khác, khi nhận được đúng dữ liệu phải phúc đáp cho người gửi.

PVC **Permanent Virtual Circuit PVC** (Mạch ảo cố định) gửi tất cả các gói dữ liệu qua cùng một đường dẫn. Điều này giúp cho truyền số liệu nhanh hơn vì các gói không cần phân mảnh.

R

- RCPT** Trong [SMTP](#), máy client dùng lệnh RCPT để thông báo địa chỉ cho server .
- RIP** Routing Information Protocol **RIP** (Giao thức thông tin định tuyến) là giao thức định tuyến dùng cho định tuyến động.

S

- SMTP** Simple Mail Transfer Protocol **SMTP** (Giao thức truyền thư điện tử đơn giản) dùng để truyền email.
- SN** Trong một kết nối [TCP](#), mỗi gói tin cần phải có một Sequence Number (số thứ tự) để máy nhận có thể sắp xếp chúng theo đúng thứ tự. Giá trị của SN phụ thuộc vào số byte của gói dữ liệu trước. Khuôn dạng là: SN (của gói mới) = SN (của gói trước) + số bytes (của gói trước). Máy nhận sử dụng số SN nhận được để tạo ra một [ACK-Number](#).
- SNMP** Simple Network Management Protocol **SNMP** (Giao thức quản lý mạng đơn giản) giám sát các router, server, máy in và các thiết bị mạng khác và giải quyết các vấn đề liên quan đến các thiết bị này.
- SSL** Secure Socket Layer hỗ trợ việc thiết lập kết nối tin cậy của web server.
- Subnet ID** Để chia một mạng thành các mạng con, mỗi đoạn mạng phải sử dụng một Subnet ID (Chỉ số nhận dạng mạng con) riêng. Subnet ID được tạo ra bằng cách chia các bit của phần [Host ID](#) (Chỉ số nhận dạng máy chủ) ra thành hai phần, một phần xác định mạng con, phần còn lại xác định máy chủ.

T

- TCP** Giống như [UDP](#), Transmission Control Protocol **TCP** (Giao thức điều khiển truyền) là một giao thức chính của tầng Giao vận. TCP cung cấp thông tin hướng liên kết và tin cậy khi truyền một lượng lớn dữ liệu tại cùng một thời điểm và có phức tạp khi đã nhận được dữ liệu.
- TCP header** **TCP header** (Tiêu đề TCP) là phần đầu tiên của một [TCP segment](#) (phân đoạn TCP) có kích thước thay đổi. Ví dụ khi không sử dụng thì có kích thước là 20 bytes.

TCP segment **Phân đoạn TCP** (TCP segment) là đơn vị truyền dẫn trong [TCP](#). Nó bao gồm một tiêu đề TCP ([TCP header](#)) để cho các ứng dụng số liệu.

TCP/IP **TCP/IP** là viết tắt của **Transmission Control Protocol/ Internet Protocol** (Giao thức điều khiển truyền dẫn/ Giao thức Internet). Mặc dù tênTCP/IP chỉ gồm hai giao thức, thực ra nó gồm rất nhiều các giao thức khác nhau gọi là một họ hay một nhóm giao thức.

TFTP **Trivial File Transfer Protocol** (Giao thức truyền tệp thông thường) TFTP là giao thức truyền số liệu hỗ trợ rất ít lệnh và không có độ tin cậy cao. Tuy nhiên, TFTP là giao thức truyền số liệu tốc độ cao.

TR **Token Ring** là kỹ thuật của tầng Liên kết. Mạng Token Ring thường có cấu hình dạng vòng ring.

TTL **Time-To-Live** (Trường thời gian sống) trong tiêu đề IP ([IP header](#)) chỉ ra thời gian tồn tại của một gói IP ([IP datagram](#)) trước khi nó bị router xóa đi.

U

UDP **User Datagram Protocol** (Giao thức gói người dùng) UDP là giao thức chính thứ hai của tầng giao vận sau [TCP](#). Ngược lại với TCP, UDP cung cấp thông tin không kết nối và không đảm bảo gói dữ liệu có thể đến đích. Thông thường, các chương trình sử dụng UDP chỉ truyền một khối lượng nhỏ dữ liệu tại một thời điểm.

O

VCI Chỉ số nhận dạng kênh ảo VCI được chứa trong phần tiêu đề [ATM](#) và có khả năng hỗ trợ tới 65.536 kênh ảo riêng biệt với mỗi mạch ảo.

VPI Chỉ số nhận dạng mạch ảo VPI chứa trong phần tiêu đề [ATM](#) của gói dữ liệu và có khả năng hỗ trợ 4.069 mạch ảo cho mỗi kết nối