

BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC QUỐC GIA VIỆT NAM
LOAN N^o 1718 - VIE (SF)

NGUYỄN VŨ QUỐC HUNG (Chủ biên) - NGUYỄN THẾ LỘC

MẠNG MÁY TÍNH



Thư viện ĐH Trà Vinh



1 1 0 6 9 5 9

65
56
2005

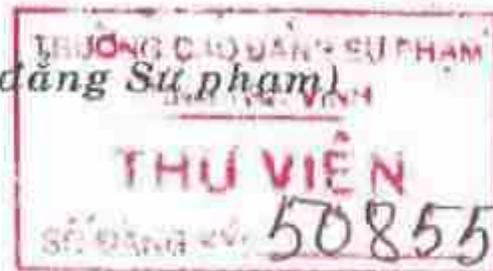


NHÀ XUẤT BẢN ĐẠI HỌC SƯ PHẠM

NGUYỄN VŨ QUỐC HƯNG (Chủ biên)
NGUYỄN THẾ LỘC

MẠNG MÁY TÍNH

(Giáo trình Cao đẳng Sư phạm)



NHÀ XUẤT BẢN ĐẠI HỌC SƯ PHẠM

MỤC LỤC

LỜI NÓI ĐẦU.....7

CHƯƠNG 1

KHÁI NIỆM CƠ BẢN VỀ MẠNG MÁY TÍNH

1.	SỰ CẦN THIẾT PHẢI NỐI MẠNG MÁY TÍNH	9
2.	ÍCH LỢI CỦA MẠNG	10
3.	PHÂN LOẠI MẠNG	10
3.1.	Khái niệm LAN, MAN, WAN	10
3.2.	Mô hình mạng sơ khai.....	11
3.3.	Mạng dựa trên Server (Server Based)	12
3.4.	Mạng ngang hàng (Peer to Peer).....	13
3.5.	Mạng kết hợp.....	14
4.	KIẾN TRÚC MẠNG	15
4.1.	Khái niệm Topology.....	15
4.2.	Lược đồ Bus (kiến trúc tuyến tính)	16
4.3.	Lược đồ Star (kiến trúc hình sao)	18
4.4.	Lược đồ Ring (kiến trúc vòng).....	20
4.5.	Các lược đồ biến thể.....	22
	CÂU HỎI CUỐI CHƯƠNG	24

CHƯƠNG 2

CÁC THÀNH PHẦN CƠ BẢN CỦA MẠNG

1.	ĐƯỜNG TRUYỀN MẠNG	27
1.1.	Các đặc trưng của đường truyền	27
1.2.	Chế độ truyền băng tần cơ sở và chế độ băng tần rộng.....	28
1.3.	Cáp đồng trục (Coaxial Cable).....	29
1.4.	Cáp xoắn (Twisted Pair Cable).....	31
1.5.	Cáp quang (Fiber Optic Cable).....	33

1.6.	So sánh các loại cáp.....	35
1.7.	Truyền thông trên mạng vô tuyến	35
2.	BẢNG MẠCH GIAO TIẾP MẠNG.....	49
2.1.	Tên gọi và chức năng.....	49
2.2.	Các tham số cấu hình.....	51
2.3.	Kiến trúc bus	54
2.4.	Boot ROM.....	55
3.	TRÌNH ĐIỀU KHIỂN.....	55
3.1.	Vai trò, chức năng của trình điều khiển	55
3.2.	Trình điều khiển cho NIC.....	56
3.3.	Xuất xứ của trình điều khiển	57
3.4.	Cài đặt.....	58
CÂU HỎI CUỐI CHƯƠNG		59

CHƯƠNG 3 MỘT SỐ MÔ HÌNH MẠNG

1.	MÔ HÌNH OSI.....	61
1.1.	Bối cảnh ra đời.....	61
1.2.	Kiến trúc phân tầng	62
1.3.	Giới thiệu mô hình OSI.....	63
1.4.	Tầng Vật lí.....	66
1.5.	Tầng Liên kết dữ liệu	68
1.6.	Tầng Mạng.....	89
1.7.	Tầng Giao vận.....	98
1.8.	Tầng Phiên.....	105
1.9.	Tầng Trình diễn.....	110
1.10.	Tầng Ứng dụng.....	112
1.11.	An toàn thông tin trên mạng (network securiti)	113
1.12.	Giao thức quản lí mạng đơn giản	126
2.	MÔ HÌNH TCP/IP.....	127
2.1.	Phân tầng TCP/IP	127
2.2.	Bộ giao thức TCP/IP.....	129
CÂU HỎI CUỐI CHƯƠNG		130

CHƯƠNG 4

GIAO THỨC

1.	CHỨC NĂNG CỦA GIAO THỨC	133
2.	GIAO THỨC TRONG KIẾN TRÚC PHÂN TẦNG	135
3.	CÁC GIAO THỨC CHUẨN	137
4.	CÀI ĐẶT VÀ GỠ BỎ GIAO THỨC	141
	CÂU HỎI CUỐI CHƯƠNG	144

CHƯƠNG 5

QUẢN TRỊ MẠNG

1.	QUẢN LÝ TÀI KHOẢN MẠNG.....	145
1.1.	Khái niệm tài khoản (Account).....	145
1.2.	Chiến lược quản trị tài khoản.....	146
2.	PHÒNG CHỐNG MẤT DỮ LIỆU.....	148
2.1.	Những nguy cơ đe dọa dữ liệu	148
2.2.	Các hệ thống dung lỗi.....	149
2.3.	Lưu trữ dự phòng	154
	CÂU HỎI CUỐI CHƯƠNG	158

CHƯƠNG 6

HỆ ĐIỀU HÀNH WINDOWS 2000 SERVER

1.	CÀI ĐẶT	159
1.1.	Yêu cầu phần cứng	159
1.2.	Trù tính trước khi tiến hành cài đặt	160
1.3.	Các giai đoạn cài đặt Windows 2000 Server.....	162
2.	TÌM HIỂU ACTIVE DIRECTORY.....	166
2.1.	Miền (domain).....	166
2.2.	Nhóm (group).....	167
2.3.	Đơn vị tổ chức (Organization Unit - OU)	170
2.4.	Địa bàn (site)	170
2.5.	Cây và rừng.....	171

3.	MỘT SỐ CÔNG CỤ CỦA WINDOWS 2000.....	172
3.1.	Chức năng Network	172
3.2.	Sơ lược về Microsoft Management Console (MMC).....	179
3.3.	Quản lí các thiết bị phần cứng bằng Device Manager	182
4.	QUẢN LÝ CÁC TÀI KHOẢN NGƯỜI DÙNG.....	185
4.1.	Tạo và quản lí các tài khoản tại chỗ.....	185
4.2.	Tạo tài khoản trên miền bằng Active Directory Users and Computers	186
5.	CHIA SẺ FILE VÀ FOLDER TRÊN MẠNG.....	194
5.1.	Tạo và quản lí các folder dùng chung.....	194
5.2.	Quyền truy cập ở cấp Share.....	196
5.3.	Các Permission chi tiết	198
5.4.	Phân bố Permission trên File và Folder	199
6.	CHIA SẺ MÁY IN TRÊN MẠNG.....	201
6.1.	Chia sẻ máy in từ Print Server.....	201
6.2.	Kết nối vào máy in mạng từ một máy trạm.....	204
	BÀI TẬP CUỐI CHƯƠNG	207
	BẢNG TRA CỨU THUẬT NGỮ.....	208
	TÀI LIỆU THAM KHẢO.....	226

Lời nói đầu

Giáo trình này được viết cho sinh viên các trường Cao đẳng Sư phạm ngành Tin học theo chương trình khung đã được Bộ Giáo dục và Đào tạo ban hành, nó cũng có thể dùng làm giáo trình tham khảo cho những ai có ý định tìm hiểu những kiến thức cơ bản về mạng máy tính. Để học tốt giáo trình này cần phải nắm vững những kiến thức về Tin học cơ sở, Kiến trúc máy tính và Quản lí hệ thống máy tính.

Giáo trình biên soạn nhằm đạt được những mục tiêu sau:

- Cung cấp cho sinh viên những khái niệm về mô hình công nghệ kết nối cơ bản của mạng máy tính.
- Giúp sinh viên biết lắp đặt, quản trị mạng máy tính, sử dụng một số phần mềm cơ bản của mạng.

Giáo trình gồm có 6 chương, để học mỗi chương cần có các kiến thức của chương trước.

Chương 1 giới thiệu về các khái niệm cơ sở về mạng. Chương này cung cấp những khái niệm cơ bản hết sức quan trọng về mạng như: mô hình LAN, lược đồ mạng...

Chương 2 giới thiệu về các thành phần cơ bản của mạng máy tính. Chương này cung cấp cho sinh viên những kiến thức về các thành phần vật lí cấu tạo nên mạng máy tính. Chúng gồm môi trường truyền thông, bảng mạch và phần mềm điều khiển mạng.

Chương 3 giới thiệu về mô hình kiến trúc và nguyên lí kết nối của mạng. Chương này tập trung mô tả Mô hình tham chiếu hệ thống mở OSI, Project 802 của IEEE và mô hình TCP/IP.

Chương 4 giới thiệu về các giao thức mạng. Chương này mô tả khái niệm giao thức trong các hoạt động của mạng. Tập trung giải thích vai trò của giao thức và mô tả phương thức hoạt động của các giao thức.

Chương 5 nói về các khái niệm và hoạt động quản trị mạng. Mạng máy tính không thể tự hoạt động mà phải có người *quản trị mạng*, công việc chính của họ là quản lí tài khoản người dùng và các tài nguyên. Chương này trình bày khái quát về những công việc đó.

Chương 6 giới thiệu tóm tắt về cách sử dụng hệ điều hành Windows 2000 Server trong quản trị mạng. Chương này trình bày tóm lược cách cài

đặt, vận hành khai thác và quản trị một trong những hệ điều hành mạng phổ biến nhất hiện nay, đó là Windows 2000 Server cùng với các máy trạm.

Khi biên soạn giáo trình này chúng tôi đã tham khảo các tài liệu trong và ngoài nước cùng với các bài giảng về mạng máy tính đã thực hiện cho nhiều khóa đào tạo cử nhân Công nghệ thông tin. Chúng tôi xin chân thành cảm ơn các đồng nghiệp đã đóng góp ý kiến, đặc biệt chúng tôi xin cảm ơn PGS. TS. Hồ Sỹ Đàm đã góp ý về cấu trúc giáo trình, TS. Trần Công Nhung và TS. Nguyễn Mạnh Hùng đã dành nhiều thời gian đọc kỹ và có những ý kiến sâu sắc.

Tuy có rất nhiều cố gắng trong công tác biên soạn nhưng chắc chắn cuốn sách còn nhiều thiếu sót, nhiều vấn đề còn cần phải bổ sung. Chúng tôi rất mong nhận được các ý kiến đóng góp để cuốn sách được hoàn thiện hơn trong lần xuất bản sau.

Các ý kiến đóng góp xin gửi về: hungnvq@dhsphn.edu.vn hoặc hungnvq@hnue.edu.vn; lnguyen@jaist.ac.jp

Các tác giả

KHÁI NIỆM CƠ BẢN VỀ MẠNG MÁY TÍNH

Chương này giúp độc giả trả lời câu hỏi "Tại sao phải nối mạng máy tính?" và cung cấp những khái niệm cơ bản hết sức quan trọng về mạng như mô hình LAN, lược đồ mạng...

1. SỰ CẦN THIẾT PHẢI NỐI MẠNG MÁY TÍNH

Khái niệm *môi trường làm việc độc lập* (stand alone environment): Khi một cụm máy tính tuy đặt cạnh nhau, cùng hướng về một mục đích chung nhưng không trao đổi dữ liệu cũng như chia sẻ thông tin với nhau thì ta gọi môi trường đó là môi trường của các máy độc lập. Chúng ta cùng xem xét những trường hợp thực tế sau đây.

Một văn phòng với 10 máy tính do 10 nhân viên sử dụng. Trung bình mỗi người cần in khoảng 10 trang giấy một ngày, văn phòng có 2 máy in. Nếu những máy tính của họ là độc lập thì mỗi khi cần in họ phải sao dữ liệu lên đĩa, mang tới máy tính có kết nối máy in và in nhờ.



Rõ ràng mô hình này có nhiều bất tiện. Đó là thời gian chờ đợi, nhất là những thời điểm công việc dồn đến nhiều có thể các nhân viên phải xếp hàng chờ đến lượt được in, môi trường làm việc của nhân viên không được độc lập thoải mái. Tất nhiên có thể trang bị cho mỗi máy tính một máy in kèm theo. Giải pháp này lãng phí và quan trọng hơn là không phải bao giờ cũng giải quyết được vấn đề. Hãy xét một ví dụ khác.

Tại chi nhánh thứ nhất của ngân hàng, nhân viên A của công ti X đến rút tiền mặt. Sau đó tại chi nhánh thứ hai – ở cách xa chi nhánh thứ

nhất – nhân viên B cũng của công ti X đến rút tiền. Làm sao nhân viên ngân hàng biết được số tiền này có vượt quá số còn lại trong tài khoản hay không nếu như thời điểm giao dịch của A và B chỉ cách nhau vài phút, lại ở vị trí địa lí cách xa nhau?



Giải pháp cho tất cả những vấn đề trên là: nối mạng máy tính.

2. ÍCH LỢI CỦA MẠNG

Ngày nay, ta có thể bắt gặp những mạng máy tính ở khắp nơi, từ những cửa hàng "Game nối mạng" ngoài phố cho đến các những mạng tác nghiệp lớn tại các công sở ngân hàng, các mạng cấp bộ hay cấp quốc gia. Tổng kết lại mạng có thể giúp các máy trạm chia sẻ những tài nguyên sau đây:

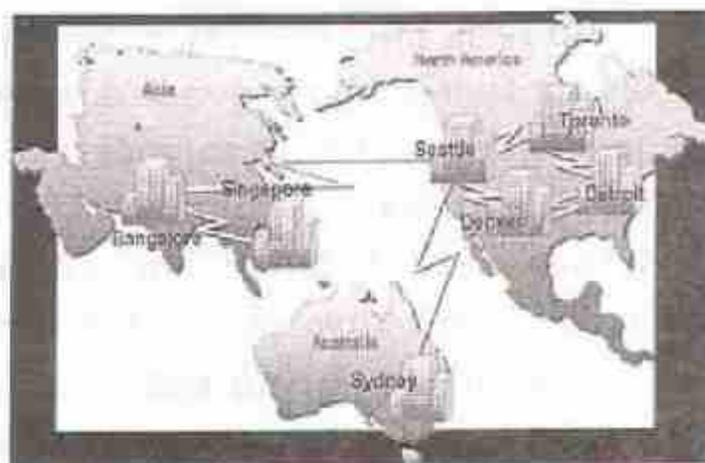
- Dữ liệu tác nghiệp.
- Những thông tin nóng, cần chuyển nhanh như: thông báo (message), thư tín điện tử (email).
- Các tài nguyên cứng: máy in, fax / modem, camera...
- Năng lực tính toán của CPU, tài nguyên RAM, Hard disk...

3. PHÂN LOẠI MẠNG

3.1. Khái niệm LAN, MAN, WAN

Mạng LAN (Local Area Network – mạng cục bộ): là mô hình mạng cỡ nhỏ, nối kết các máy tính trong phạm vi một văn phòng, một cơ quan nhỏ. Nói chung số lượng máy trạm từ vài chục đến vài trăm máy, khoảng cách xa nhất cỡ vài trăm mét thì được coi là mạng LAN. Các thiết bị mạng có thể sử dụng những công nghệ rẻ tiền và đơn giản.

Mạng MAN (Metropolitan Area Network – mạng thành phố): là mạng được lắp đặt trong phạm vi



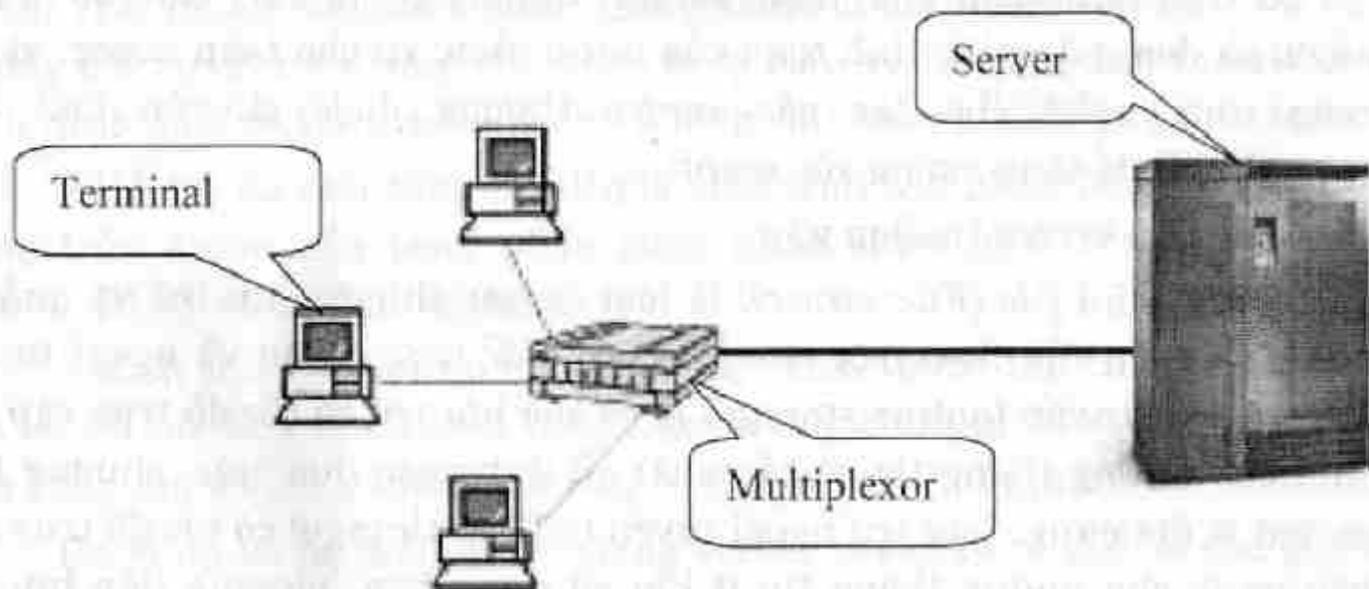
một đô thị hay một trung tâm kinh tế với bán kính khoảng vài chục kilômet. Kỹ thuật lắp đặt và giá thành cao hơn LAN.

Mạng WAN (Wide Area Network – mạng diện rộng) có thể bao phủ một phạm vi rộng lớn, thậm chí ra ngoài địa cầu. WAN thường được hình thành từ nhiều LAN, MAN hợp lại. Internet là một ví dụ về mạng WAN. Đã có những con tàu vũ trụ kết nối thông tin với trái đất thông qua Internet. WAN chia thành hai loại:

- WAN dành cho bộ, ngành, tổ hợp công nghiệp (Enterprise WAN). Loại này có tính chuyên môn hóa cao, mang tính đặc thù của ngành.
- WAN công cộng: phục vụ cho toàn thể cộng đồng xã hội. Ví dụ như Internet.

3.2. Mô hình mạng sơ khai

Từ những năm 1960, đã xuất hiện những mạng máy tính gồm những *thiết bị đầu cuối* (terminal) được nối với một server (máy xử lý trung tâm) thông qua những thiết bị *dồn kênh* (multiplexor).



Hình 1.1. Sơ đồ mạng sơ khai

Đặc điểm của mô hình này là mọi công việc xử lý, tính toán đều tập trung về thực hiện tại server, vì thế đây thường là một máy mini hay main-frame rất mạnh. Còn các trạm đầu cuối chỉ là các thiết bị vào ra đơn giản lo việc nạp và chuyển yêu cầu về server, sau đó nhận kết quả từ server và hiển thị lên màn hình.

3.3. Mạng dựa trên server (Server Based)

3.3.1. Đặc trưng

- Được thiết kế cho các mạng quy mô lớn, số máy trạm (client) có thể lên tới hàng ngàn.
- Phần lớn tài nguyên quan trọng tập trung tại các server.
- Các tài nguyên được quản lý và chia sẻ một cách có tổ chức.
- Người sử dụng (user) chia thành nhiều cấp với những mức quyền hạn tương ứng.
- Có những người quản trị mạng chuyên nghiệp (administrator) lo việc quản lý tài nguyên và các user.
- Tính an toàn và độ bảo mật cao.
- Nhưng kèm theo là chi phí lắp đặt, huấn luyện sử dụng và phí bảo trì cũng cao. Hệ thống có thể khó sử dụng.

3.3.2. Khái niệm, phân loại server

Ở trên ta đã gặp khái niệm server, thường gọi là máy chủ, đó là một máy tính đem năng lực tính toán của mình phục vụ cho toàn mạng, vì thế trong công nghệ chế tạo các server thường được chuyên biệt hóa (specialized) để tăng cường sức mạnh.

Các loại server thường gặp:

– *Máy chủ file (File server)*: là loại server chuyên lưu trữ và quản lý các tài nguyên file theo một trong hai cơ chế: trực tuyến và ngoại tuyến. Lưu trữ trực tuyến (online storage) là cơ chế lưu trữ có tốc độ truy cập cao dành cho những thông tin có tần suất sử dụng cao dựa trên phương tiện lưu trữ là đĩa cứng. Lưu trữ ngoại tuyến (offline storage) có tốc độ truy cập thấp dành cho những thông tin ít khi sử dụng hơn, phương tiện lưu trữ thường là băng từ, đĩa quang. Các file server luôn được trang bị những ổ đĩa dung lượng rất lớn, tốc độ truy xuất cao như đĩa cứng Fast wide SCSI, tủ băng từ, tủ đĩa quang...

– *Máy chủ in ấn (Print server)*: quản lý các máy in và những thao tác in ấn của người dùng trên mạng. Print server có thể là một thiết bị vật lý hay chỉ do một phần mềm đảm nhiệm.

– *Máy chủ truyền thông (Communication server)*: có thể bao gồm mail server, fax server. Chức năng của loại server này là quản lý luồng dữ

liệu, e-mail, message với bên ngoài. Các chức năng Firewall (tường lửa), proxy có thể được cài đặt tại Communication server. Loại server này được trang bị những thiết bị truyền thông đặc biệt như cầu nối (bridge), bộ định tuyến (route), cáp quang...

– *Máy chủ ứng dụng* (Application server): khi một câu hỏi truy vấn (query) được đưa tới cho file server, toàn bộ cơ sở dữ liệu có chứa thông tin cần tìm sẽ được gửi trả cho máy trạm. Còn Application server, thông qua một phần mềm quản trị được thiết kế để chạy trên server, sẽ tìm và chỉ gửi cho máy trạm đúng những bản ghi cần thiết.

3.3.3. Hệ điều hành mạng Server based

Các server được chế tạo đặc biệt và được trang bị mạnh. Để khai thác tốt nền tảng phần cứng đó, hệ điều hành mạng (NOS – Network Operating System) cần phải có những tính năng tương ứng. Đó là:

– SMP (Symmetric Multi Processing – đa xử lý đối xứng) khi server có nhiều CPU, tính năng SMP giúp hệ điều hành mạng chia công việc thành nhiều phần tương đương và giao cho mỗi CPU đảm nhiệm một phần. Trái ngược với SMP, AMP (Assymmetric Multi Processing – đa xử lý không đối xứng) chia công việc theo từng loại, ví dụ như: tính toán số học, xử lý hình ảnh và âm thanh, ... chứ không chia theo khối lượng tính toán.

– Hỗ trợ đa nền tảng (Multiple platform) cho phép NOS có thể hoạt động trên nhiều nền tảng phần cứng khác nhau như: Intel x86, MIPS R4000, RISC và Digital Alpha...

– Kích thước phân vùng (partition), kích thước tập tin cho phép rất lớn so với hệ điều hành trên máy trạm thông thường. Ví dụ Windows NT cho phép tệp với kích thước lên đến 16 Exa byte (2^{34} Gyga byte).

Để ví dụ về hệ điều hành mạng server based ta có thể kể tên một số đại biểu như:

Novell Netware 3.11, 4.1

Windows NT server, Windows 2000 server.

IBM OS/2 LAN Server.

3.4. Mạng ngang hàng (Peer to Peer)

Có nhiều cách dịch tên mô hình mạng này: mạng ngang hàng, mạng đồng đẳng.

3.4.1. Đặc trưng

- Thích hợp với các mạng quy mô nhỏ, trên dưới 10 máy trạm trong bán kính vài chục mét.
- Tài nguyên rải khắp toàn mạng.
- Không có server chuyên dụng và những người quản trị mạng chuyên nghiệp.
- Mọi máy trạm đều bình đẳng. Các user tự quản lý tài nguyên của mình.
- Chi phí lắp đặt thấp, dễ sử dụng.
- Tính an toàn, độ bảo mật không cao.

3.4.2. Một số hệ điều hành mạng Peer to Peer tiêu biểu

- Microsoft Windows for Workgroup 3.11
- MS. Windows 9x, Windows 2000, Windows XP
- MS Windows NT Workstation
- Novell Personal Netware
- AppleTalk (cho hệ máy Apple Macintosh)
- Artisoft LAN tastic

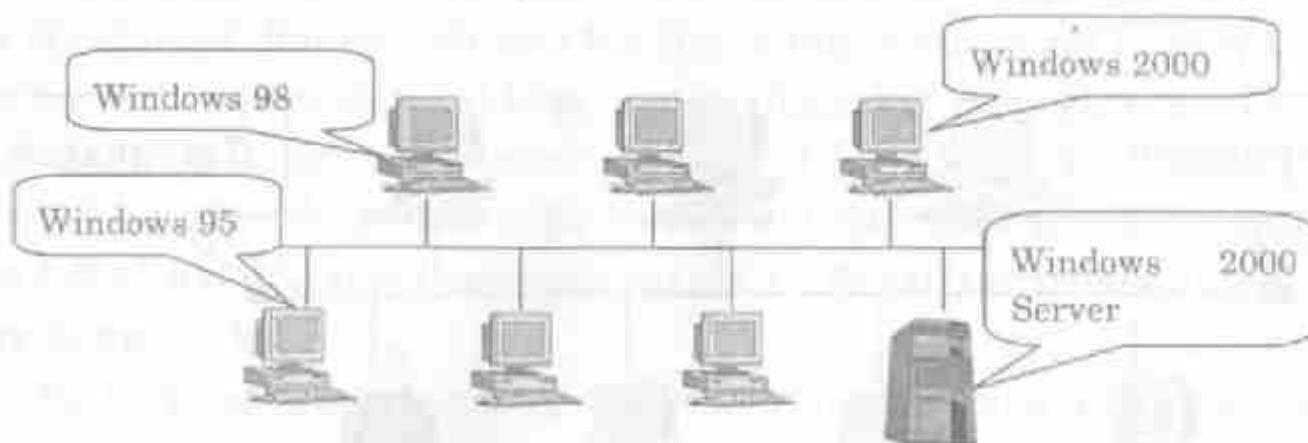
3.5. Mạng kết hợp

Chúng ta nhận thấy hai loại mạng nêu trên hoàn toàn trái ngược nhau về mọi tiêu chí: quy mô, tính an toàn, chi phí, phân bố tài nguyên. Nguồn gốc căn bản của mọi sự khác nhau là cách thức quản lý tài nguyên của chúng. Chính vì tài nguyên được tập trung vào một nơi nên mạng Server based cần có nơi để lưu trữ (các máy server), cần người quản lý kho tài nguyên đó (administrator), và do đó có độ an toàn cao, nhưng cũng kéo chi phí lên cao. Không có tất cả những điều đó nên mạng Peer to Peer có chi phí thấp nhưng đồng thời lỏng lẻo, tính bảo mật thấp.

Cả hai loại mạng trên đều có những ưu điểm và nhược điểm, ưu điểm của loại này là nhược điểm của loại kia. Để dung hòa, người ta đã đề xuất mô hình Mạng kết hợp nhằm phối hợp các tính năng tốt và hạn chế bớt nhược điểm của chúng.

Chúng ta cùng xem xét giải pháp mạng kết hợp của Microsoft. Mạng gồm có máy server và các máy trạm, trên server cài đặt hệ điều hành

Windows NT Server hay Windows 2000 Server (thuộc loại server based). Server chịu trách nhiệm chia sẻ các ứng dụng và dữ liệu chính trên mạng.



Hình 1.2. Sơ đồ mạng kết hợp

Các máy trạm sử dụng Windows 9x (thuộc loại Peer to Peer), chúng vừa có thể truy cập để sử dụng các tài nguyên trên server, vừa có sẵn dữ liệu cá nhân trên đĩa cứng của mình để sử dụng. Rõ ràng là với mô hình này, người quản trị mạng sẽ tốn rất nhiều công sức hoạch định, duy trì độ an toàn và tính dễ sử dụng của mạng.

4. KIẾN TRÚC MẠNG

4.1. Khái niệm Topology

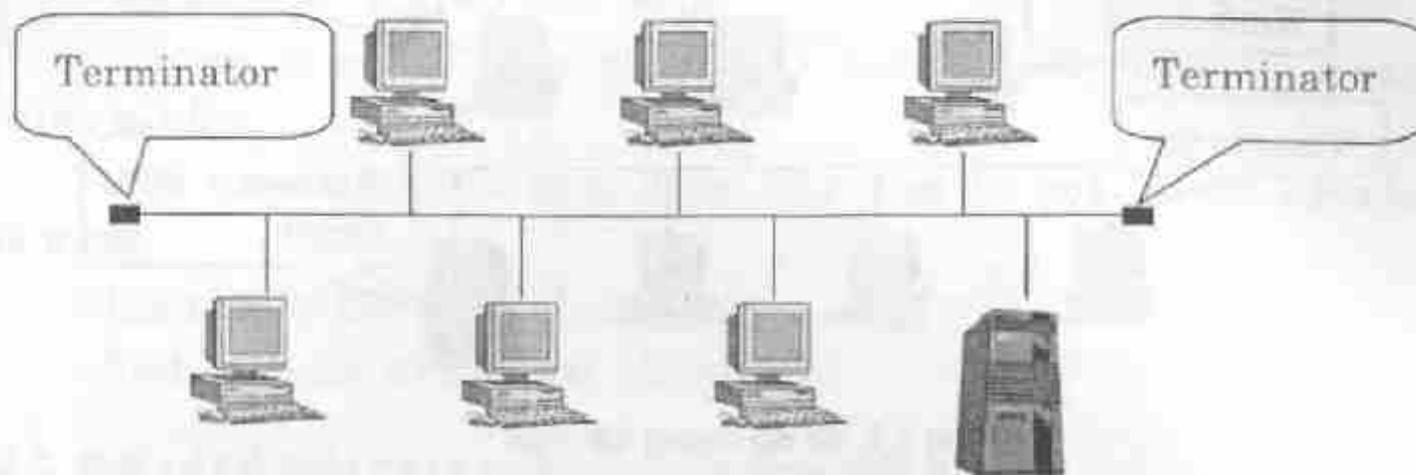
Trong tiếng Anh có nhiều thuật ngữ được sử dụng để chỉ khái niệm này, ví dụ như Physical layout, Network design, Diagram, Map... Cũng đã có nhiều cách dịch thuật ngữ này sang tiếng Việt như: cấu hình mạng, kiến trúc mạng, lược đồ mạng... Chúng ta quy ước sẽ sử dụng cách gọi sau cùng. Có thể định nghĩa Topology – lược đồ mạng – là kiểu sắp xếp, bố trí các máy trạm, dây cáp và các thiết bị mạng khác trên phương diện vật lý. Việc lựa chọn topology khi thiết kế mạng là rất quan trọng vì nó sẽ quyết định:

- Chung loại thiết bị mạng sẽ sử dụng.
- Khả năng của mạng.
- Tương lai phát triển của mạng sau này.
- Cách thức quản lý, bảo trì mạng.

Vì vậy chúng ta cần hiểu thấu đáo các kiểu lược đồ mạng để có lựa chọn thích hợp.

4.2. Lược đồ Bus (kiến trúc tuyến tính)

4.2.1. Sơ đồ



Hình 1.3. Sơ đồ kiến trúc tuyến tính

4.2.2. Đặc trưng

Chỉ có một đường cáp duy nhất chạy xuyên suốt nối các máy trạm với nhau. Tất cả các trạm cùng dùng chung đường truyền này. Tín hiệu từ một trạm được phát đi theo cả hai chiều.

Hai đầu cáp phải được gắn bởi một thiết bị gọi là *terminator* (thiết bị chống dội tín hiệu). Các máy trạm được nối vào mạng nhờ thiết bị *T-connector*.



Terminator

Mỗi thời điểm chỉ một trạm được gửi dữ liệu, gói dữ liệu này đi tới mọi trạm khác trên mạng nhưng chỉ có trạm đích, sau khi so khớp địa chỉ của mình với địa chỉ ghi trên gói, nhận gói dữ liệu này.

Bus là cấu hình thụ động, nghĩa là máy trạm chỉ *lắng nghe* đường truyền để thu nhận gói tin, nếu thấy một gói tin không phải gửi cho mình thì máy trạm không làm gì thêm, nghĩa là nó không chịu trách nhiệm chuyển gói tin đó cho máy kế tiếp.

Do mỗi lần chỉ có một trạm được quyền gửi, nên khi số máy trạm tăng lên thì hiệu suất của mạng giảm nhanh chóng, số máy phải chờ và thời gian chờ để gửi càng tăng lên.

4.2.3. Sự cố trên mạng bus (đọc)

Hiện tượng dội tín hiệu: như ta đã biết, khi một trạm gửi dữ liệu, tín hiệu đó sẽ đi từ đầu này tới đầu kia của mạng. Nếu không có gì chặn lại, tín hiệu sẽ dội lại và đi mãi không ngừng chiếm hết đường truyền. Do đó ở hai đầu cáp phải gắn terminator – thiết bị chống dội tín hiệu. Nhưng nếu vì một lí do nào đó cáp đứt giữa chừng, khi đó mạng bị tách thành hai phần mà cả hai đều thiếu một terminator, do đó lập tức truyền thông trên mạng bị ngừng lại.

Xử lí: Trước hết ta phải tìm ra chỗ cáp bị đứt. Việc này có thể được thực hiện bằng cách lần lượt chặn terminator vào từng điểm có gắn T-connector để thu hẹp dần phạm vi tìm kiếm. Sau khi tìm ra vị trí đứt, ta thay thế đoạn cáp đó.

4.2.4. Khả năng mở rộng (đọc)

Mạng bus có thể được mở rộng bằng cách sử dụng các thiết bị sau:

- Barrel connector (bộ nối trực tròn) hay T-connector
- Repeater (bộ lặp)
- Multiport (các bộ chuyển tiếp đa cổng)

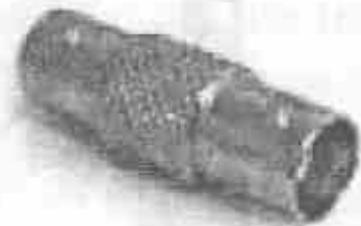
Trong các thiết bị trên, Barrel connector thô sơ nhất. Nó chỉ đơn thuần là cầu nối kim loại truyền dẫn tín hiệu điện tử, do đó sẽ làm yếu tín hiệu và có thể sinh nhiễu.

Repeater là thiết bị công nghệ cao với chức năng tái tạo và khuếch đại tín hiệu, lọc bỏ nhiễu để truyền tín hiệu được xa hơn. Bộ chuyển tiếp đa cổng không chỉ thực hiện được chức năng tái tạo tín hiệu mà còn có nhiều kiểu cổng cho phép nhiều loại cáp cắm vào (cáp đồng trục, cáp xoắn, cáp quang).

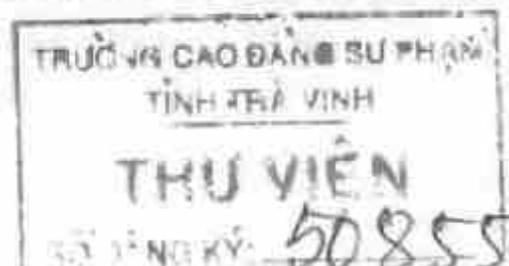
Khi tiến hành mở rộng bao giờ mạng bus cũng phải dừng hoạt động cho đến khi hoàn tất việc lắp đặt, điều này không thích hợp với những cơ quan cần hoạt động liên tục 24 giờ trong một ngày như mạng ngân hàng, an ninh, tổng đài viễn thông ...



T-connector

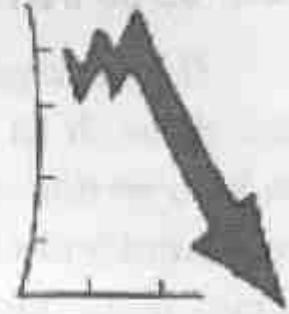


Barrel connector



4.2.5. Nhận xét

- Chi phí thấp, công nghệ thiết bị thường đơn giản.
- Tuy dễ lắp đặt nhưng việc bảo trì rất khó khăn.
- Mạng khó mở rộng quy mô. Khi số máy trạm tăng thì kéo theo hiệu suất mạng giảm nhanh chóng.
- Đã trở thành lỗi thời.



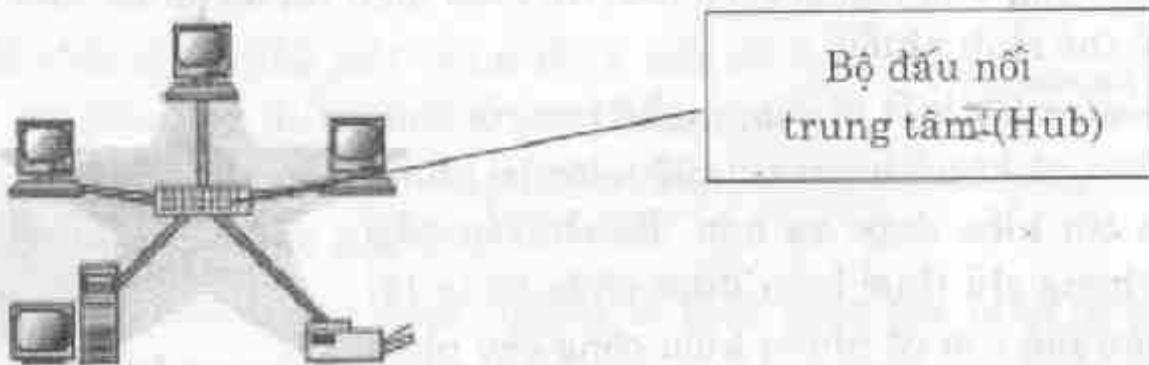
Hình 1.4. Sự hồi phục tín hiệu qua repeater

4.3. Lược đồ Star (kiến trúc hình sao)

4.3.1. Sơ đồ

Tất cả các trạm (kể cả máy in mạng, server,...) trên mạng đều nối cáp vào một thiết bị đấu nối trung tâm gọi là Hub.

4.3.2. Sự cố



Hình 1.5. Sơ đồ kiến trúc hình sao

Sự cố xảy ra trên đoạn cáp của trạm nào thì chỉ riêng trạm đó bị cô lập khỏi mạng, những trạm khác không bị ảnh hưởng gì.

Nếu sự cố xảy ra với bộ đấu nối trung tâm (Hub) thì toàn bộ truyền thông trên mạng bị ngưng ngay tức khắc.

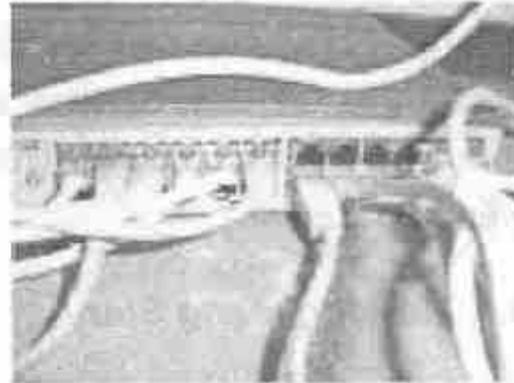
4.3.3. Các loại Hub

– Hub thụ động (*Passive Hub*)

Không cần nguồn điện nuôi vì nó cấu tạo rất đơn giản, không có một linh kiện điện tử nào. Hub thụ động chỉ là một thiết bị nối mạch đơn giản tương tự như một ổ cắm điện nhiều lỗ.

Không có chức năng lọc nhiễu cũng như tái tạo khuếch đại tín hiệu, ngược lại còn hấp thụ một phần tín hiệu.

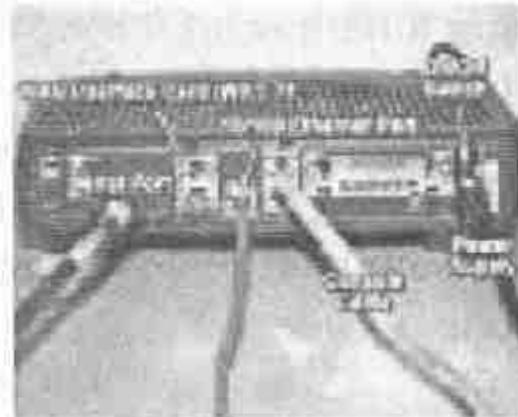
Do kĩ thuật thô sơ nên hiện nay Hub thụ động không còn được sử dụng nữa .



– Hub chủ động (*Active Hub*)

Phát triển hơn Hub thụ động, Hub chủ động cần nguồn nuôi để thực hiện chức năng lọc nhiễu, tái tạo và khuếch đại tín hiệu.

Tín hiệu nhận được từ một cổng sau khi được lọc nhiễu và khôi phục sẽ được phát ra tất cả các cổng của Hub.



– Hub lai (*Hybrid Hub*)

Là một bộ đầu nối có nhiều loại cổng giao tiếp cho phép cắm nhiều loại cáp.

– Hub thông minh (*Intelligent Hub*)

Là những Hub chủ động được bổ sung thêm những tính năng sau:

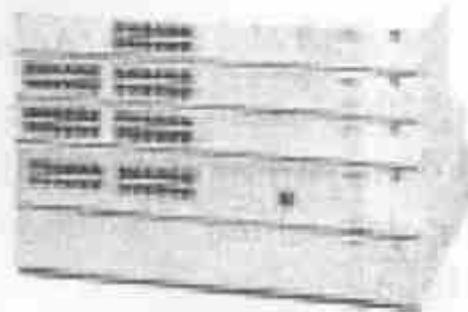
+ *Cho phép quản lí, điều khiển từ xa.* Bằng cách hỗ trợ các giao thức như SNMP (Simple Network Management Protocol: giao thức quản trị mạng đơn giản), Hub thông minh gửi những thông tin qua một cổng riêng về trung tâm quản trị mạng. Những thông tin này cho biết tình trạng hiện thời của Hub, chẳng hạn như cổng số mấy đang hoạt động, cổng nào không hoạt động, lưu lượng dữ liệu trên mạng đang quá tải... Đồng thời Hub thông minh nhận và thực hiện các chỉ lệnh từ trung tâm, chẳng hạn đóng (cắt kết nối) cổng nào đó, khôi phục kết nối cho một cổng khác... Tất nhiên để làm được việc đó, trung tâm mạng phải có những phần mềm thích hợp, ví dụ như phần mềm COMPAQ Insight Manager.

+ *Chuyển mạch*: là công nghệ mới nhất trong lĩnh vực chế tạo Hub. Hub chuyển mạch (Switching Hub) có những hệ định tuyến rất nhanh giữa các cổng. Khi nhận được gói dữ liệu, thay vì phát gói đó ra tất cả các cổng và làm bận đường truyền thì Switching Hub nhận ra và chỉ phát gói đó lên cổng tương ứng với trạm đích, nơi sẽ nhận gói tin đó. Một số Switching Hub còn có khả năng xác định đường truyền ngắn nhất tới trạm đích để gửi dữ liệu đi theo cổng tương ứng. Với những khả năng đó, các Switching Hub đang dần thay thế vai trò của cầu nối (Bridge) và bộ định tuyến (Router).

4.3.4. Mở rộng mạng Star

Có thể dễ dàng mở rộng quy mô cho mạng hình sao mà không cần ngưng hoạt động của mạng.

Việc mở rộng mạng, bổ sung thêm máy trạm thường sử dụng các Hub xếp chồng (Stackable hub), ổ gắn tường (wall plate).



4.3.5. Nhận xét

- Chi phí cao hơn lược đồ Bus.
- Công nghệ chế tạo hub, repeater... là những công nghệ tân tiến, thường xuyên ra đời những thế hệ sản phẩm mới.
- Việc lắp đặt, bảo trì, mở rộng rất dễ dàng thuận tiện, mạng không bị gián đoạn.
- Là lược đồ thông dụng nhất hiện nay.

4.4. Lược đồ Ring (kiến trúc vòng)

Đối với Ring ta phân biệt hai loại: lược đồ logic và lược đồ vật lý. Lược đồ vật lý mô tả hình dạng bên ngoài của mạng, chủng loại thiết bị và cách kết nối vật lý của chúng. Lược đồ logic thì chỉ ra đường truyền của tín hiệu bên trong mạng.

4.4.1. Lược đồ logic

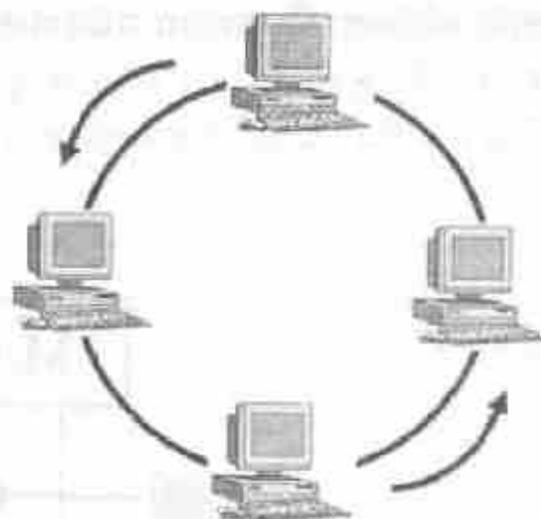
Phương pháp truyền tín hiệu trên mạng Ring có tên là Token-Passing (chuyển thẻ bài) gồm những quy định sau:

- Trên mạng luôn có duy nhất một token (thẻ bài) luân chuyển vòng quanh trên mạng.

- Trạm nào nhận được token thì được quyền phát dữ liệu trong một thời hạn nhất định. Sau đó phải chuyển token cho trạm kế tiếp.

- Gói tin được phát đi kèm theo token.

- Sau khi trạm đích nhận gói tin, nó đánh dấu và gửi trả gói tin về trạm phát kèm theo token.

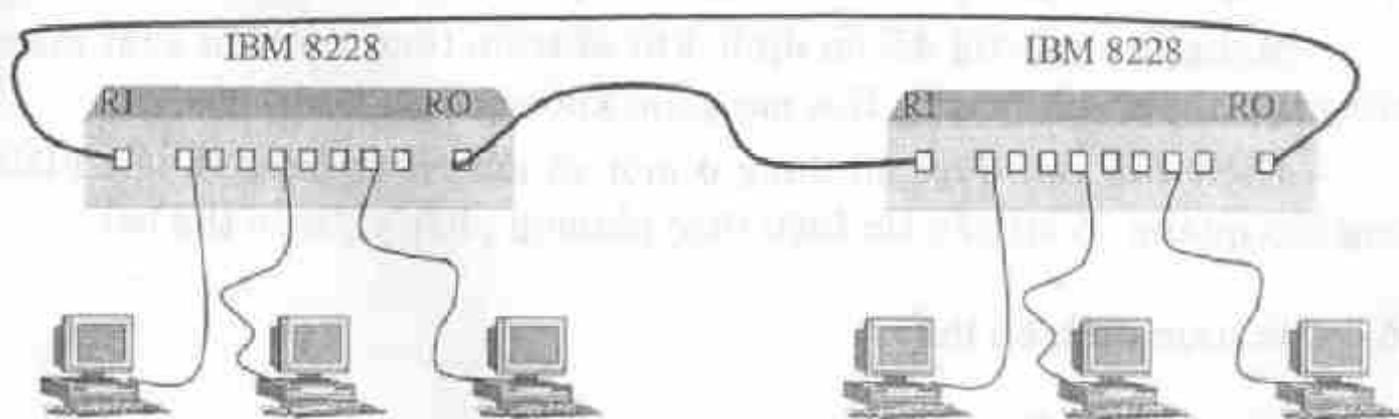


Ring là lược đồ chủ động, nghĩa là mỗi trạm khi nhận được một gói tin không phải của mình thì phát lại gói tới trạm tiếp sau.

Mỗi trạm đóng vai trò như một repeater, nghĩa là chuyển tiếp và khuếch đại tín hiệu tới máy trạm tiếp theo

4.4.2. Lược đồ vật lí

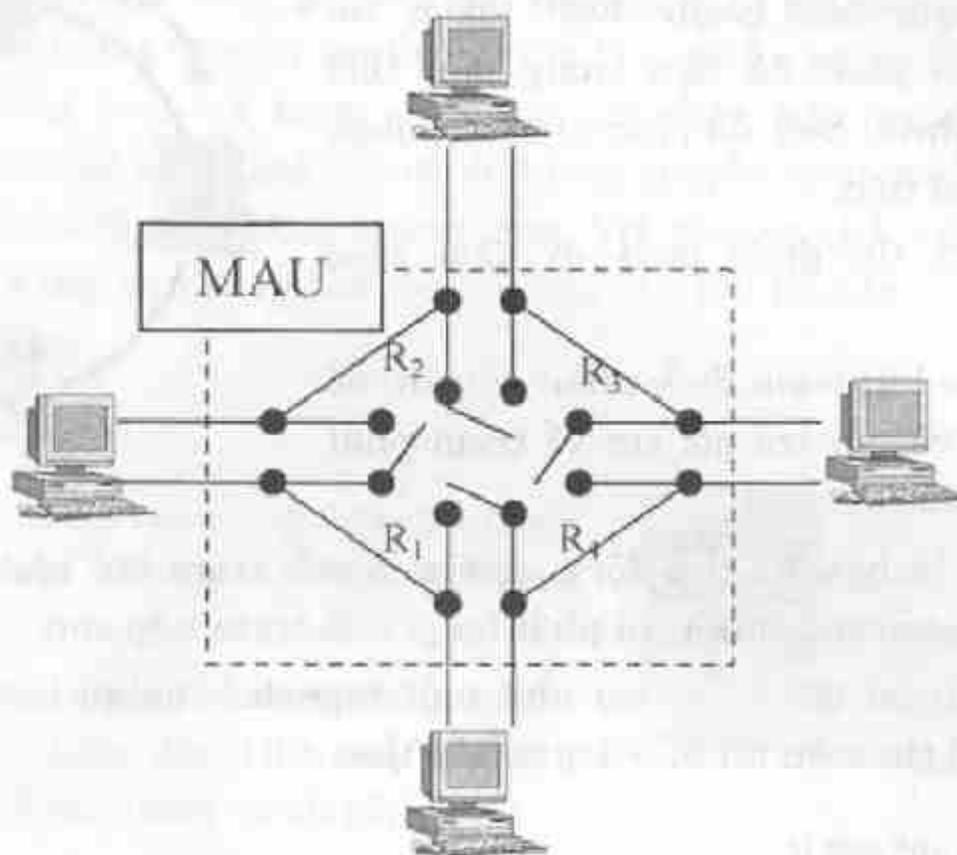
Các máy trạm nối cáp vào một thiết bị đầu nối trung tâm gọi là MAU (Multi station Access Unit). Chẳng hạn như loại IBM 8228 MAU có 8 cổng dành cho máy trạm và 2 cổng đặc biệt RI (Ring In) và RO (Ring Out) để kết nối các MAU với nhau (gần giống như các Hub xếp chồng trong kiến trúc hình sao).



Nguyên tắc hoạt động bên trong MAU

MAU gồm các cổng nối cáp với các trạm, mỗi cổng có một rơle RI. Khi máy trạm hoạt động, nó cung cấp nguồn điện làm mở rơle để tín hiệu từ

MAU đến được trạm. Khi trạm không hoạt động, role này đóng mạch, tín hiệu không vào trạm nữa mà đi tắt qua role.



Hình vẽ trên minh họa trường hợp 4 máy trạm đều hoạt động, các role đều mở.

4.4.3. Nhận xét

- Do có lược đồ vật lý hình sao nên việc mở rộng quy mô, cắm thêm trạm tương đối đơn giản, không gây gián đoạn mạng
- Mạng Ring tương đối ổn định, khi số trạm tăng thì hiệu suất mạng không sụt nhanh như mạng Bus mà giảm xuống chậm hơn.
- Hiện vẫn còn được sử dụng ở một số nơi, ví dụ như chuẩn FDDI dùng cáp quang và truyền tín hiệu theo phương pháp chuyển thể bài.

4.5. Các lược đồ biến thể

4.5.1. Lược đồ Star-Bus

Đây là sự kết hợp giữa hai lược đồ Star và Bus. Cáp nhánh từ mỗi Hub tỏa ra các máy trạm như cấu hình Star. Còn các Hub được liên kết với nhau theo kiểu Bus thông qua đường *cáp trục chính* (cáp back-bone). Đây thường là loại cáp có độ bền và tốc độ truyền tin cao.

4.5.2. Lược đồ Star-Ring

Trông bề ngoài lược đồ Star-Ring tương tự như Star-Bus, các đoạn cáp tới máy trạm đều tỏa ra từ các Hub. Tuy nhiên trong lược đồ Star-Ring các hub này được nối vào hub chính, và bên trong hub chính tín hiệu truyền đi theo một vòng (ring) thực sự.

CÂU HỎI CUỐI CHƯƠNG

1. Hãy xác định đâu là mạng cục bộ LAN trong các trường hợp sau và đánh dấu vào ô tương ứng.

- Ba máy tính và một máy in bố trí trong một văn phòng, nối với nhau thông qua Printer Switch box (một thiết bị cho phép 2, 4, 8 máy tính dùng chung một máy in) để dùng chung máy in.
- Hai máy tính, một ở Hà Nội, một ở Hòa Bình thường dùng chung dữ liệu và gửi e-mail cho nhau.
- Khoảng 200 máy tính trong một cơ quan – bố trí trong một tòa nhà 8 tầng – cùng sử dụng phần mềm MS Word để xử lý văn bản.
- Trên 100 máy tính của một cơ quan đặt trong 3 tầng của một tòa nhà, nối cáp với nhau để chia sẻ và dùng chung tập tin, máy in và gửi thông báo cho nhau.

2. Điền từ (cụm từ) vào chỗ trống để những câu sau trở thành những mệnh đề hợp lý

Lí do đầu tiên của việc lắp đặt mạng là để dùng chung.....

Tài nguyên..... thường được dùng chung trên mạng, ví dụ như máy in Laser.

Ngoài tài nguyên phần cứng ra, mạng còn dùng để chia sẻ và

3. Một văn phòng có nhiều máy tính để bàn và một máy in duy nhất. Để dùng chung máy in có 2 phương án:

a) Mỗi khi cần in thì ghi ra đĩa mềm mang sang máy khác in nhờ.

b) Nối mạng cục bộ để chia sẻ máy in.

Hãy đánh dấu vào trước các mệnh đề mà anh (chị) cho là đúng:

- Phương án a) so với b) có nhược điểm là dễ bị lây lan virus hơn do việc dùng chung đĩa mềm giữa các máy.
- Phương án a) gây nên sự gián đoạn công việc lẫn nhau giữa những người trong phòng.
- Phương án a) tiêu tốn thời gian hơn so với Phương án b)
- Hai phương án có chi phí xấp xỉ nhau: Phương án a) phải mua thêm đĩa mềm còn b) phải chi phí cho việc lắp đặt mạng.

4. Những hệ điều hành mạng sau đây thuộc loại nào: (gạch bỏ ý trả lời sai)

Windows NT Server 4.0	Peer to Peer	Server – Based
Windows for Workgroup 3.11	Peer to Peer	Server – Based
Windows NT Workstation 3.51	Peer to Peer	Server – Based
Windows 9x	Peer to Peer	Server – Based
Novell Netware 4.x	Peer to Peer	Server – Based

5. Trong mạng ngang hàng, mỗi máy tính có thể kiêm cả hai vai trò: và

6. Trên mạng Server – Based, loại máy phục vụ chuyên nhận và xử lý những yêu cầu (request) về dữ liệu và trả lại kết quả cho các máy trạm được gọi là:

- Specialized server (Server chuyên dụng)
- Application server
- File server
- Mail server

7. Mọi kiểu thiết kế mạng đều xuất phát từ 3 cấu hình cơ bản là: và

8. Khi nối cáp qua khoảng cách xa, tín hiệu được khuếch đại lên trước khi vượt qua khoảng cách cực đại bởi thiết bị có tên là

9. Mô tả nào đúng cho lược đồ Bus

- Cần nhiều cáp hơn các cấu hình khác
- Số lượng máy trạm không ảnh hưởng đến hiệu suất thi hành
- Thiết bị rẻ tiền và dễ lắp đặt
- Dễ bảo trì hơn các lược đồ khác

10. Trong lược đồ Bus, nếu cáp bị đứt tại một điểm thì toàn bộ mạng sẽ ngưng hoạt động.

- Đúng
- Sai

11. Trong lược đồ Ring, nếu cáp bị đứt tại một điểm thì toàn bộ mạng sẽ ngưng hoạt động.

- Đúng
- Sai

CÁC THÀNH PHẦN CƠ BẢN CỦA MẠNG

Chương này cung cấp cho sinh viên những kiến thức về các thành phần vật lý cấu tạo nên mạng máy tính. Chúng gồm môi trường truyền thông (đường truyền), bảng mạch và phần mềm điều khiển mạng.

1. ĐƯỜNG TRUYỀN MẠNG

1.1. Các đặc trưng của đường truyền

Băng thông (bandwidth – còn gọi là dải thông): Trong lĩnh vực truyền thông, băng thông của một đường truyền được hiểu là miền tần số của tín hiệu mà đường truyền đó chấp nhận. Còn trong mạng máy tính, băng thông đồng nghĩa với tốc độ truyền dữ liệu. Đơn vị đo băng thông là Hz ($1\text{Hz} = 1$ chu kì dao động trong 1 giây).

Ví dụ: một cáp truyền thông có băng thông từ 400 đến 4000Hz nghĩa là nó có thể truyền các tín hiệu với tần số từ 400 đến 4000 chu kì dao động /giây. Một mạng LAN có băng thông 100 Mbps nghĩa là nó có tốc độ truyền tin tối đa là 100 Megabit trong một giây.

Thông lượng (Throughput): chỉ tốc độ truyền dữ liệu của đường truyền. Đơn vị đo thông lượng là bps (bit per second – bit /giây).

Chú ý: thuật ngữ *băng thông* trong một số ngữ cảnh còn được dùng thay cho thuật ngữ *thông lượng* với ý nghĩa tương đương nhau, cùng để chỉ tốc độ truyền tin.

Sự suy giảm tín hiệu (attenuation): là hiện tượng tín hiệu bị yếu đi trong khi truyền trên đường truyền, các đặc trưng của tín hiệu điện như cường độ dòng điện, hiệu điện thế... bị suy giảm khi chiều dài cáp tăng lên. Đây là lí do khiến cho mỗi loại cáp đều có một giới hạn tối đa về độ dài, vượt quá giới hạn đó tín hiệu sẽ bị suy yếu đến mức không thể nhận dạng nổi.

— **Nhiều điện từ** (electromagnetic interference – EMI): là hiện tượng các sóng điện từ trong môi trường bên ngoài làm biến dạng tín hiệu được

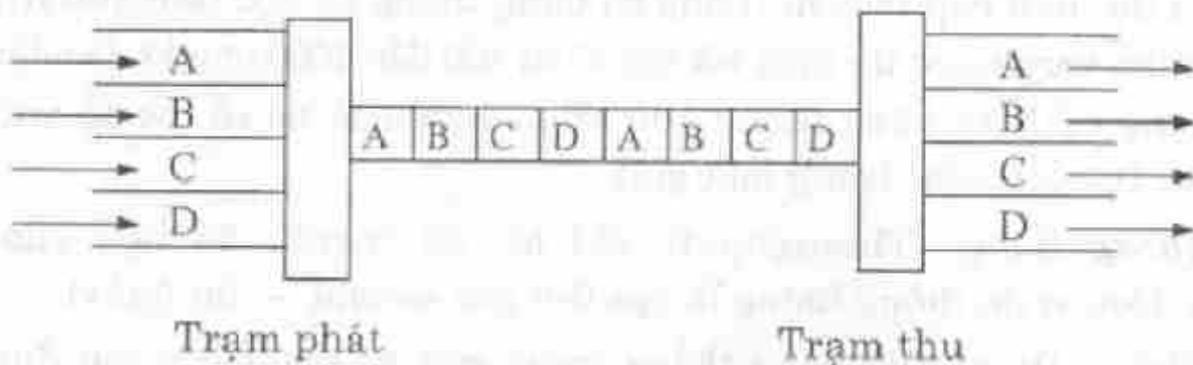
truyền trên cáp. Có thể lấy ví dụ về nhiễu điện từ: đó là khi có tia chớp tín hiệu của đài phát thanh AM sẽ bị ảnh hưởng, hoặc khi xảy ra các cơn bão từ trên bề mặt mặt trời thì nhiễu phương tiện vô tuyến trên trái đất cũng bị ảnh hưởng.

Nhiều xuyên âm: là một dạng đặc biệt của nhiễu điện từ, khi mà nguồn nhiễu xuất hiện do các dây cáp chạy song song gây ảnh hưởng lẫn nhau.

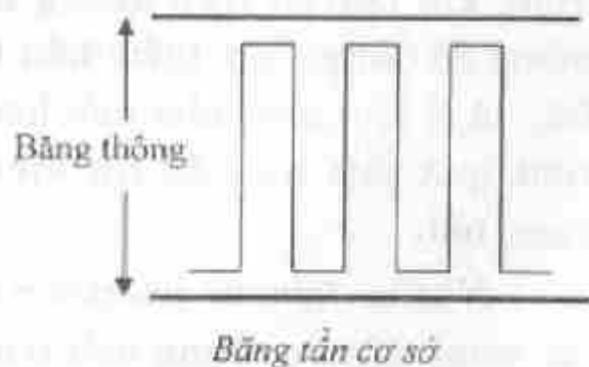
1.2. Chế độ truyền băng tần cơ sở và chế độ băng tần rộng

Có 2 chế độ sử dụng dải thông của cáp: chế độ *băng tần cơ sở* (Based band) và chế độ *băng tần rộng* (Broad band).

Chế độ băng tần cơ sở: dành toàn bộ dải thông cho một kênh truyền thông, tín hiệu truyền có thể là tín hiệu số (digital) hay tín hiệu tương tự (analog). Đây là chế độ truyền của đa số các mạng LAN. Trong chế độ này, kĩ thuật *Đồn kênh phân theo thời gian* (TDM – Time Division Multiplexing) được sử dụng để phục vụ cùng lúc nhiều cuộc truyền, và chỉ phục vụ cho các tín hiệu đã số hóa. Kĩ thuật TDM chia thời gian thành nhiều đoạn nhỏ – lát cắt thời gian – và phân bổ xen kẽ các cuộc truyền vào dãy lát cắt liên tiếp.



Phương pháp phân các lát cắt thời gian cho các kênh truyền cũng là vấn đề quan trọng. Nếu phân một cách cố định thì khi kênh đó tạm ngừng, các lát thời gian dành cho nó sẽ bị bỏ trống. Đã có nhiều chiến lược phân bổ lát cắt thời gian cho các kênh truyền, ví dụ như phân theo thống kê TDM (statistical Time Division Multiplexing – Stat TDM), Đồng bộ TDM (Synchronized Time Division Multiplexing)

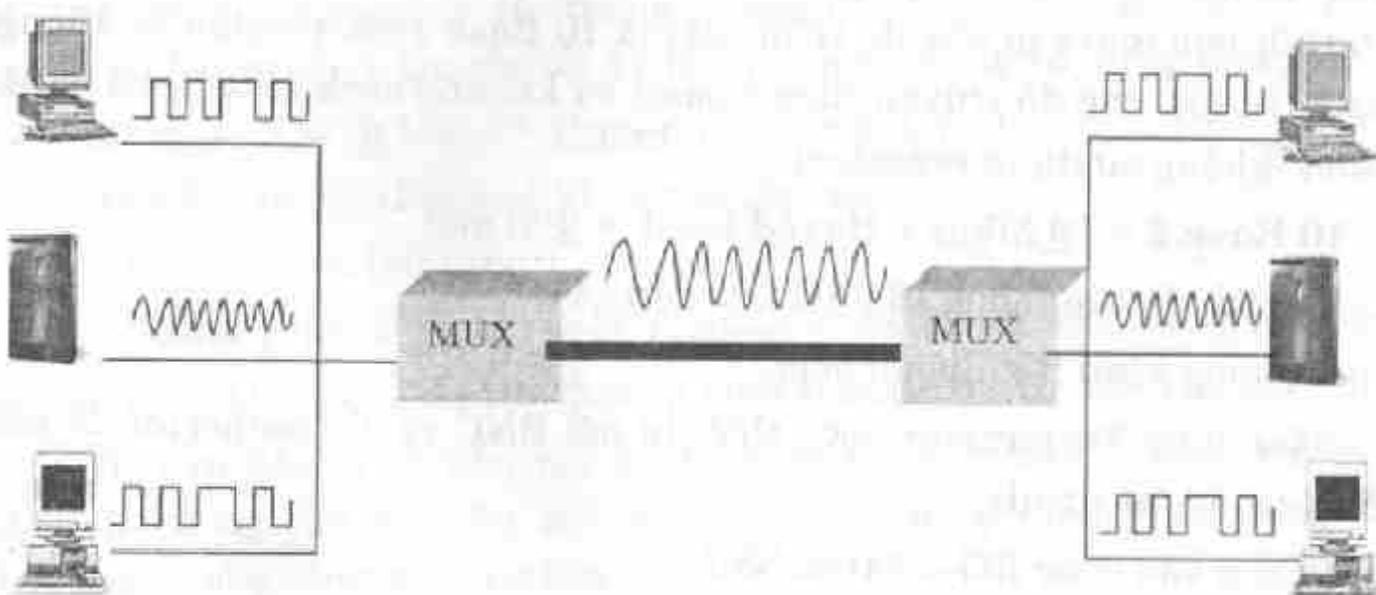


Trái với Based band, chế độ

băng tần rộng (broad band) cho phép nhiều kênh truyền thông dùng chung dải thông của đường truyền bằng cách chia nhỏ dải thông thành nhiều khoảng tần số. Đường cáp chạy từ ăng-ten vào tivi là một đường truyền băng tần rộng, nơi mà nhiều tín hiệu tivi có thể dùng chung dải thông của cáp.

Kĩ thuật thường dùng trên các kênh broad band để truyền tín hiệu tương tự có tên là *Đồn kênh phân theo tần số* (FDM – Frequency – Division Multiplexing). Ở đầu phát một thiết bị thực hiện việc *đồn kênh* (multiplexing), tức là tổ hợp nhiều kênh dữ liệu lại để truyền trên cùng một đường truyền.

Ở trạm thu, thiết bị này lại làm công việc ngược lại, *phân kênh* (demultiplexing), tức là tách tín hiệu nhận được thành các kênh riêng biệt ban đầu. Thiết bị đồn kênh và phân kênh đó gọi là *bộ đồn kênh* (multiplexer).



1.3. Cáp đồng trục (coaxial cable)

1.3.1. Cấu tạo

Cáp đồng trục là loại cáp đầu tiên được sử dụng cho các mạng LAN. Các thành phần của cáp đồng trục gồm:

Lõi truyền tín hiệu, thường là một dây đồng đặc hay bó nhiều sợi nhỏ bện lại.

Lưới kim loại chống nhiễu điện từ* bọc phía ngoài lõi

* Còn gọi là nhiễu EMI.

Giữa lõi và lưới kim loại ngăn cách bởi một lớp chất cách điện, thường là nhựa tổng hợp.

Ngoài cùng là lớp vỏ bảo vệ chống va đập, cọ xát. Vỏ thường làm bằng nhựa tổng hợp hay cao su.



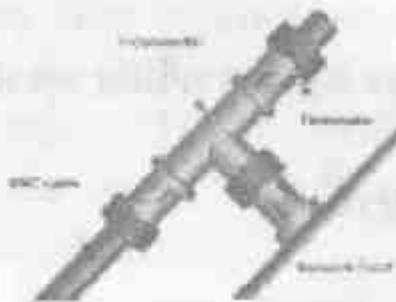
1.3.2. Cáp đồng trục mảnh (thin net)

Cáp đồng trục mảnh – còn gọi là cáp gậy – là loại cáp mạng rất thông dụng trong các mạng LAN thời kì đầu. Cáp gậy dễ lắp đặt, không đòi hỏi những dụng cụ chuyên dụng, khỏe và chịu nhiều tốt nhờ lớp lưới kim loại, tuy vậy thông lượng không cao. Tên gọi chính thức của loại cáp này do IEEE đặt là 10 Base 2 với ý nghĩa là: thông lượng 10 Mbps, chế độ truyền Based band và khoảng cách truyền tối đa là 200 mét (không sử dụng repeater).

$$10 \text{ Base } 2 = 10 \text{ Mbps} + \text{Based band} + 200 \text{ mét}$$

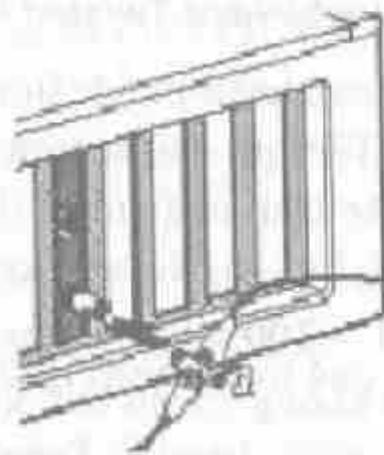
Sau đây là các thông số khác của cáp gậy:

- Đường kính tiết diện 0,5cm.
- Sử dụng Terminator 50Ω, thiết bị nối BNC và T-connector để nối với NIC trong máy tính.
- Cắm vào cổng RG-58 trên NIC.
- Cáp gậy còn được gọi là cáp RG-58 để phân biệt với một số loại cáp đồng trục khác như:
 - Cáp RG-59 dùng cho truyền hình cáp, sử dụng Terminator 75Ω.
 - Cáp RG-62 dùng cho ARC net, sử dụng Terminator 93Ω.



T-connector

Sử dụng T-connector để nối cáp gây vào cổng RG58 của NIC trong máy



1.3.3. Cáp đồng trục dày (thick net)

Cáp đồng trục dày, còn gọi là cáp béo, là một loại cáp có lớp chống nhiễu tốt, cho phép truyền tín hiệu đi xa, tuy nhiên nặng nề khó uốn, khó lắp đặt và giá thành cao. Tên gọi chính thức của loại cáp này do IEEE đặt là 10 Base 5 với ý nghĩa là: thông lượng 10 Mbps, chế độ truyền Based band và khoảng cách truyền tối đa là 500 mét (không sử dụng repeater).

10 Base 5 = 10 Mbps + Based band + 500 mét

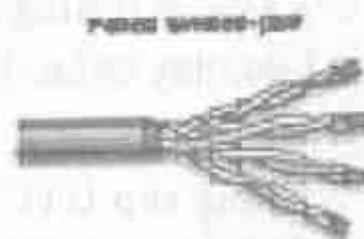
Sau đây là các thông số khác của cáp béo

- Đường kính tiết diện 1,3cm
- Sử dụng một thiết bị tên là Tranceiver để nối với NIC trong máy tính.
- Nối vào cổng AUI (Attachment Unit Interface) trên NIC của máy tính.

Do cáp béo có độ bền vật lí cao, chống chịu nhiễu tốt và truyền tín hiệu đi tương đối xa nên đôi khi nó được dùng làm cáp xương sống (backbone) cho những mạng lớn.

1.4. Cáp xoắn (Twisted Pair Cable)

Hiện nay, cáp xoắn đã trở nên thông dụng và thống lĩnh thị trường mạng LAN thay cho cáp đồng trục. Ưu thế của cáp xoắn so với cáp đồng trục là dễ lắp đặt và bảo trì, hơn nữa giá thành lại thấp.



1.4.1. Cấu tạo

Cáp xoắn gồm các đôi dây bện vào nhau một cách đều đặn (để chống nhiễu), bên ngoài có thể có một lớp màng kim loại chống nhiễu. Ngoài cùng là lớp vỏ bảo vệ làm bằng nhựa.

1.4.2. Cáp UTP (Unshielded Twisted Pair – Cáp xoắn không có vỏ bảo vệ)

Đây là loại cáp xoắn phổ biến nhất hiện nay, có thể bắt gặp ở hầu hết các mạng LAN. Tên gọi chính thức của loại cáp này do IEEE đặt là 100 Base T, để chỉ các tính chất như: thông lượng tối đa là 100 Mbps, chế độ truyền Based band và có cấu trúc xoắn các đôi dây

100 Base T = 100 Mbps + Based band + Twisted Pair

Do cấu tạo không có lớp lưới kim loại chống nhiễu như cáp đồng trục nên cáp UTP phải có một cơ chế chống nhiễu khác. Đó là các cặp dây được xoắn vào nhau một cách đều đặn để giảm thiểu nguồn nhiễu từ các đôi dây kế cận và từ môi trường bên ngoài. Dù vậy mức độ chịu nhiễu của cáp UTP vẫn không thể so sánh với cáp đồng trục và khoảng cách truyền tín hiệu tối đa của cáp UTP chỉ là 100 mét.

Phân loại

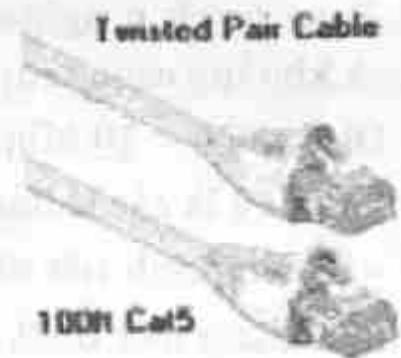
Tổ chức EIA /TIA đã định nghĩa các loại cáp UTP như sau:

- Loại 1 (Category 1 – CAT1): là loại cáp điện thoại truyền thống, gồm 1 đôi dây
- Loại 2 (Category 2 – CAT2): tốc độ truyền dữ liệu tối đa 4 Mbps, gồm 2 đôi dây xoắn nhau.
- Loại 3 (Category 3 – CAT3): tốc độ truyền dữ liệu tối đa 10 Mbps, gồm 4 đôi dây xoắn nhau, cứ mỗi foot (30,48cm) có 3 mắt xoắn.
- Loại 4 (Category 4 – CAT4): tốc độ truyền dữ liệu tối đa 16 Mbps, gồm 4 đôi dây xoắn.
- Loại 5 (Category 5 – CAT5): tốc độ truyền dữ liệu tối đa 100 Mbps, gồm 4 đôi dây xoắn. Đây là loại cáp UTP chủ yếu hiện nay trong các mạng LAN.

Trong cáp UTP CAT5, 8 sợi dây được nhuộm màu riêng để phân biệt nhau khi đấu nối. Các màu được sử dụng cho 4 đôi dây là: Da cam – trắng, Nâu gạch – trắng, Xanh lá cây – trắng, Xanh nước biển – trắng.

Các thiết bị đi kèm:

- Cáp UTP được lắp vào đầu nối RJ-45 connector và cắm vào cổng UTP (còn gọi là cổng RJ-45) của NIC trong máy tính. Chú ý: đầu nối



RJ-45 có cấu tạo và hình dạng rất giống đầu nối cáp điện thoại (có tên là RJ-11) mà ta vẫn thấy tại các máy điện thoại để bàn. Điểm khác nhau duy nhất là RJ-45 to hơn do phải chứa 8 sợi dây, còn RJ-11 chỉ có 4 sợi và thường để trống 2 chỗ.

- Ổ gắn tường (Wall plate), giá phân phối (Patch panel)

1.4.3. Cáp STP (Shielded Twisted Pair – Cáp xoắn có vỏ bảo vệ)

Cáp STP có cấu tạo tương tự như cáp UTP, chỉ thêm lớp vỏ bọc chống nhiễu bằng giấy có phủ một lớp kim loại và được nối đất. Cáp STP được dùng trong mạng Token-Ring của IBM để chống nhiễu EMI và trong mạng Apple Talk của Apple.

Các thông số khác của cáp STP:

- Giá thành cáp STP dĩ nhiên cao hơn cáp UTP nhưng vẫn rẻ hơn cáp đồng trục dày (10 Base 5) và cáp quang.
- Kích thước to hơn cáp UTP, do đó cũng khó lắp đặt hơn.
- Thông lượng trên lí thuyết có thể đạt tới 500 Mbps, nhưng trên thực tế không vượt quá 155 Mbps trên độ dài cáp tối đa 100 mét.

Nói chung cáp STP xuất hiện muộn và không thông dụng như cáp UTP.

1.5. Cáp quang (Fiber Optic Cable)

Cáp quang là loại cáp tiên tiến nhất hiện nay, khắc phục được hầu hết những nhược điểm của các loại cáp khác. Cáp quang chỉ có vấn đề về giá thành và kĩ năng lắp đặt, tuy nhiên nhờ được ứng dụng và sản xuất đại trà nên công nghệ cáp quang không ngừng được cải tiến với giá thành hạ nhanh chóng. Hiện nay cáp quang đang nhanh chóng trở nên phổ biến và chiếm lĩnh thị trường.

1.5.1. Cấu tạo

Trong cáp quang, tín hiệu được truyền đi dưới dạng ánh sáng. Lõi sợi quang truyền tín hiệu được làm bằng thủy tinh hữu cơ hay nhựa tổng hợp có độ trong suốt rất cao, bề mặt được phủ một lớp lót phản chiếu ánh sáng để tín hiệu không lọt ra ngoài. Bên ngoài có một lớp vỏ nhựa bảo vệ. Giữa lớp lót phản chiếu ánh sáng và vỏ bọc có thể là một lớp nhựa tổng hợp hay

cao cấp hơn là một lưới kim loại để tăng độ bền cho cáp. Trong thực tế, nhờ có kích thước nhỏ, cáp quang thường được bó nhiều sợi với nhau.

Tín hiệu truyền trên cáp quang được tạo bởi một nguồn sáng laser hay nguồn sáng LED. Nguồn LED (Light Emitting Diodes – diot phát quang) rẻ tiền hơn nhưng chất lượng ánh sáng không cao, tia sáng tạp và độ dài cáp không thể vượt quá vài kilômet. Nguồn sáng laser ILD (Injection Lasser Diode) cho tia sáng đơn sắc, song song thường được dùng trong các mạng LAN với độ dài cáp có thể tới hàng trăm kilômet.

1.5.2. Một số kiểu cáp quang thường dùng

- Lõi 8.3 micron, lớp lót 125 micron, chế độ đơn (1 micron = $1\mu\text{m} = 10^{-6}\text{met}$).
- Lõi 62.5 micron, lớp lót 125 micron, đa chế độ.
- Lõi 50 micron, lớp lót 125 micron, đa chế độ.
- Lõi 100 micron, lớp lót 140 micron, đa chế độ.



1.5.3. Các đặc tính

- Thông lượng: trong phòng thí nghiệm, cáp quang có thể truyền tin với tốc độ rất cao: đến 200.000 Mbps. Trên thực tế, cáp quang có thể cho thông lượng cỡ Gbps trong các mạng LAN cỡ vài kilômet.
- Chống chịu nhiễu và suy yếu: do tín hiệu được truyền đi dưới dạng ánh sáng nên mọi loại nhiễu điện từ không ảnh hưởng gì đến tín hiệu được truyền trên cáp quang. Nhờ đặc tính trong suốt cao của lõi cáp nên tín hiệu hầu như không bị yếu đi trên đường truyền, đảm bảo cho cáp một khoảng cách an toàn rất xa.
- Chống thu trộm: do không gây nên một từ trường xung quanh như những loại cáp dùng tín hiệu điện nên cáp quang không thể bị thu trộm bởi các thiết bị phát hiện bức xạ điện từ.
- Lắp đặt: cáp quang tương đối khó lắp đặt so với các loại cáp khác vì khi nối hai đoạn cáp quang, cần phải đặt hai đầu tiết diện cáp – vốn chỉ nhỏ cỡ μm – thật thẳng hàng và phải đảm bảo cho chúng thật phẳng. Cáp có một bán kính cong tối thiểu mà nếu bị uốn quá giới hạn này chúng sẽ bị

gãy. Tuy nhiên hiện nay nhờ các công cụ cải tiến, việc này không quá khó khăn nữa.

Giá thành: cáp quang có giá thành và chi phí lắp đặt cao so với các loại cáp khác. Đồng thời các bo mạch, các thiết bị mạng có cổng nối với cáp quang cũng có giá cao hơn so với các thiết bị cùng chức năng chỉ làm việc với cáp xoắn và cáp đồng trục.

1.6. So sánh các loại cáp

Cáp	Cáp đồng trục mảnh (10 Base 2)	Cáp đồng trục dày (10 Base 5)	Cáp xoắn không bọc (100 Base T)	Cáp quang
Tiêu chí				
Chi phí	Cao hơn cáp xoắn nhưng vẫn thấp	Cao hơn cáp đồng trục mảnh	Thấp nhất	Cao nhất
Độ dài tối đa cho phép	185 m	500 m	100 m	Vài km
Tốc độ truyền dữ liệu	10 Mbps	10 Mbps	100 Mbps	Trên 100 Mbps
Tính chất vật lí	Khá mềm dẻo, dễ lắp đặt	To nặng, khó uốn, khó lắp đặt	Nhỏ, dễ uốn, rất dễ lắp đặt	Kĩ thuật lắp đặt đòi hỏi độ chính xác cao
Khả năng kháng nhiễu	Tốt	Rất tốt	Kém	Không bị tác động bởi nhiễu
Ứng dụng thực tế	Hiện nay rất ít gặp trong mạng LAN	Rất ít gặp trong mạng LAN	Phổ biến trong các mạng LAN	Đang phát triển, càng ngày càng phổ biến.

1.7. Truyền thông trên mạng vô tuyến

Tại sao đã có cáp mạng (mạng hữu tuyến) rồi mà chúng ta còn phải xét đến môi trường truyền vô tuyến. Đó là vì có những trường hợp đặc biệt mà mạng hữu tuyến không thể sử dụng được, chẳng hạn như:

– Phải kết nối hai máy tính cách nhau bởi một xa lộ. Rõ ràng chúng ta không thể lắp cáp truyền ở bên trên cũng như ở phía dưới xa lộ đó.

– Kết nối các máy trạm di động trang bị cho những nhân viên do đặc thù công việc thường xuyên phải đi lại.

– Trong một số trường hợp khác, tuy việc lắp đặt cáp là có thể nhưng phương thức truyền vô tuyến tỏ ra ưu việt hơn hẳn. Đó là khi chúng ta phải nối mạng:

– Để cung cấp đường truyền dự phòng cho một mạng hữu tuyến để mạng không gián đoạn khi xảy ra sự cố với cáp (động đất, chiến tranh ...)

– Cung cấp kết nối tạm thời, trong thời gian ngắn, cho một vài trạm nào đó với mạng cáp có sẵn. Trường hợp này nếu lắp đặt tuyến cáp cố định cho những trạm đó thì rất lãng phí vì chỉ sau một thời gian ngắn chúng sẽ chấm dứt hoạt động.

Những khu vực khó lắp đặt dây cáp như: những tòa nhà biệt lập có nhiều chướng ngại, những địa điểm thường xuyên bị xê dịch nội thất (chẳng hạn các gian triển lãm), những di tích lịch sử lâu đời không cho phép sửa chữa nhiều.

1.7.1. Các loại mạng vô tuyến

Mạng vô tuyến được chia thành ba loại dựa trên công nghệ truyền tín hiệu của chúng.

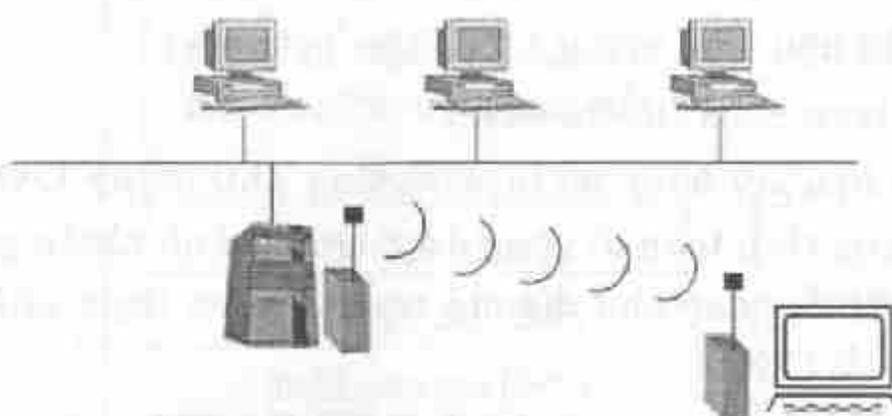
- Mạng cục bộ vô tuyến (wireless LAN).
- Mạng cục bộ vô tuyến mở rộng (extended wireless LAN).
- Mạng tính toán di động (mobile computing).

Điểm khác nhau chính giữa ba loại là ở thiết bị truyền tín hiệu. Mạng cục bộ vô tuyến và mạng cục bộ mở rộng dùng máy thu và máy phát của một công ti sản xuất thiết bị mạng nào đó, còn mạng di động vô tuyến dùng các hãng truyền thông công cộng như AT&T, MCI và những công ti điện thoại để cung cấp các dịch vụ truyền thông công cộng để truyền và nhận tín hiệu.

1.7.2. Mạng cục bộ vô tuyến (wireless LAN)

Loại mạng này có cấu tạo và hoạt động tương tự như mạng LAN hữu tuyến thông thường, ngoại trừ việc nó sử dụng môi trường truyền vô tuyến. Hiện nay mạng cục bộ vô tuyến có thể bao gồm một LAN hữu tuyến kết nối với các máy trạm vô tuyến thông qua các *điểm truy nhập* (access

point). Đó là các thiết bị thu phát tín hiệu vô tuyến rồi chuyển tín hiệu điện lên đường cáp mạng.



Mạng cục bộ vô tuyến sử dụng các công nghệ truyền tín hiệu sau:

- Tia hồng ngoại (infrared).
- Tia laser.
- Sóng vô tuyến dải hẹp, còn gọi là đơn tần (narrow band).
- Sóng vô tuyến phổ rộng.

1.7.3. Mạng cục bộ vô tuyến mở rộng (extended wireless LAN)

Đây thực chất là các mạng LAN kết nối với nhau bằng đường truyền vô tuyến. Nhiệm vụ kết nối được giao cho một thiết bị gọi là Cầu nối vô tuyến (wireless bridge). Chẳng hạn cầu nối AIRLAN/ BRIDGE PLUS, sử dụng công nghệ truyền sóng vô tuyến phổ rộng để tạo ra một trục sóng vô tuyến có thể dài đến 5km nối liền các vị trí của các mạng LAN thành phần. Hơn thế nữa, loại cầu nối vô tuyến tầm xa (long range wireless bridge) còn có thể phủ sóng vô tuyến phổ rộng trong phạm vi lên đến 40km để truyền cả âm thanh, hình ảnh và dữ liệu.

1.7.4. Mạng tính toán di động (mobile computing)

Hình thức nối mạng này thường dành cho những nhân viên thường xuyên phải di chuyển (chẳng hạn các phóng viên). Họ sẽ nối mạng để truyền dữ liệu từ các thiết bị xách tay như máy tính xách tay, PDA (Personal Digital Assistant). Các thiết bị này phải gắn các NIC vô tuyến với những anten nhỏ để thu và phát sóng vô tuyến lên không trung, liên lạc với tháp vô tuyến gần nhất hoặc vệ tinh. Tốc độ truyền của mô hình này còn chậm, khoảng 30Kbps.

Mạng tính toán di động yêu cầu phải có những dịch vụ truyền thông công cộng để truyền nhận dữ liệu theo một trong các phương thức sau:

- Truyền dữ liệu gói bằng vô tuyến (packet-radio communication)
- Truyền dữ liệu trên mạng ô (cellular network)
- Sử dụng trạm viba (microwave)

Truyền dữ liệu gói bằng vô tuyến: giống như mạng LAN hữu tuyến, dữ liệu trong mạng tính toán di động được chia thành nhiều gói và được bổ sung các thông tin header như địa chỉ trạm thu và trạm phát, chỉ số của gói và các mã dò lỗi CRC.

Truyền dữ liệu trên mạng ô: phương thức này cũng chia dữ liệu thành các gói, sau đó dùng các công nghệ truyền như điện thoại ô (cellular telephone) chuyển dữ liệu thành tín hiệu tương tự (analog) rồi đưa lên mạng truyền thông (analog voice network). Giống như các hình thức mạng vô tuyến khác, cần phải có một kết nối với mạng hữu tuyến có sẵn. Những kết nối như vậy có thể liệt kê như EIU của Nortel.

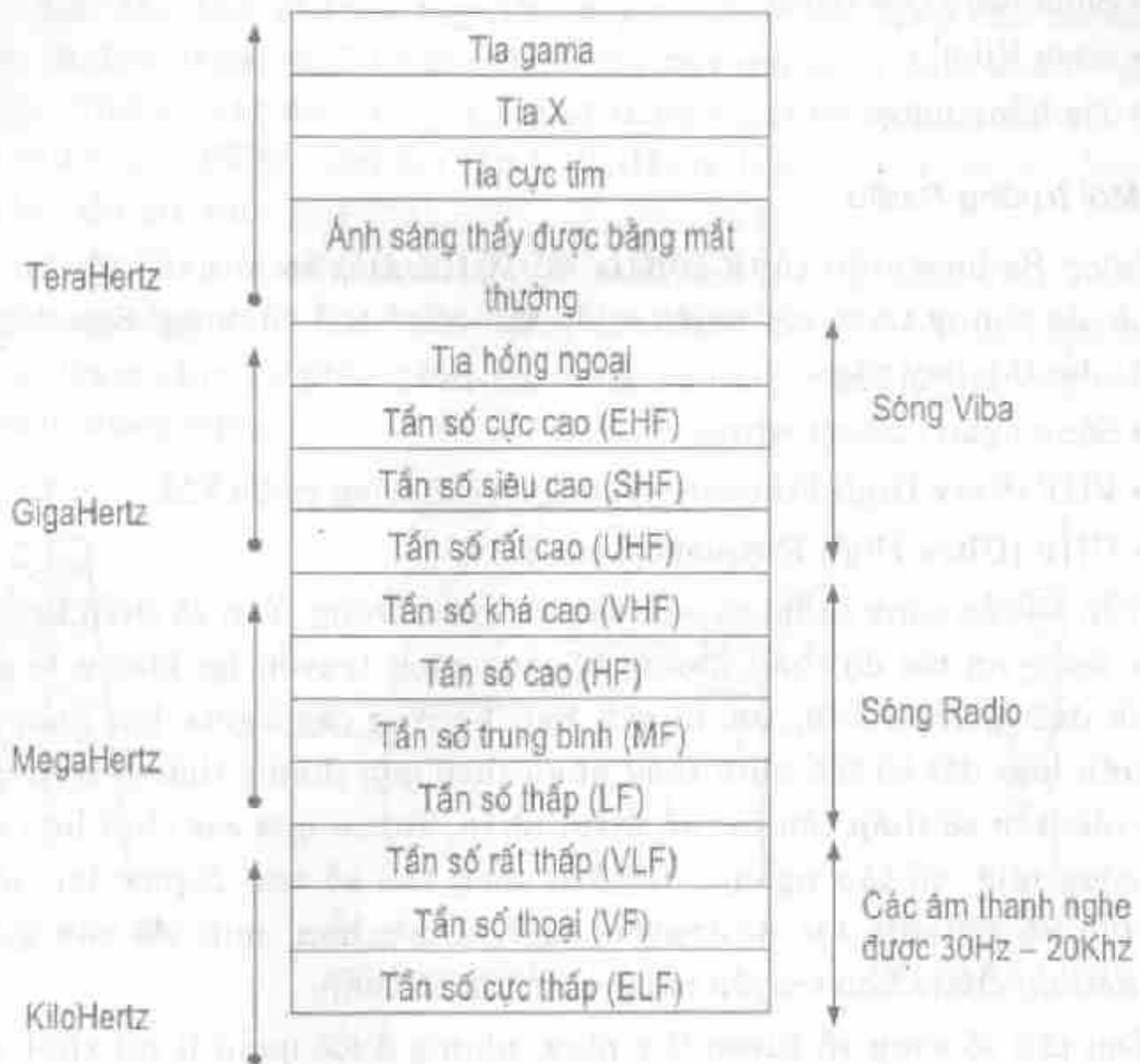
Sử dụng trạm viba: hệ thống viba là phương thức thuận tiện để liên kết các máy trạm, các mạng LAN đặt ở:

- Trong các tòa nhà của một quần thể kiến trúc (trường đại học, công viên phần mềm ...).
- Các vị trí ngăn cách nhau bởi những khoảng trống rộng và bằng phẳng như cánh đồng, sa mạc, sông hồ.

Phương thức truyền này đòi hỏi trạm thu và trạm phát phải có máy thu phát radio sử dụng hai ăngten định hướng về phía nhau. Những ăngten này phải được đặt càng cao càng tốt (nóc nhà cao tầng, đỉnh tháp phát sóng) để mở rộng tầm thu phát và tránh những vật cản như các nhà cao tầng, cây cối và đồi núi.

1.7.5. Môi trường truyền vô tuyến

Sóng vô tuyến có thể có nhiều tần số khác nhau, sau đây là bảng các giá trị tần số của sóng vô tuyến mà ta có thể sử dụng để truyền tín hiệu.



Trong bảng trên, các sóng tần số radio, còn gọi là sóng radio, thường được dùng để phát tín hiệu trong mạng LAN thông qua cáp xoắn, cáp đồng trục hoặc sóng vô tuyến.

Các kĩ thuật truyền viba dùng cho các cuộc truyền điểm – điểm (*point to point*). Sóng viba có thể dùng để liên lạc giữa trạm mặt đất với vệ tinh hay phát ngang (*light of sight*) giữa các trạm mặt đất với nhau. Sóng viba công suất thấp được dùng để phủ tín hiệu theo kiểu *broadcast* giữa các trạm trong mạng ô (*cellular network*).

Tia hồng ngoại thường được dùng cho việc truyền thông trên mạng với khoảng cách tương đối ngắn theo kiểu điểm – điểm (*point to point*) hay quảng bá (*broadcast*). Tia hồng ngoại và những ánh sáng tần số cao hơn có thể được truyền bằng cáp quang. Hiện nay môi trường vô tuyến có những dạng sau đây:

- Sóng Radio và Laser
- Sóng Viba
- Tia hồng ngoại

1.7.6. Môi trường Radio

Sóng Radio có tần số từ 10KHz tới 1GHz. Đây là một dải tần số rất rộng, do đó chúng ta có rất nhiều miền tần số có thể sử dụng. Sau đây là một vài dải tần hay gặp:

- Sóng ngắn (Short wave)
- VHF (Very High Frequency) sóng tivi và sóng radio FM
- UHF (Ultra High Frequency) sóng tivi

Tần số của sóng radio có một vai trò quan trọng. Tần số thấp tuy chỉ truyền được với tốc độ thấp nhưng khoảng cách truyền lại không bị giới hạn bởi đường chân trời, tức là giới hạn khoảng cách giữa hai điểm xa nhất trên mặt đất có thể nhìn thấy nhau theo một đường thẳng. Hơn nữa sóng radio tần số thấp còn có thể thâm nhập, xuyên qua các chất liệu đặc như tường nhà, vỏ tàu ngầm... tốt hơn sóng tần số cao. Ngược lại, sóng radio tần số cao cho tốc độ truyền dữ liệu cao hơn, mức độ suy giảm (attenuation) chậm hơn truyền bằng sóng tần số thấp.

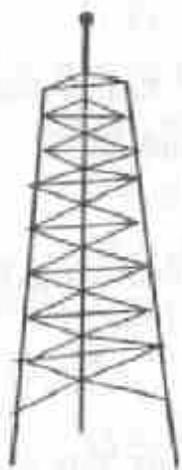
Dải tần số sóng vô tuyến tuy rộng, nhưng được quản lý rất chặt chẽ chứ không thể sử dụng tùy thích. Chúng ta hãy xét ví dụ nước Mỹ, Ủy ban truyền thông liên bang FCC (Federal Communication Commission) phụ trách quản lý việc sử dụng các dải tần số vô tuyến. Phần lớn việc sử dụng các tần số vô tuyến đều phải có giấy phép. Mỗi tổ chức có giấy phép được độc quyền sử dụng một miền tần số cụ thể nào trong một phạm vi địa lý nhất định. Việc quản lý và phân bổ đó đảm bảo cho chủ sở hữu giấy phép được dùng một kênh truyền radio rõ và không bị những nguồn phát khác gây nhiễu.

Tuy nhiên còn một phần nhỏ trong dải tần số vô tuyến không được cấp giấy phép, có nghĩa là mọi người được tự do dùng những tần số trong dải tần đó. Ví dụ như FCC quy định ba dải tần không cấp phép là:

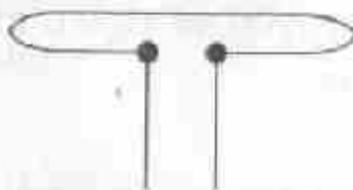
- 902 – 928MHz
- 2,4 MHz
- 5,72 – 5,85GHz

Dải tần thứ nhất tương đối rộng và được sử dụng cho nhiều mục đích, từ điện thoại di động cho đến máy bay mô hình điều khiển bằng vô tuyến. Nhiều hãng điện tử đang phát triển các thiết bị hoạt động trên dải tần thứ hai, 2,4GHz. Còn dải tần 5,72GHz ít được dùng nhất do công nghệ chế tạo chi phí cao.

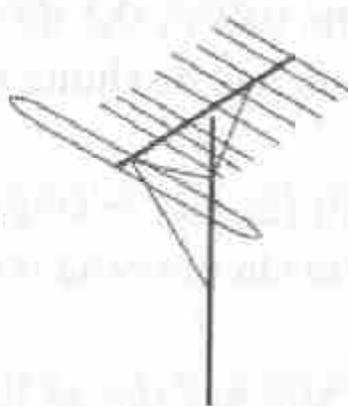
Một phiên truyền radio có thể theo mọi hướng hoặc định hướng để tập trung công suất vào một hướng thu nhất định. Để thực hiện truyền radio, trạm thu và phát phải sử dụng ăngten. Sau đây là một số kiểu ăngten thông dụng.



Ăngten tháp



Ăngten lưỡng cực bán sóng



Yagi



Ăngten dây chiều dài ngẫu nhiên

Tháp phủ sóng Dùng để phủ sóng trên phạm vi rộng theo mọi hướng, có thể dựng trên nóc nhà cao tầng hoặc trên đồi, núi.

Ăngten lưỡng cực: có miền tần số khá rộng và có thể định hướng thu

Ăngten dây chiều dài ngẫu nhiên dùng để phát hoặc thu. Chiều dài ăngten không được chọn gắn với một tần số nào cả.

Yagi là một dạng của Ăngten chùm (beam antenna), dùng nhiều thành phần để chỉnh ăngten theo một miền tần số cụ thể và theo định hướng. Ăngten chùm dùng để tạo một chùm tập trung hướng đến một điểm thu cụ thể.

Hệ thống truyền thông radio có thể sử dụng một trong ba dạng sau

- Sóng radio tần số đơn, công suất thấp.
- Sóng radio tần số đơn, công suất cao.
- Sóng radio quang phổ trải.

1.7.7. Tần số đơn, công suất thấp

Kĩ thuật truyền có công suất thấp được lựa chọn để hạn chế hiệu ứng gây nhiễu giữa các hệ thu phát radio đặt cạnh nhau. Tâm phát sóng chỉ ngắn cỡ vài chục mét. Tương tự như mạng tế bào (cellular network), kĩ thuật này cũng chia không gian địa lí thành các vùng độc lập, không gây nhiễu lẫn nhau mặc dù có chung tần số phủ sóng.

Sóng radio tần số thấp có thể xuyên qua các bức tường, nhưng tốc độ truyền quá chậm nên có thể khó đáp ứng yêu cầu cao của các mạng LAN. Sau đây là các đặc tính của môi trường truyền tần số đơn, công suất thấp.

Miền tần số

Mọi tần số radio đều có thể được dùng, nhưng các tần số cao ở mức GHz thường được chọn hơn do chúng cho tốc độ truyền dữ liệu cao hơn.

Chi phí

Thấp hơn so với các môi trường truyền vô tuyến khác. Nói chung tốc độ truyền càng cao thì chi phí càng tăng.

Cài đặt

Tương đối dễ. Một vài tần số nằm trong cấp phép thì phải xin giấy phép trước khi sử dụng, nhưng có những hãng truyền thông còn lo hộ khách thủ tục xin cấp phép của FCC. Một số hệ thống khác sử dụng những tần số tự do không cần giấy phép nhưng phải có khả năng tự điều chỉnh khi bị nhiễu từ các thiết bị truyền thông hay từ vùng lân cận sử dụng cùng tần số.

Tốc độ truyền

Các hệ thống sử dụng sóng radio tần số đơn, công suất thấp hiện có tốc độ khoảng 10 Mbps

Khoảng cách tối đa

Như đã biết, sóng radio công suất thấp có khoảng cách truyền nhỏ, hiện tượng suy giảm ở mức cao nhưng có thể lợi dụng chính đặc điểm này để thiết kế các mạng tế bào. Phạm vi liên lạc được chia thành nhiều khu độc lập, tín hiệu trong mỗi khu không vượt được ra ngoài do đó không gây nhiễu cho các khu lân cận.

Tính chịu nhiễu EMI

Ở mức thấp, nhất là khi sử dụng những tần số tự do không cần giấy phép. Các mạng LAN sử dụng sóng radio đều dễ bị thu trộm bằng thiết bị

điện tử mặc dù thiết bị thu trộm cũng phải đặt trong phạm vi phủ sóng rất hẹp của sóng.

1.7.8. Tần số đơn, công suất cao

Sóng radio công suất cao có tốc độ truyền tương tự như radio công suất thấp nhưng có phạm vi phủ sóng rộng lớn hơn. Phạm vi truyền chỉ giới hạn bởi tầm phát ngang, còn gọi là đường chân trời (line of sight), thậm chí có thể mở rộng hơn bằng cách đưa tín hiệu lên bầu khí quyển.

Miền tần số

Giống như radio công suất thấp, ta có thể dùng mọi tần số trong dải tần của sóng radio và các tần số cỡ GHz hay được sử dụng hơn vì mang lại tốc độ truyền dữ liệu cao.

Chi phí

Các thiết bị truyền tín hiệu công suất cao đắt hơn nhiều so với loại truyền công suất thấp.

Cài đặt

Việc cài đặt là dễ dàng, tuy nhiên phải có giấy phép sử dụng thiết bị radio công suất cao. Việc bảo trì cũng phải tiến hành thường xuyên vì thiết bị hoạt động không tốt không chỉ gây gián đoạn phiên truyền mà có thể ảnh hưởng nhiều cho các vùng lân cận.

Tốc độ truyền

Có thể đáp ứng các yêu cầu của LAN, khoảng 100 Mbps.

Khoảng cách tối đa

Sóng radio công suất cao có độ suy giảm khá chậm, hơn nữa ta có thể dùng các bộ truyền lặp để mở rộng tầm phát tín hiệu

Tính chịu nhiễu EMI

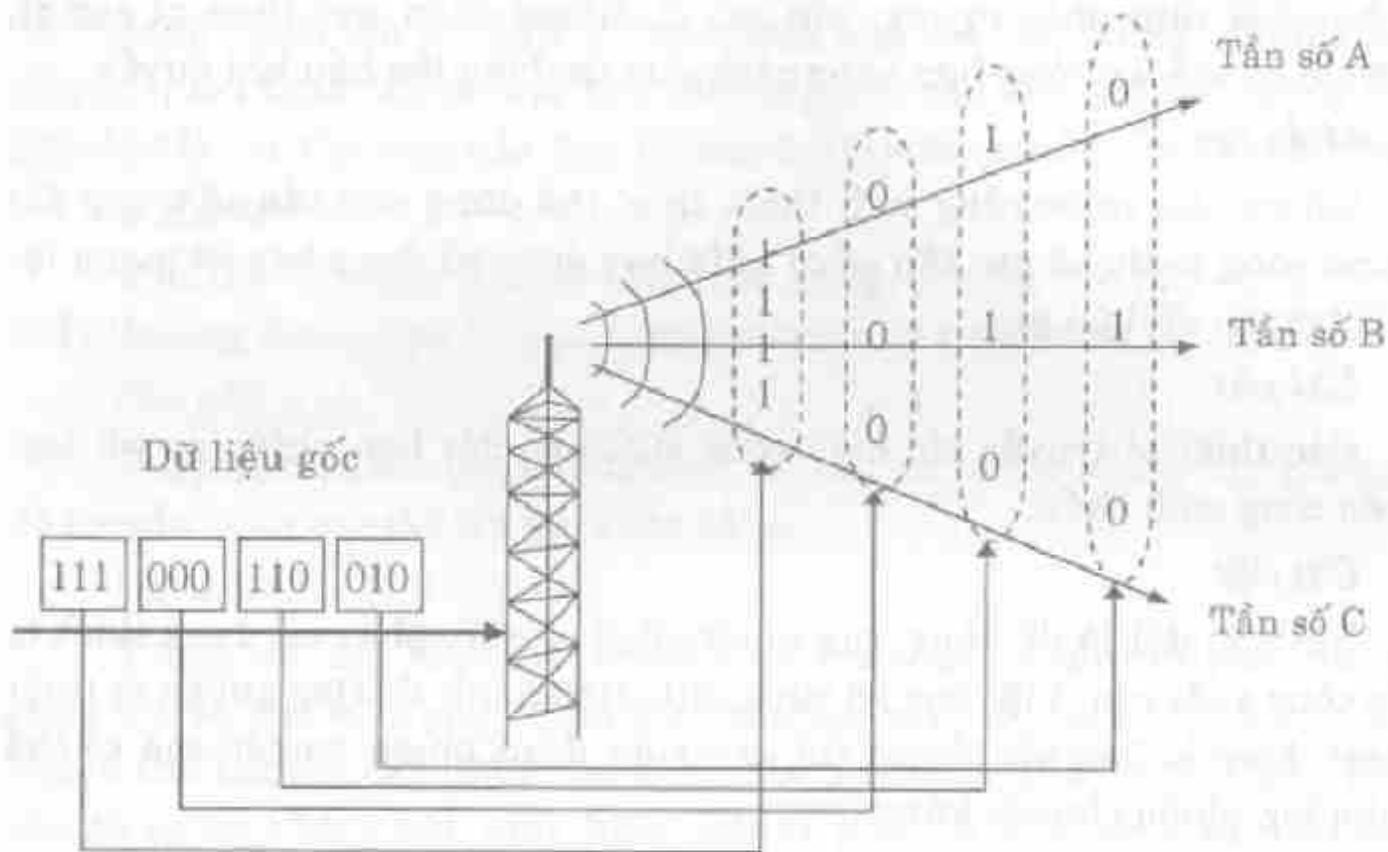
Giống như sóng radio công suất thấp, sóng công suất cao có khả năng chống nhiễu EMI thấp đồng thời rất dễ bị thu trộm do vùng phủ sóng rộng

1.7.9. Radio trải phổ (spread spectrum)

Công nghệ trải phổ ban đầu được áp dụng trong quân sự để tăng độ tin cậy và chống thu trộm. Nó sử dụng nhiều tần số để truyền dữ liệu chứ không chỉ sử dụng một tần số như các kỹ thuật tần số đơn đã xét. Hai kỹ thuật thường dùng là điều biến chuỗi trực tiếp và lập chạng tần số.

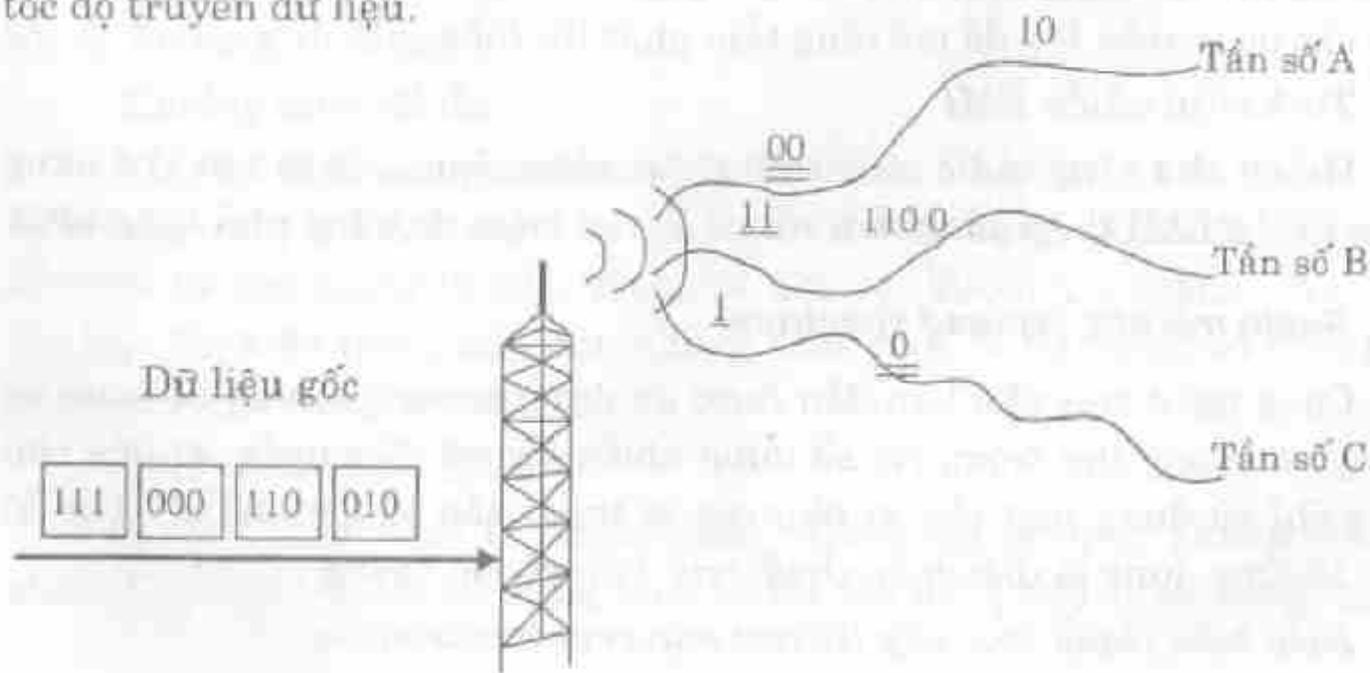
Điều biến chuỗi trực tiếp (Direct sequence modulation)

Dữ liệu ban đầu được tách thành các đoạn gọi là chip để truyền trên những tần số riêng biệt. Trạm phát có thể phát những dữ liệu giả trên những tần số riêng để đánh lừa thiết bị thu trộm. Trạm thu sẽ biết những tần số có dữ liệu thật, thu lấy các chip rồi khớp lại thành dữ liệu ban đầu. Kỹ thuật này có thể hoạt động trong các môi trường có nhiều cuộc truyền khác bởi có thể chọn nhiều tần số khác nhau.



Lập chãng tần số (frequency hopping)

Kỹ thuật này yêu cầu trạm phát và trạm thu phải hoạt động đồng bộ với nhau. Một số hệ thống truyền đồng thời trên nhiều tần số để nâng cao tốc độ truyền dữ liệu.



Miền tần số

Các hệ quang phổ trải thường hoạt động trong miền tần số tự do, tần số hay gặp nhất là 1 GHz và 2,4 GHz.

Chi phí

Ở mức trung bình

Cài đặt

Phụ thuộc từng hệ thống và tần số sử dụng, nói chung là kĩ thuật lắp đặt không phức tạp.

Tốc độ truyền

Với hệ thống sử dụng tần số 1 GHz sẽ cho tốc độ truyền tin khoảng 10 Mbps. Tần số cao hơn như 2,4 GHz sẽ cho tốc độ cao hơn.

Khoảng cách tối đa

Độ suy dẫn của tín hiệu sóng còn phụ thuộc vào tần số và công suất mà hệ thống đang sử dụng. Các LAN quang phổ trải thường hoạt động với công suất thấp và do đó có độ suy giảm cao.

Tính chịu nhiễu EMI

Mặc dù trên từng tần số đơn thì tín hiệu dễ bị ảnh hưởng bởi các nguồn phát sóng lạ, nhưng do hệ thống quang phổ trải có chọn nhiều dải tần khác nhau nên những tần số có mức nhiễu thấp nhất, cho tín hiệu rõ nhất sẽ được chọn.

1.7.10. Viba

Truyền thông viba có hai dạng: viba mặt đất và viba vệ tinh.

• *Viba mặt đất*

Trong kĩ thuật viba mặt đất, trạm phát và trạm thu đều đặt trên mặt đất, tại các điểm cao như nóc nhà cao tầng, tháp phủ sóng... Các tần số được dùng nằm trong dải tần thấp nhất của sóng viba để hạn chế tín hiệu không vượt qua đường chân trời. Trạm phát có thể sử dụng ăngten parabol để tạo ra một tín hiệu hẹp có độ định hướng cao, trạm thu cũng dùng ăngten parabol đã được căn chỉnh thật chính xác hướng về trạm phát. Cũng có thể dùng phương pháp truyền không định hướng, đặt các Hub vô tuyến để tiếp sóng và phủ sóng khắp trên phạm vi đặt các máy trạm.

Miền tần số: thường nằm trong dải tần số 4 – 6GHz và 21 – 23GHz

Chi phí: Tùy theo công suất và tần số mà hệ thống sử dụng. Các hệ viba đường dài thường tốn kém hơn tầm ngắn.

Cài đặt: Do các tần số sử dụng nằm trong dải tần được quản lý nên việc lắp đặt phải xin phép. Kỹ thuật cài đặt các ăngten không đơn giản và thường được tiến hành bởi các công ti truyền thông chuyên nghiệp.

Tốc độ truyền: có thể cao cỡ 100 Mbps

Hiện tượng suy dẫn: phụ thuộc vào công suất, tần số và kiểu ăngten thu phát. Ngoài ra, các điều kiện tự nhiên như mưa gió, sương mù... có thể làm tăng độ suy dẫn của tín hiệu.

Tính chịu nhiễu EMI: các hệ thống viba mặt đất dễ bị nhiễu và bị nghe trộm điện tử. Người ta phải dùng các kỹ thuật mã hóa để tránh bị thu trộm.

• Viba vệ tinh

Sử dụng các vệ tinh địa tĩnh để tiếp sóng phiên truyền. Các vệ tinh này hoạt động trên độ cao 22.300 dặm so với mặt đất, đó là khoảng cách lớn so với đường kính trái đất, do đó khoảng cách từ trạm phát tới trạm thu gần như là không phụ thuộc vào vị trí cụ thể trên mặt đất của chúng. Thời gian để tín hiệu truyền từ trạm phát tới trạm thu do đó bằng một đại lượng không đổi gọi là *độ trễ lan truyền – propagation delay*, có giá trị từ 0,5 đến 5 giây.

Miền tần số: thường nằm trong dải tần số 11–14 MHz.

Chi phí: rất cao. Chi phí để phóng và duy trì một vệ tinh có thể lên tới hàng tỉ đôla, do đó các dịch vụ truyền qua vệ tinh thường được cho thuê qua nhiều cấp người dùng.

Cài đặt: Việc lắp các trạm thu mặt đất tương đối đơn giản nhưng phải có giấy phép sử dụng vì tần số nằm trong miền tần số được quản lý.

Tốc độ truyền: có thể rất cao. Tùy theo số tiền thuê mà băng thông là cao hay thấp.

Hiện tượng suy giảm: phụ thuộc vào công suất, tần số và kiểu ăngten thu phát. Ngoài ra, các điều kiện tự nhiên như mưa gió, sương mù... có thể làm tăng độ suy giảm của tín hiệu.

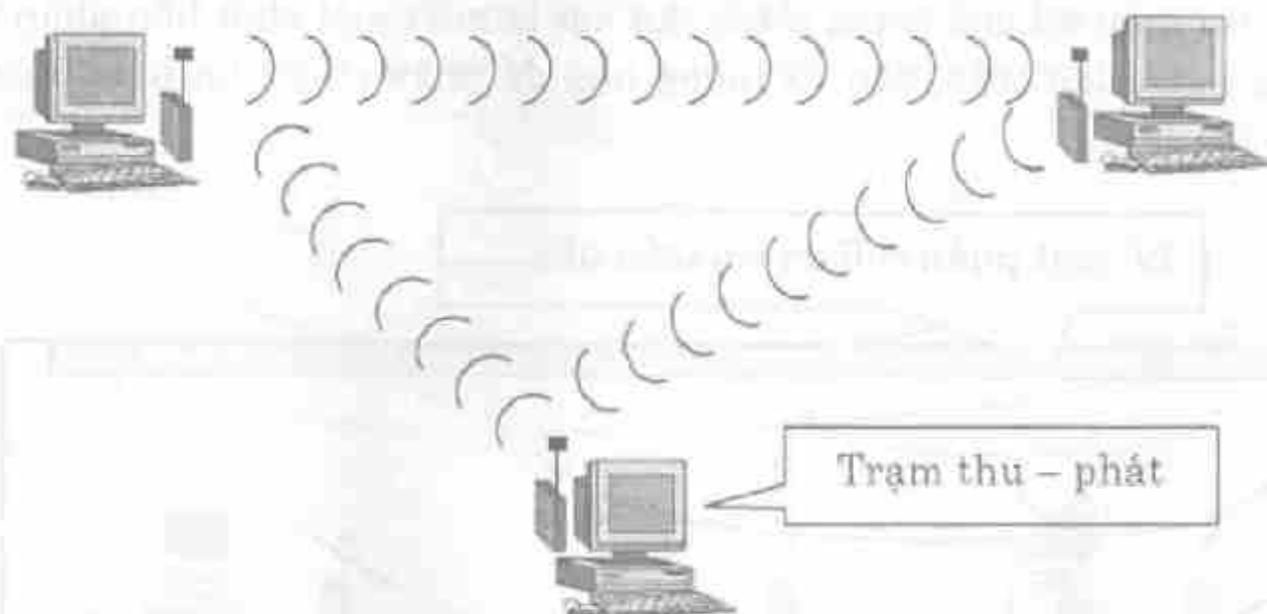
Tính chịu nhiễu EMI: các hệ thống viba mặt đất dễ bị nhiễu và bị nghe trộm điện tử. Người ta phải dùng các kỹ thuật mã hóa để tránh bị thu trộm.

1.7.11. Tia hồng ngoại

Hai phương pháp truyền tin bằng tia hồng ngoại đang được sử dụng là: *Điểm nối Điểm (point to point)* và *Quảng bá (broadcast)*.

Phương pháp Điểm nối Điểm

Mạng Point to Point hoạt động bằng cách tiếp sóng các tín hiệu tia hồng ngoại từ thiết bị này đến thiết bị kế tiếp. Tín hiệu được tập trung trong một chùm tia hẹp hướng từ trạm phát thẳng tới trạm thu. Do đó hai trạm phải được định vị chính xác về phía nhau và phương pháp này không thích hợp khi các máy trạm phải di chuyển thường xuyên.



Khi các máy trạm đặt ở xa cỡ vài kilômet, có thể dùng tia laser thay thế cho tia hồng ngoại vì tia hồng ngoại không thể tập trung công suất với khoảng cách xa như vậy.

Miền tần số: Tia hồng ngoại thường nằm trong dải tần dưới mức ánh sáng mắt thường nhìn thấy được, từ 100 GHz đến 1000 THz.

Chi phí: Cao hơn so với hệ thống mạng hữu tuyến. Hầu hết những mạng hồng ngoại thông thường đều sử dụng tia hồng ngoại phát ra từ các đèn LED. Để phát đi xa phải thay nguồn sáng LED bằng công nghệ Laser công suất cao với mức chi phí đắt hơn nhiều.

Cài đặt: Tương đối dễ dàng để điều chỉnh các trạm thu và phát chiếu thẳng vào nhau. Chú ý khi dùng tia Laser công suất cao vì nó có thể làm tổn thương võng mạc khi chiếu vào mắt người.

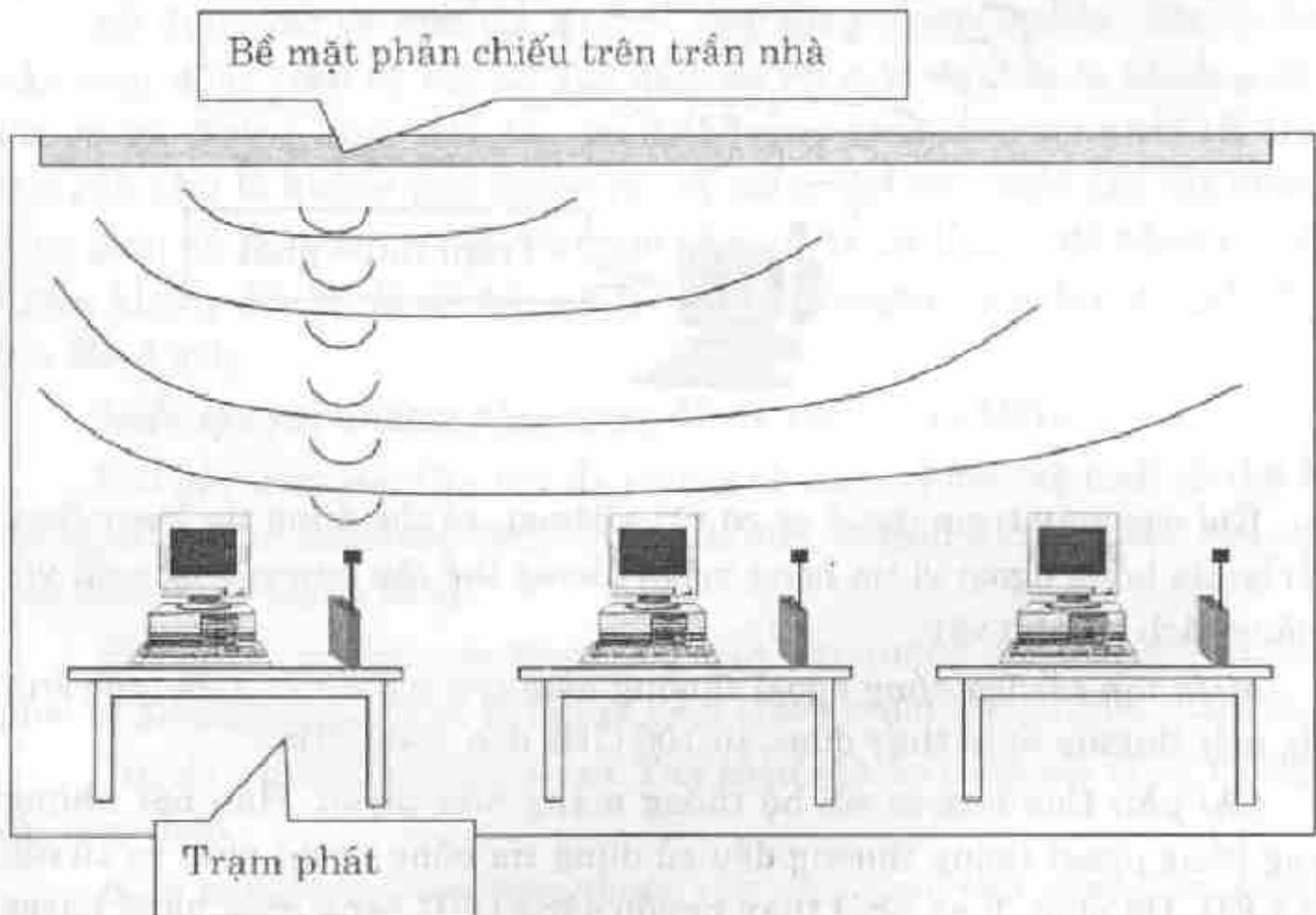
Tốc độ truyền: Có thể cao cỡ 100 Mbps

Hiện tượng suy giảm: phụ thuộc vào công suất, các chướng ngại vật trên đường truyền và các điều kiện tự nhiên như mưa gió, sương mù... có thể làm tăng độ suy giảm của tín hiệu.

Tính chịu nhiễu EMI: các hệ thống mạng tia hồng ngoại không nhạy cảm với các nhiễu radio nhưng lại bị ảnh hưởng bởi các loại tia sáng khác. Do hướng truyền thu hẹp và tập trung nên khó bị thu trộm điện tử.

• *Phương pháp Quang bá:*

Thay vì một chùm tia tập trung như phương pháp trên, tín hiệu được phủ rộng để nhiều trạm có thể thu được đồng thời. Có hai kĩ thuật thường dùng. Cách thứ nhất là đặt một thiết bị Thu - Phát tại vị trí cao để phát tín hiệu tới mọi trạm. Cách thứ hai là quét một chất liệu phản xạ tia hồng ngoại lên trần, sàn và tường nhà để phản chiếu tia hồng ngoại đi khắp tòa nhà.



Miền tần số: tia hồng ngoại thường nằm trong dải tần dưới mức ánh sáng mắt thường nhìn thấy được, từ 100 GHz đến 1000 THz.

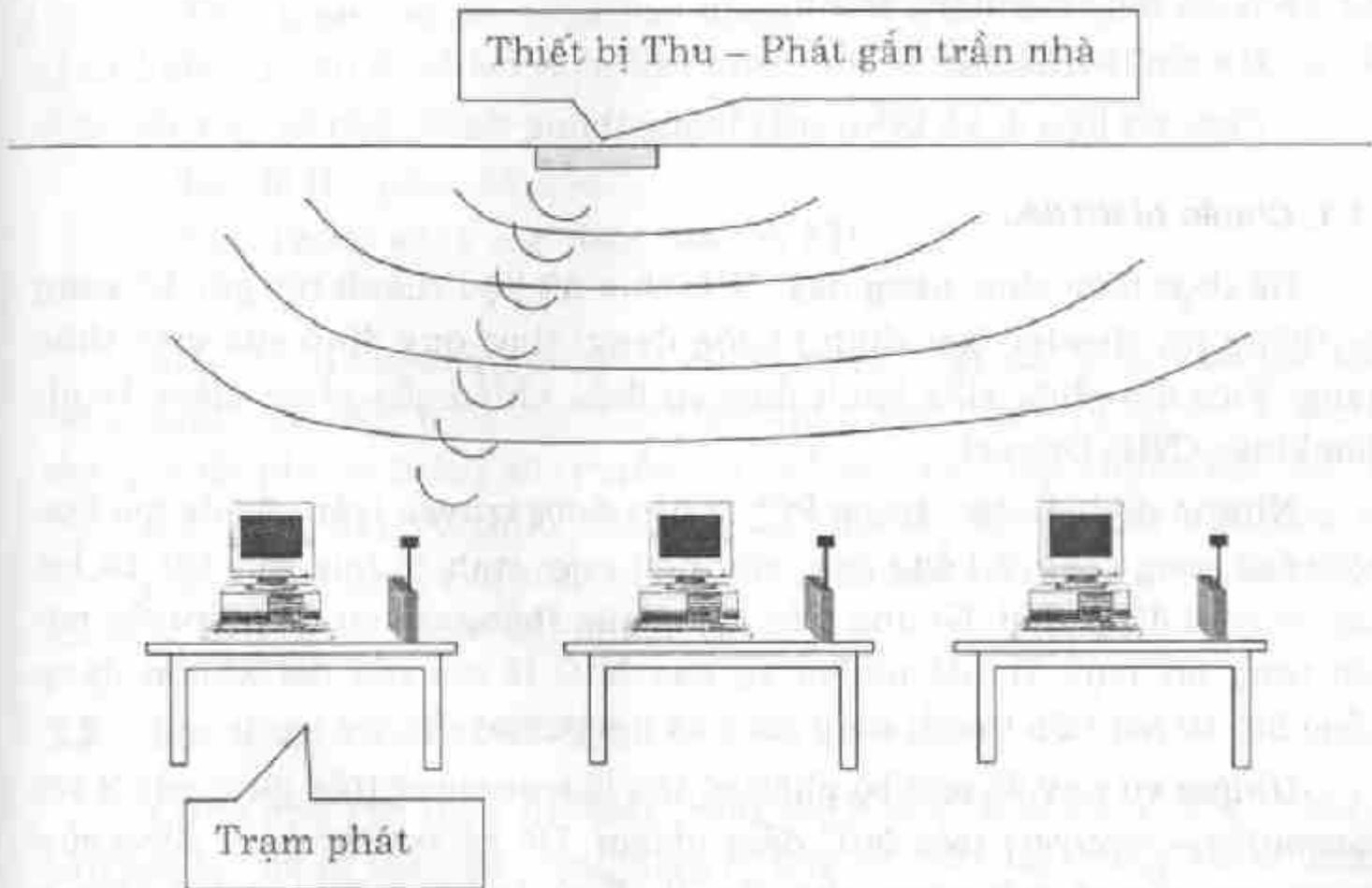
Chi phí: cao hơn so với hệ thống mạng hữu tuyến. Tia Laser không thích hợp cho loại mạng này vì nó truyền tập trung chứ không phủ rộng.

Cài đặt: rất dễ dàng vì không cần phải điều chỉnh để các trạm thu và phát chiếu thẳng vào nhau.

Tốc độ truyền: thấp hơn mạng Point to Point.

Hiện tượng suy dần: phụ thuộc vào công suất, các chướng ngại vật trên đường truyền và các điều kiện khí hậu. Khoảng cách tối đa không quá 100 mét. Các thiết bị thu và phát dễ bị ảnh hưởng bởi các nguồn sáng chói nên phải lưu ý điều chỉnh độ sáng của môi trường xung quanh.

Tính chịu nhiễu EMI: các hệ thống mạng tia hồng ngoại không nhạy cảm với các nhiễu radio nhưng lại bị ảnh hưởng bởi các loại tia sáng khác.

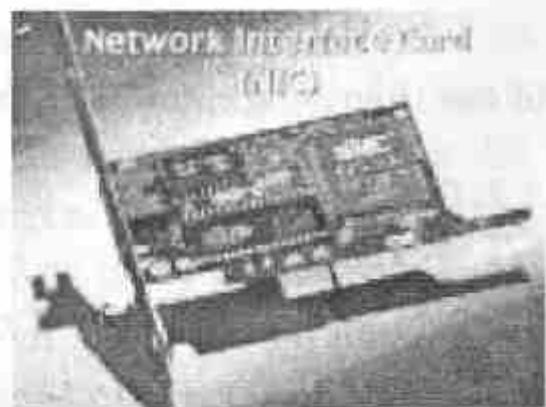


2. BẢNG MẠCH GIAO TIẾP MẠNG

2.1. Tên gọi và chức năng

Trong tiếng Anh, bảng mạch giao tiếp mạng được gọi là:

- Network Interface Card (NIC)
- Network board



- Network Adapter

- LAN card

...

Còn trong tiếng Việt có một số cách dịch: NIC, bo mạch mạng,

NIC đóng vai trò kết nối vật lý giữa máy tính với đường truyền mạng. Trước kia nó được cắm vào một trong các khe cắm mở rộng (Expansion slot) trên bo mạch chính còn hiện nay thường được tích hợp luôn vào bo mạch này. NIC được nối với cáp mạng thông qua một trong các loại cổng: AUI, BNC, RJ45, cổng cáp quang.

- NIC có hai chức năng chính

- Chuẩn bị dữ liệu.

- Phát dữ liệu đi và kiểm soát luồng thông tin.

2.1.1. Chuẩn bị dữ liệu

Để thực hiện chức năng này, NIC chia dữ liệu thành các gói, bổ sung các thông tin Header (xác định khuôn dạng) theo quy định của giao thức mạng. Việc này được tiến hành dưới sự điều khiển của phần mềm Trình điều khiển (NIC Driver).

Như ta đã biết, bên trong PC dữ liệu được truyền trên các đường bus một cách song song. Chẳng hạn như nếu máy tính có bus ISA thì 16 bit được truyền đồng thời. Nhưng trên cáp mạng thông tin lại được truyền nối tiếp từng bit một. Do đó nhiệm vụ của NIC là chuyển đổi khuôn dạng luồng bit, từ nối tiếp thành song song và ngược lại.

Nhiệm vụ này do một bộ phận có tên là *tranceiver* (tên ghép của 2 từ: *transmitter* - *receiver*) trên NIC đảm nhiệm. Để hỗ trợ cho hoạt động của *tranceiver*, cần có một vùng nhớ đệm (*buffer*) để lưu trữ tạm thời những dữ liệu chưa kịp gửi đi hay xử lý. Vùng nhớ đệm này có thể có 2 xuất xứ:

- NIC tự có một chip nhớ riêng. Thường thấy ở các NIC hiện nay.
- PC dành một phần RAM cho NIC dùng làm *buffer*, đây là các NIC chế tạo theo công nghệ thấp trước đây.

2.1.2. Gửi dữ liệu

Địa chỉ mạng

Để liên lạc với nhau, mỗi thiết bị mạng phải có một địa chỉ phân biệt. Địa chỉ này do IEEE cấp theo cơ chế: các hãng sản xuất được phân những

vùng địa chỉ khác nhau, mỗi hãng tự gán những địa chỉ phân biệt trong vùng được phép cho các sản phẩm của mình. Những địa chỉ này được *ghi cứng** vào ROM của thiết bị để người sử dụng không thể can thiệp thay đổi được.

Cơ chế bắt tay (hand shaking)

Trước khi NIC thật sự gửi dữ liệu đi, nó phải tiến hành đàm phán với NIC ở đầu nhận để cùng thống nhất các thông số cuộc truyền như:

- Kích thước tối đa của gói tin.
- Thời gian nghỉ giữa hai lần phát dữ liệu.
- Thời gian chờ tín hiệu báo nhận. Nếu quá thời gian này mà bên phát không nhận được tín hiệu báo nhận, nó sẽ hiểu là dữ liệu không đến được đích và sẽ phát lại.
- Tốc độ thu phát dữ liệu.
- Kích thước vùng nhớ đệm của hai NIC.

.....

Nếu 2 NIC khác nhau, một cũ và chậm, cái kia được chế tạo theo công nghệ cao nên hiện đại hơn thì chúng phải đàm phán với nhau để thống nhất những thông số truyền mà cả hai cùng chấp nhận được. Một số NIC mới hiện nay có chức năng tự điều chỉnh tốc độ cho phù hợp với những thiết bị chậm hơn trên mạng. Chỉ sau khi thống nhất về các thông số, cuộc truyền mới được bắt đầu.

2.2. Các tham số cấu hình

Cũng như các thiết bị khác trong máy tính, NIC có những thông số cần xác lập để có thể hoạt động nhịp nhàng với toàn hệ thống. Đó là những thông số cấu hình sau đây.

2.2.1. Ngắt (IRQ: Interrupt Request Line)

Ngắt là số hiệu đường truyền qua đó NIC cũng như một thiết bị ngoại vi gửi tín hiệu tới CPU yêu cầu được phục vụ. Có nhiều ngắt với những mức ưu tiên khác nhau. Nói chung, để tránh xảy ra xung đột về ngắt có thể dẫn đến treo máy, mỗi thiết bị ngoại vi như NIC, sound card, modem... nên chọn lấy một ngắt riêng biệt, kể cả trong các hệ thống mới tự

* Việc ghi cứng được thực hiện bằng tia cực tím hoặc bằng điện áp rất cao

động phân bố ngắt như PCI. Để làm điều đó, trước khi lắp đặt bảng mạch cần phải tìm ra những ngắt nào còn trống để gán cho bảng mạch vào ngắt đó.

Bảng các ngắt thông dụng

Số hiệu IRQ	Thiết bị
2 (9)	Bảng mạch màn hình (video graphic adapter)
3	Bỏ trống
4	COM 1, COM 3
5	Bỏ trống (trừ khi dùng cho cổng LPT 2 hoặc Sound card)
6	Floppy disk controler
7	LPT 1
8	Time clock
10	Bỏ trống
11	Bỏ trống
12	Mouse PS/2
13	Math co-processor
14	Hard disk controler
15	Bỏ trống

Giá trị mặc định (default) cho NIC là IRQ 3 hoặc 5. Việc gán một ngắt cho NIC, cũng như việc xác lập các thông số cấu hình khác của nó, có thể được thực hiện theo hai cách.

Cách thứ nhất dành cho những bảng mạch đời cũ sử dụng những Jumper (cầu nhảy), Switch (công tắc)... để xác lập các thông số cấu hình cho vỉ mạch. Việc này phải thực hiện một cách khá thủ công. Trước hết phải tắt máy, mở vỏ máy, rút bảng mạch ra, tìm và gạt các mức tương ứng trên các Jumper hay Switch. Sau đó cắm bảng mạch vào, bật máy chạy thử, nếu chưa được lại phải làm lại. Việc này đòi hỏi sự khéo léo và nhiều kinh nghiệm nên chỉ những nhân viên chuyên nghiệp mới làm nổi và rõ ràng nó rất bất tiện, gây khó khăn cho những người sử dụng thông thường.

Cách thứ hai: những bảng mạch đời mới đã khắc phục nhược điểm

trên bảng cách cho phép xác lập cấu hình hoàn toàn thông qua phần mềm. Người sử dụng chỉ việc chạy những phần mềm – thường nằm trong bộ phần mềm Driver đi kèm bảng mạch – là có thể dễ dàng chọn và xác lập các thông số cấu hình. Một số phần mềm Plug and Play còn tự động tìm kiếm và khuyến cáo những thông số tối ưu cho người sử dụng, thậm chí tự động xác lập các thông số cấu hình.

2.2.2. Cổng nhập xuất (I/O port)

Là kênh truyền dữ liệu giữa một thiết bị ngoại vi, chẳng hạn NIC, với CPU. Cổng nhập xuất là một địa chỉ dạng hexa, ví dụ như

Bảng các cổng I/O cơ bản

Số hiệu cổng	Thiết bị	Số hiệu cổng	Thiết bị
200 – 20F	Cổng trò chơi (Game port)	370 – 37F	LPT 2
230 – 23F	Mouse	380 – 3BF	LPT 1
270 – 27F	LPT 3	3C0 – 3CF	Bảng mạch EGA / VGA
2F0 – 2FF	COM 2	3F0 – 3FF	Bảng mạch điều khiển đĩa

Mỗi thiết bị trong hệ thống cần có một cổng riêng biệt, tương tự như đối với ngát.

2.2.3. Địa chỉ vùng nhớ cơ sở (base memory address)

Như phần 2.1.1 "Chuẩn bị dữ liệu" đã trình bày, NIC cần có một vùng nhớ đệm (buffer) để lưu trữ tạm thời những dữ liệu chưa kịp chuyển đi. Nếu buffer này NIC không có sẵn mà phải lấy từ RAM của hệ thống thì địa chỉ của vùng RAM này được gọi là *địa chỉ vùng nhớ cơ sở (base memory address)*. Thông thường địa chỉ này là D8000. Với phần mềm xác lập cấu hình đi kèm theo driver của vỉ mạch, chúng ta có thể lựa chọn địa chỉ và kích thước – khoảng 16 hay 32 KB – cho vùng buffer này.

2.2.4. Cổng kết nối

NIC có thể có 1, 2 thậm chí 3 cổng để kết nối với cáp mạng bên ngoài. Thông qua phần mềm xác lập cấu hình đi kèm theo bảng mạch chúng ta sẽ ấn định loại cổng phù hợp với cáp mạng hiện có. Ví dụ:

- Cổng RJ-45, hay còn gọi là 100 Base T, cho cáp xoắn.
- Cổng RG58, còn gọi là BNC hay 10 Base T, cho cáp đồng trục mảnh.
- Cổng AUI, còn gọi là DB15 vì có 15 chân female, cho cáp đồng trục dày.

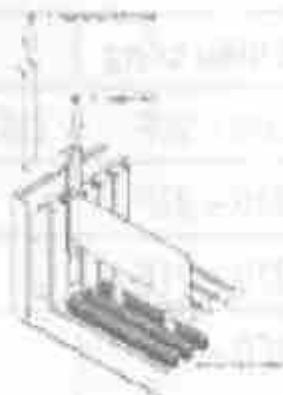
Sau đó, dữ liệu sẽ chỉ được đưa ra những cổng đã chọn mà không ra những cổng còn lại nếu có.

2.3. Kiến trúc bus

Với những NIC được tích hợp vào trong bo mạch chính (on board) thì không có gì phải bàn, nhưng nếu NIC là một bảng mạch rời thì trước khi cắm vào máy chúng ta phải xem xét liệu nó có tương thích với kiến trúc bus của máy hay không. Sau đây là một số loại bus chính của PC.

2.3.1. ISA (*Industry Standard Architecture*)

Có 2 loại: loại 8 bit và loại 16 bit. ISA do IBM đưa ra thị trường vào năm 1984. Bảng mạch 8 bit có thể cắm vào khe cắm (slot) 16 bit. Bus ISA có tốc độ truyền 8 Mbps, không cho phép chia sẻ ngắt (non-shareable interrupt) và có màu đen.



2.3.2. EISA (*Extended Industry Standard Architecture*)

EISA là chuẩn bus do tập đoàn 9 hãng lớn trong lĩnh vực công nghiệp máy tính là: AST, Compaq, Epson, HP, NEC, Olivetti, Tandy, Wyse và Zenit đưa ra vào năm 1988. EISA cung cấp đường truyền dữ liệu 32 bit với tốc độ truyền 33Mbps nhưng vẫn tương thích với ISA, nghĩa là các bảng mạch ISA có thể cắm và hoạt động trên các slot EISA. Điểm mạnh của EISA là tính năng bus-master, đây là công nghệ cải tiến hơn so với DMA cho phép các thiết bị ngoại vi có nhiều quyền tự chủ hơn trong việc truyền dữ liệu và nhờ vậy giải phóng CPU khỏi công việc quản lý đường bus. EISA có hình dạng và kích thước giống như ISA, chỉ khác ở màu xanh lá cây. Kiến trúc bus EISA thường được dùng trong các máy server chứ rất ít gặp trong các máy trạm.

2.3.3. Local Bus

Local bus là một công nghệ mang tính đột phá làm tăng đáng kể hiệu năng của hệ thống bus trong PC, cho phép các ngoại vi truyền dữ liệu

trên những đường bus với độ rộng và tốc độ xung nhịp nhanh hơn nhiều, sánh ngang với các thành phần vốn vẫn được ưu tiên như Memory, CPU. Ban đầu local bus có hai biến thể: VL và PCI. Trải qua sự sàng lọc của thực tế, VL (VESA local bus) lộ rõ sự yếu kém và bị đào thải. Hiện nay PCI (Peripheral Component Interconnect) là kiến trúc bus chủ yếu trong các máy tính PC và Apple Macintosh. Nó cung cấp đường truyền có độ rộng 32, 64, 128 và thậm chí lên đến 256 bit với tốc độ 133 Mbps cho các ngoại vi. PCI hỗ trợ tính năng Plug and Play cho phép xác lập và thay đổi cấu hình thiết bị một cách dễ dàng, gần như tự động để hầu hết mọi người sử dụng đều có thể tự làm được. Tính năng bus master vẫn được hỗ trợ trên bus PCI. Kích thước của slot PCI ngắn chỉ bằng một nửa so với ISA và có màu trắng.

2.4. Boot ROM

Trong một số cơ quan, do yếu tố bảo mật nên người ta cần phải xây dựng những mạng máy tính với các máy trạm không có ổ đĩa (diskless workstation) để hạn chế việc sao chép trộm thông tin. Vấn đề là làm thế nào để khởi động các máy trạm đó. Giải pháp cho việc này là sử dụng những NIC được gắn thêm một chip đặc biệt có tên là Remote boot PROM, còn gọi tắt là Boot ROM. Trong chip ROM này đã cài đặt sẵn đoạn mã khởi động máy tính và chương trình này sẽ tìm đến máy chủ để tải về những phần còn lại của hệ điều hành mạng đủ cho máy trạm hoạt động bình thường và đăng nhập mạng.

3. TRÌNH ĐIỀU KHIỂN

3.1. Vai trò, chức năng của trình điều khiển

Trình điều khiển thiết bị, thường gọi tắt là trình điều khiển (device driver), là phần mềm cho phép hệ điều hành của máy tính làm việc với một thiết bị phần cứng nào đó. Sau khi đã kết nối máy tính với thiết bị bên ngoài hay mở vỏ máy để lắp đặt thiết bị vào bên trong, ta vẫn chưa thể làm việc ngay cho đến khi trình điều khiển tương ứng được cài đặt. Trình điều khiển sẽ giúp hệ điều hành biết cách quản lý, làm việc với thiết bị ra sao, điều khiển nó như thế nào. Hầu như có bao nhiêu loại thiết bị ngoại vi thì có chừng ấy trình điều khiển tương ứng phải được cài đặt, đó là:

Các thiết bị nhập như mouse, scanner, camera...

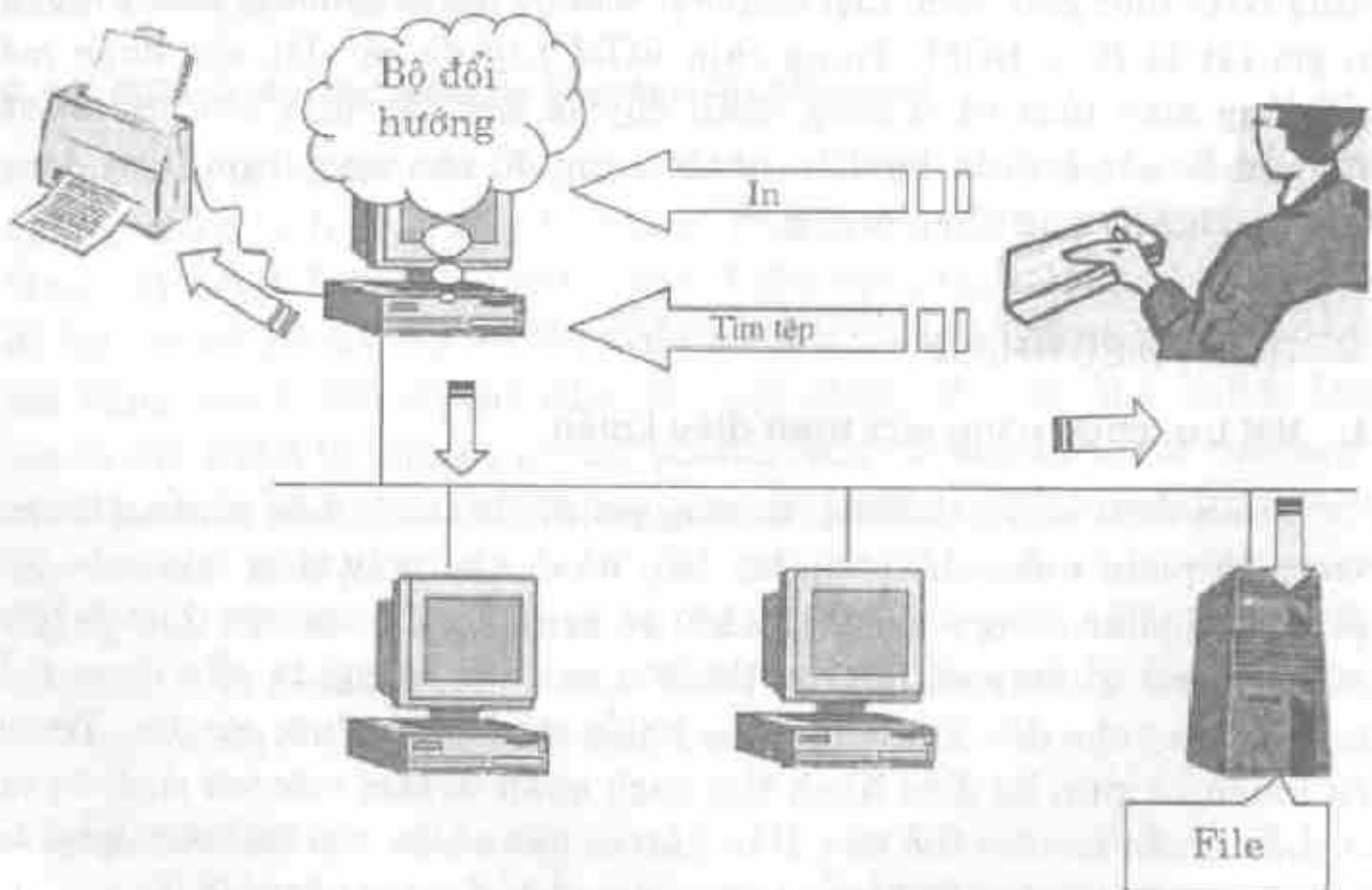
- Bảng mạch điều khiển đĩa (disk controller) SCSI, IDE, Flash memory, ...
- Bảng mạch âm thanh, NIC, bảng mạch tăng tốc đồ họa...
- Máy in, máy vẽ, ổ băng từ (tape)...

3.2. Trình điều khiển cho NIC

Trình điều khiển NIC có những vai trò cụ thể sau

3.2.1. Giao tiếp với bộ đổi hướng

Khái niệm: Bộ đổi hướng mạng (network redirector) thực ra không phải là thiết bị phần cứng mà là công cụ phần mềm thực hiện một chức năng của hệ điều hành mạng. Nó nhận các yêu cầu nhập, xuất các tài nguyên rồi xem xét. Nếu đó là các tài nguyên cục bộ hiện có trên máy tính, chẳng hạn đó là yêu cầu in ra một máy in đang nối vào cổng LPT1, thì chuyển cho hệ điều hành để truy xuất tài nguyên đó. Nếu đó là các tài nguyên mạng thì chuyển thành lời yêu cầu gửi lên đường truyền mạng.



3.2.2. Bảo đảm giao tiếp giữa hệ điều hành với NIC

Trình điều khiển thực hiện một trong các chức năng của tầng con MAC trong tầng Datalink*, hay nó là một thực thể của tầng này. Chức năng đó là cung cấp khả năng truy nhập NIC cho các thiết bị ở tầng vật lí. Nói cách khác, trình điều khiển NIC hỗ trợ cho việc giao tiếp giữa các phần mềm mạng với NIC



3.3. Xuất xứ của trình điều khiển

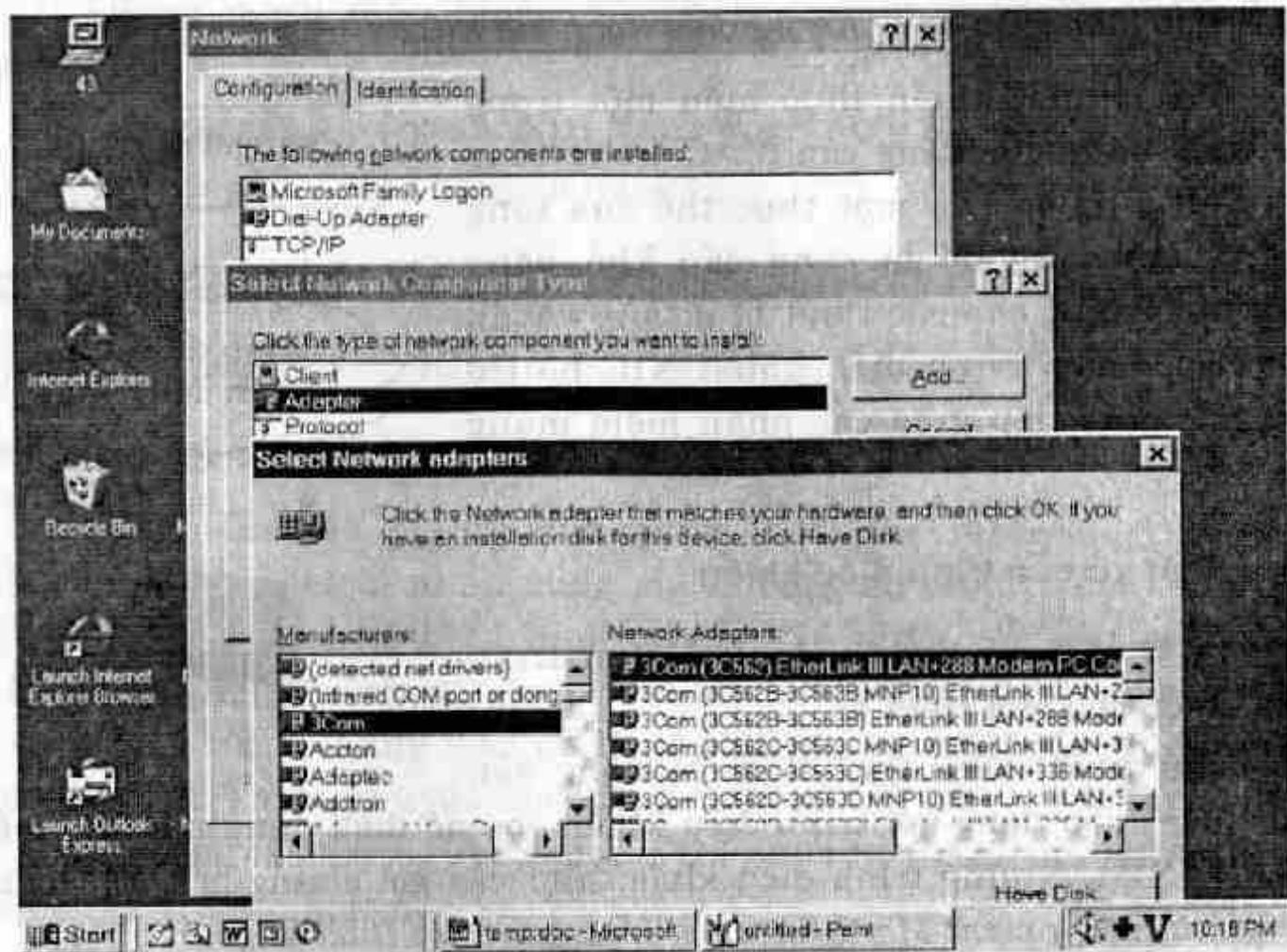
Có 3 cách có thể áp dụng để tìm trình điều khiển cho một thiết bị.

Thứ nhất, kèm theo thiết bị hãng sản xuất luôn luôn đóng gói trình điều khiển cho nó dưới dạng một đĩa mềm hay CDROM. Những trình điều khiển như vậy gọi chung là *OEM driver* (*Original Equipment Manufacturer: Nhà sản xuất thiết bị gốc*).

Nếu đĩa chứa trình điều khiển bị thất lạc, ta có thể tìm nó tại trang Web của hãng sản xuất dựa theo tên, số seri của thiết bị. Trên Internet có những Web site cung cấp miễn phí rất nhiều driver cho đủ các loại thiết bị ngoại vi, chẳng hạn như *www.hardwarecentral.com* hay *www.hardwarezone.com*.

Nếu là một thiết bị không quá hiếm, có thể tìm thấy nó trong *Danh sách phần cứng tương thích (hardware compatibility list – HCL)* của hệ điều hành. Đây là danh sách những thiết bị thông dụng mà trình điều khiển của chúng đã được kiểm định và tích hợp sẵn vào trong hệ điều hành.

* Xem Chương 3, phần Mô hình OSI



3.4. Cài đặt

Khi nào thì phải tiến hành cài đặt trình điều khiển cho NIC? Ta đều biết rằng thiếu trình điều khiển thì NIC không thể hoạt động được, do vậy cần phải cài đặt khi:

- Install hệ điều hành mạng vào máy.
- Có sự thay đổi: NIC cũ bị tháo bỏ thay thế bằng NIC mới khác loại.

Việc cài đặt này, thường được gọi là install hay setup, được tiến hành sau khi đã hoàn tất các thao tác lắp phần cứng. Có hai phương pháp cài đặt:

– Với những hệ điều hành Plug and Play như họ Windows, hệ điều hành sẽ tự động nhận biết chủng loại NIC và chọn lựa những thông số cấu hình tối ưu cho nó, nghĩa là việc cài đặt diễn ra gần như tự động. Khi gặp phải những NIC hiếm, không có trong HCL thì phải tiến hành theo cách thứ hai sau đây.

– Sử dụng phần mềm install đi kèm với driver của NIC. Phần mềm này sẽ hỗ trợ người dùng chọn lựa những thông số cấu hình tối ưu cho NIC. Đây là phương pháp tốt và nên áp dụng.

CÂU HỎI CUỐI CHƯƠNG

Điền từ (cụm từ) vào chỗ trống:

1. Coaxial dịch ra là, còn cáp xoắn dịch từ thuật ngữ tiếng Anh là
2. Cáp quang là dịch từ thuật ngữ tiếng Anh là
3. Cáp xoắn đôi trần và cáp xoắn đôi có bọc gọi theo tiếng Anh là và
4. Viện kĩ thuật điện & điện tử (IEEE) đặt tên cho cáp thick-coaxial là 10 Base 5 với ý nghĩa như sau: 10 chỉ thông lượng tối đa 10 Mbps, còn Base có nghĩa là và 5 có nghĩa là
5. Hãy so khớp các mục thông tin phù hợp trong 2 cột sau

- | | |
|-------------------------|---|
| 3 a) Cáp đồng trục mảnh | 1) có lớp vỏ chống nhiễu phủ bên ngoài. |
| 4 b) Cáp xoắn UTP | 2) nối vào RJ-11 connector. |
| 5 c) Cáp đồng trục dày | 3) gắn kết các chỗ nối trên mạng bằng BNC và T-connector. |
| 1 d) Cáp STP | 4) nối vào RJ-45 connector. |
| | 5) sử dụng bộ nối xuyên lỗ (vampire tap) và cổng AUI. |

6. Hãy so khớp các mục thông tin phù hợp trong 2 cột sau:

- | | |
|--|---|
| 2 a) Bandwidth | 1) truyền tín hiệu tương tự (analog). |
| 3 b) Throughput | 2) khoảng tần số của tín hiệu mà cáp chấp nhận. |
| 4 c) Khả năng chống nhiễu của cáp quy định | 3) tốc độ truyền tín hiệu (bps) của cáp. |
| 5 d) Baseband | 4) toàn bộ khả năng của kênh dành cho một cuộc truyền. |
| 1 e) Broadband | 6) khoảng cách cực đại của cáp mà tín hiệu truyền trên đó không bị méo. |

7. Danh sách HCL là

- Danh sách các hệ điều hành mạng.
- Danh sách phần cứng đã được hãng bán hệ điều hành kiểm định và sử dụng.
- Danh sách các NIC và trình điều khiển tương ứng.
- Danh sách trình điều khiển mạng cục bộ.

8. Việc thiết lập các thông số cấu hình như IRQ, I/O Port ... trên các NIC cũ được thực hiện bằng cách còn hiện nay được thực hiện thông qua

Chương 3

MỘT SỐ MÔ HÌNH MẠNG

Chương này tập trung mô tả Mô hình tham chiếu hệ thống mở OSI (Open Systems Interconnection), Project 802 của IEEE và mô hình TCP/IP (DoD) dành cho việc phân lớp giao thức TCP/IP.

1. MÔ HÌNH OSI

1.1. Bối cảnh ra đời

Vào thời sơ khai của ngành mạng máy tính, các nhà thiết kế mạng là những ông chủ. Khách hàng không được coi là Thượng đế mà rơi vào thế bị lệ thuộc. Mỗi khi muốn nối mạng cho mình, họ phải cân nhắc lựa chọn trong số không nhiều những hãng cung cấp như IBM, DEC, HP, Honey Well, Sperry and Burroughs (nay là Unisys). Một khi đã quyết định mua thiết bị mạng của công ti nào rồi, khách hàng xem như bị khóa chặt vào công ti đó. Mọi việc bảo trì, cập nhật, thay đổi thiết kế, mở rộng hệ thống, cung cấp thêm thiết bị phải do chính hãng cung cấp ban đầu thực hiện. Nguyên nhân là vì mỗi hãng đều có quyền sở hữu thiết kế riêng, độc lập với nhau và khác nhau, các công nghệ cứ mạnh ai nấy phát triển, khả năng liên kết với các mạng của công ti khác hầu như không tồn tại. Giá cả vì thế cũng không có một mặt bằng chung có tính cạnh tranh mà lại được xướng ra dựa trên khả năng chi trả của khách hàng và chẳng ai dám kêu ca.

Tình trạng trên rõ ràng gây nhiều khó khăn cho khách hàng, những người sử dụng và đồng thời cản trở sự phát triển đi lên của chính công nghệ mạng. Một khi đã không có tính cạnh tranh tất cũng không có sự cải tiến để tự nâng cao. Những công nghệ không được áp dụng rộng rãi trên diện rộng sẽ chẳng được ai ưa chuộng. Vì vậy, một yêu cầu tất yếu là phải làm sao định rõ bộ khung tiêu chuẩn để xây dựng những hệ thống mở, trên đó các thiết bị của nhiều nhà cung cấp có thể hoạt động cùng với nhau.

Vào năm 1978, tổ chức tiêu chuẩn quốc tế ISO (International Organization of Standard: Tổ chức tiêu chuẩn hóa quốc tế) ban hành tập hợp các đặc điểm kĩ thuật mô tả kiến trúc mạng dành cho việc nối kết những thiết bị không cùng chủng loại. Năm 1984, ISO phát hành bản sửa đổi mô hình này và gọi là *Mô hình tham chiếu hệ thống mở OSI (Open Systems Interconnection)*, ngày nay mô hình này trở thành tiêu chuẩn quốc tế thông dụng và nổi tiếng nhất mô tả môi trường hoạt động mạng máy tính. Nó mô tả phương thức hoạt động của phần cứng và phần mềm mạng trong kiến trúc phân tầng và cung cấp khung tham chiếu mô tả các thành phần mạng hoạt động ra sao, liên kết với nhau như thế nào. Các hãng thiết kế sản phẩm mạng đều dựa trên những đặc điểm kĩ thuật của mô hình OSI để sản phẩm của mình có thể làm việc với sản phẩm của hãng khác và do đó mới được thị trường chấp nhận.

1.2. Kiến trúc phân tầng

Để làm giảm độ phức tạp cho việc thiết kế mạng, các mô hình mạng hiện nay như OSI, DoD đều được xây dựng dựa trên nguyên lí Kiến trúc phân tầng. Mỗi thành phần của mạng (chẳng hạn như một máy trạm) đều được xem như một cấu trúc gồm nhiều tầng (layer) trong đó mỗi tầng được xây trên tầng dưới nó. Số lượng tầng và chức năng của mỗi tầng là tùy theo từng mô hình, nhưng mọi thành phần trong mạng đều có số lượng và cấu trúc tầng như nhau. Những nguyên lí chung của mọi kiến trúc phân tầng là:

Mục đích của mỗi tầng luôn là để cung cấp một số dịch vụ nhất định cho tầng ngay bên trên, nói cách khác những tầng bên trên thường xuyên gửi những yêu cầu xuống cho tầng dưới. Chúng được giải quyết một phần, phần còn lại được chuyển xuống tầng dưới làm nốt.

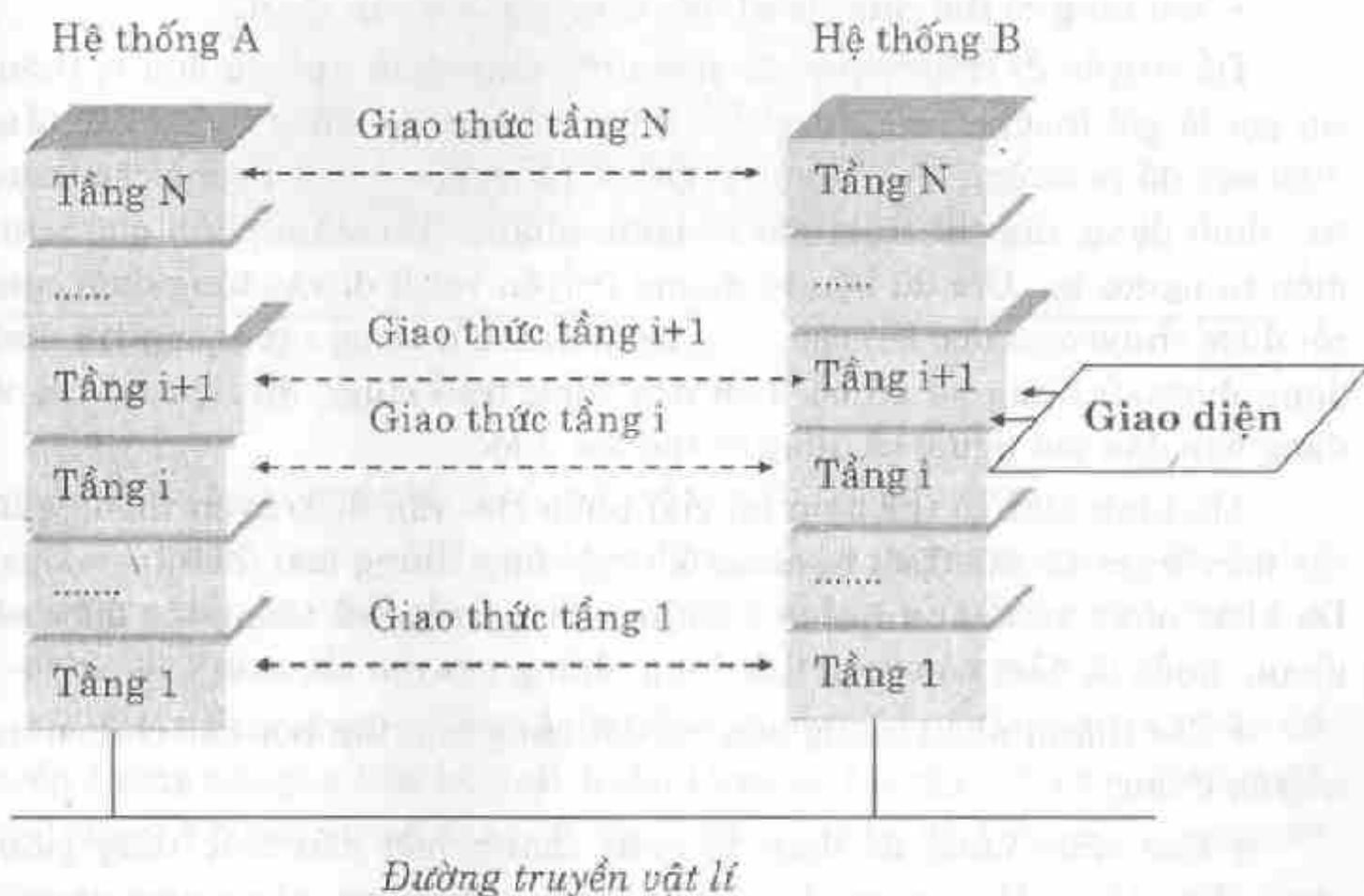
Tuy phục vụ cho tầng trên, nhưng tầng dưới luôn cố gắng che giấu cách mà nó thực hiện dịch vụ như thế nào. Về phía mình, tầng trên không hề quan tâm những chi tiết các yêu cầu gửi xuống được thực hiện ra sao. Chẳng hạn như người sử dụng e-mail không biết – và cũng không cần biết

* Thuật ngữ "Hệ thống mở" được hiểu là một hệ thống gồm các thành phần mạng có xuất xứ khác nhau có thể tương tác với nhau miễn là chúng tuân thủ đúng các chuẩn mô tả trong mô hình tham chiếu.

– những e-mail được truyền trên cáp mạng ra sao, mã hóa thành tín hiệu điện thế nào ... Ta nói rằng mỗi tầng đều cố gắng trở nên trong suốt đối với các tầng bên trên.

Nhờ không quan tâm đến hoạt động xảy ra ở tầng dưới, nên mỗi tầng đều hoạt động như thể nó đang giao tiếp với tầng đối tác cùng mức ở đầu bên kia của đường truyền. Đây là dạng giao tiếp ảo hay còn gọi là giao tiếp logic giữa những tầng đồng mức. Những bộ quy tắc quy định cách thức giao tiếp ảo gọi là giao thức.

Thực sự thì giao tiếp xảy ra giữa một tầng và tầng ngay bên dưới nó. Dòng dữ liệu từ mỗi tầng không đi thẳng sang tầng đồng mức mà đi xuống tầng dưới, đó gọi là giao tiếp vật lý. Môi trường giao tiếp vật lý giữa tầng trên với tầng dưới gọi là giao diện.



1.3. Giới thiệu mô hình OSI

1.3.1. Nguyên tắc xây dựng

Để xây dựng mô hình OSI, tiểu ban xây dựng chuẩn mạng của ISO cũng xuất phát từ các nguyên lý chung của kiến trúc phân tầng, dựa trên các nguyên tắc chủ yếu sau:

- Hạn chế số lượng các tầng để đơn giản hóa mô hình. Các chức năng giống nhau được đặt vào cùng một tầng. Những chức năng khác nhau, các loại công nghệ khác nhau được đặt trên các tầng khác nhau.

- Tạo ranh giới giữa các tầng sao cho tương tác giữa chúng là tối thiểu. Ranh giới được chọn có tham khảo những kinh nghiệm đã được thực tế chứng tỏ là thành công, sao cho có thể chuẩn hóa được những giao diện tương ứng. Ranh giới phải được chọn để giảm đến mức tối thiểu lưu lượng thông tin truyền qua.

- Một tầng được chọn khi việc xử lý dữ liệu ở đó là tách biệt với những tầng khác.

- Các chức năng được định vị sao cho có thể thiết kế lại tầng mà ảnh hưởng ít nhất đến những tầng khác.

- Mỗi tầng có thể chia thành các tầng con khi cần thiết.

Để truyền đi trên mạng, dữ liệu được chia thành nhiều đơn vị thông tin gọi là gói (packet) rồi được chuyển từ tầng trên cùng xuống các tầng dưới sau đó ra đường truyền vật lý. Ở mỗi tầng, gói được bổ sung các thông tin định dạng, địa chỉ trạm gửi và trạm nhận... Tại trạm nhận quá trình diễn ra ngược lại. Gói dữ liệu từ đường truyền vật lý đi vào tầng dưới cùng rồi được chuyển ngược lên các tầng trên. Tại mỗi tầng, các thông tin định dạng được sử dụng và gỡ bỏ. Lên đến tầng trên cùng, dữ liệu đã trở về dạng ban đầu mà người sử dụng có thể đọc được.

Mô hình OSI có thể đem lại giải pháp cho vấn đề truyền thông giữa các máy trạm và các thiết bị mạng không cùng chủng loại (heterogenous). Dù khác nhau về xuất xứ nhưng chúng vẫn liên lạc và tương tác được với nhau, miễn là đảm bảo tuân thủ đúng những nguyên tắc sau:

- Các thành phần mạng đều cài đặt cùng một tập hợp các chức năng truyền thông.

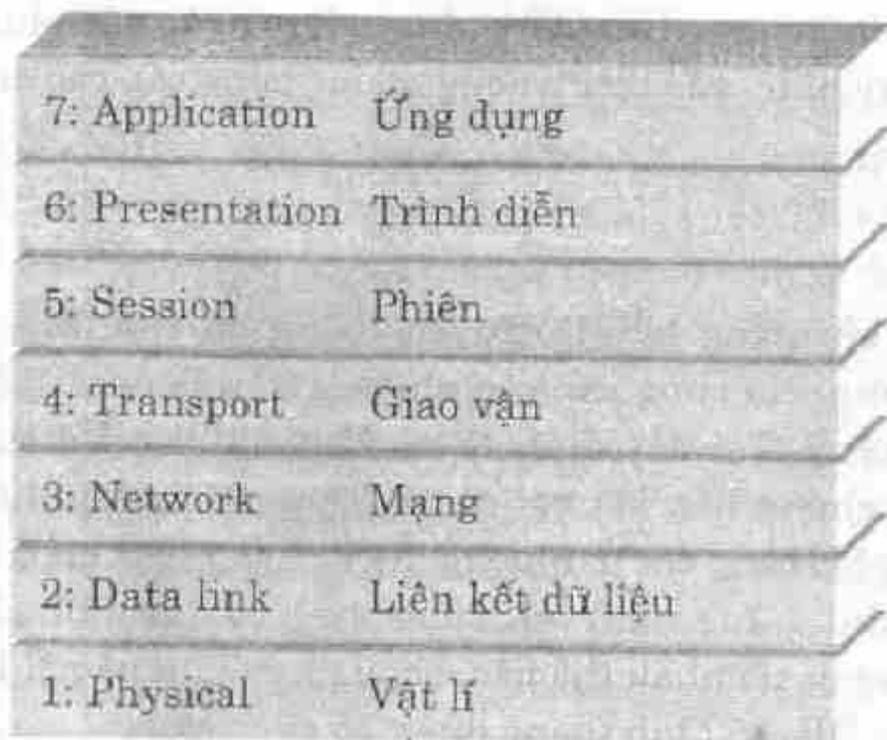
- Các chức năng đó được tổ chức thành một cấu trúc tầng giống nhau. Các tầng đồng mức phải cung cấp những chức năng như nhau – nhưng phương thức cung cấp có thể khác nhau.

- Các tầng đồng mức phải sử dụng một tập giao thức chung.

Để đảm bảo những nguyên tắc trên cần phải có những chuẩn. Chuẩn quy định chức năng và dịch vụ được cung cấp bởi mỗi tầng nhưng không ràng buộc việc chúng được cài đặt cụ thể ra sao, điều đó là khác nhau tùy theo mỗi nhà sản xuất. Mô hình OSI chính là cơ sở để xây dựng các chuẩn đó.

1.3.2. Cấu trúc

Được xây dựng theo những nguyên tắc nêu trên, mô hình OSI gồm có 7 tầng như hình sau



Đường truyền vật lí

Chức năng của các tầng có thể mô tả vắn tắt như sau

1. Physical layer – Tầng Vật lí: Truy nhập đường truyền vật lí nhờ các phương tiện cơ, điện để truyền dòng bit không có cấu trúc – còn gọi là luồng bit thô.

2. Data link layer – Tầng Liên kết dữ liệu: Cung cấp phương tiện để truyền thông tin qua liên kết vật lí đảm bảo độ tin cậy. Gửi các khung dữ liệu (frame) với các cơ chế đồng bộ hóa, kiểm soát lỗi và kiểm soát luồng dữ liệu.

3. Network layer – Tầng Mạng: Chọn đường đi tối ưu cho gói dữ liệu, điều hòa luồng thông tin để tránh hiện tượng nghẽn mạch. Cắt và gộp các gói dữ liệu nếu cần.

4. Transport layer – Tầng Giao vận: Truyền dữ liệu giữa hai trạm, kiểm soát luồng dữ liệu và khôi phục lỗi. Thực hiện việc ghép hoặc phân kênh nếu cần.

mạch tổ hợp. So với chuẩn cũ, RS-423-A đạt tốc độ 3Kbps ở khoảng cách 1000 mét và 2 Mbps ở khoảng cách 60 mét.

- **Chuẩn X21**

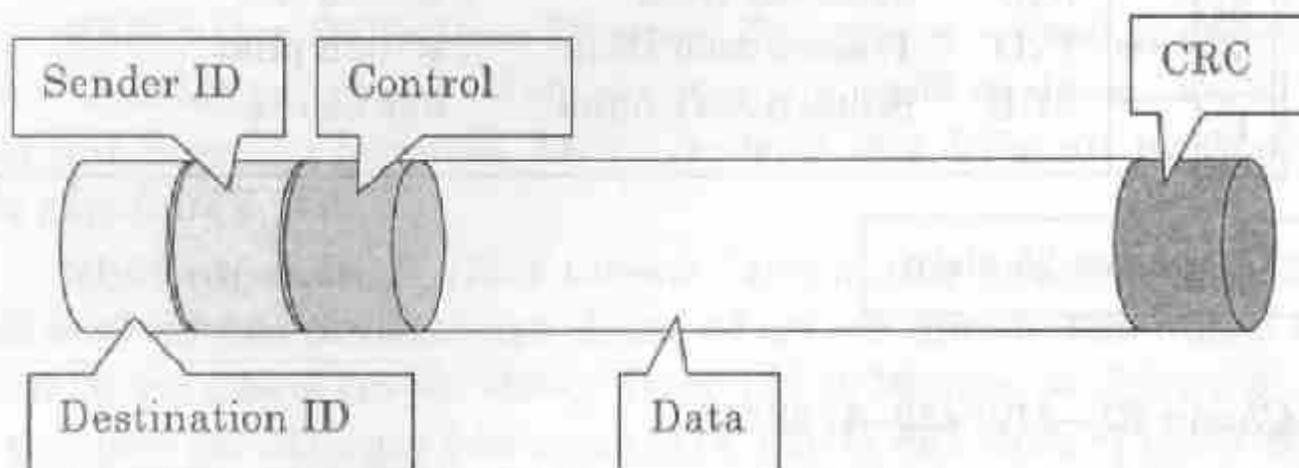
Phần cơ là một bộ nối 15 chân. Thuộc tính điện của X21 giống như chuẩn RS-422, mỗi mạch có hai đường dây, không dùng đất chung. Tốc độ đạt 100 Kbps – 10 Mbps với khoảng cách hàng kilômet.

1.5. Tầng Liên kết dữ liệu

Tầng Liên kết dữ liệu cung cấp các phương tiện để truyền dữ liệu qua đường truyền vật lí một cách đảm bảo tin cậy, không có lỗi thông qua các cơ chế đồng bộ hóa, kiểm soát lỗi và kiểm soát luồng dữ liệu. Tại đây dữ liệu được đóng gói thành các *frame* (khung dữ liệu – khung tin) để gửi xuống tầng Vật lí.

1.5.1. Cấu trúc của frame

Cấu trúc chung của một frame như sau



Sender ID: Địa chỉ máy tính gửi dữ liệu

Destination ID: Địa chỉ máy nhận

Control: Thông tin điều khiển cho biết về loại frame, đường đi và thông tin phân đoạn của frame (là frame thứ mấy trong chuỗi)

Data: Dữ liệu gốc

CRC: Cyclical Redundancy Checksum – Mã kiểm lỗi vòng: chứa những thông tin để phát hiện và sửa những bit lỗi gây ra bởi nhiễu trên đường truyền.

1.5.2. Tách khung tin, phát hiện và hiệu chỉnh lỗi

Để cung cấp dịch vụ cho tầng Mạng phía trên, tầng Liên kết dữ liệu phải sử dụng những dịch vụ do tầng Vật lý ở dưới cung cấp. Tầng Vật lý tiếp nhận các frame, chuyển thành dòng bit thô và truyền đi trên đường truyền. Dòng bit này không đảm bảo là không có lỗi – lỗi do đường truyền, do nhiễu từ ngoài xâm nhập – do đó tầng Liên kết dữ liệu phải kiểm tra và sửa những lỗi nếu có.

Tại trạm nhận, khi nhận được dòng bit chứa dữ liệu từ tầng Vật lý chuyển lên, tầng Liên kết dữ liệu phải tách thành các frame và kiểm tra để phát hiện lỗi trên từng frame. Việc tách frame được thực hiện theo một trong các phương pháp sau:

- Đếm số kí tự – hiện nay cũng ít dùng vì số đếm cũng có thể bị lỗi.
- Dùng kí tự bắt đầu (STX: Start of Text) và kí tự kết thúc (ETX: End of Text).
- Dùng cờ báo hiệu bắt đầu và cờ báo kết thúc.

Việc kiểm tra lỗi được thực hiện theo một trong các phương pháp sau:

- Dùng thông số trả lời có biên nhận ACK (Acknowledged) hoặc không biên nhận NAK (Non – Acknowledged) để biết frame đã được trạm đích nhận đúng hay có lỗi phải phát lại.
- Dùng đồng hồ báo, nếu quá thời gian quy định mà không có tín hiệu trả lời thì coi như trạm đích không nhận được và trạm phát sẽ phát lại frame.
- Đánh số những frame gửi đi. Việc này cũng cho phép nhận biết số thứ tự của frame và đảm bảo mỗi frame chỉ được nhận đúng một lần.

✶ Khi truyền tin trong hệ thống mạng, khả năng xảy ra lỗi do thiết bị trục trặc, do nhiễu bên ngoài là khá lớn. Do vậy các hệ thống mạng phải có cơ chế phát hiện và sửa lỗi. Việc phát hiện lỗi thì tương đối đơn giản song sửa lỗi thì khó hơn rất nhiều. Vì thế trong hai phương pháp xử lý lỗi sau đây thì phương pháp thứ nhất hiệu quả hơn do đó thường được áp dụng hơn.

- Phát hiện lỗi và thông báo cho trạm gửi biết để phát lại.
- Phát hiện lỗi và tự sửa.

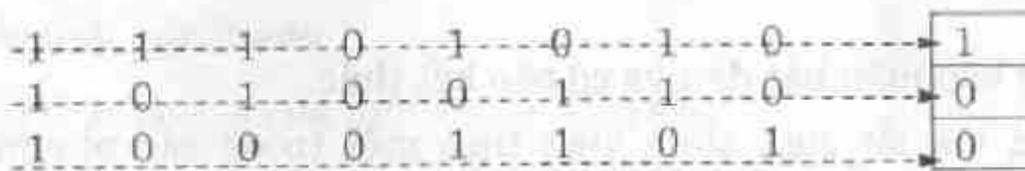
Sau đây là một số phương pháp phát hiện lỗi thông dụng:

1.5.3. Phương pháp Bit chẵn lẻ (Parity check)

Đây là phương pháp đơn giản nhất nhưng lại được áp dụng nhiều nhất để phát hiện lỗi. Một chuỗi bit dữ liệu – gọi là *chuỗi bit gốc* – được làm phép (XOR) với nhau cho một bit kết quả, bit này gọi là *bit chẵn lẻ* và nó sẽ được truyền đi cùng với chuỗi bit gốc. Tại trạm thu, phép tính trên được thực hiện lại với chuỗi bit nhận được để so sánh kết quả với bit chẵn lẻ, nếu có sự khác biệt tức là đã xảy ra lỗi. Sở dĩ gọi là bit chẵn lẻ vì nó phụ thuộc vào số lượng bit 1 trong chuỗi bit gốc, nếu số đó là chẵn thì bit chẵn lẻ có giá trị 0, lẻ thì bằng 1.

Có hai cơ chế áp dụng bit chẵn lẻ:

- Kiểm tra ngang (LRC– Longitudinal Redundancy Check): mỗi byte được tính kèm theo một bit chẵn lẻ để phát hiện lỗi, như vậy phải tốn thêm 1/8 = 12.5% dung lượng tin để truyền.



- Kiểm tra dọc (VRC–Vertical Redundancy Check): Lỗi được phát hiện trong từng khối byte thay vì trong từng byte. Người ta thêm vào mỗi khối byte một byte ở cuối, byte này cho phép phát hiện lỗi. Nó có thể được tính đơn giản bằng phép XOR tất cả các byte trong khối hoặc tính theo đa thức chuẩn như trình bày dưới đây.

Ví dụ: phối hợp cả hai phương pháp để truyền xâu kí tự 'ASCII'

	Khối kí tự cần truyền đi					LRC ↓
	A	S	C	I	I	
	1	1	1	1	1	1
	0	0	0	0	0	0
	0	1	0	0	0	1
	0	0	0	1	1	0
	0	0	0	0	0	0
	0	1	1	0	0	0
	1	1	1	1	1	1
VRC →	0	0	1	1	1	1

Nhắc lại rằng

' A ' = ASCII(65)=1000001

' C ' = ASCII(67)=1000011

' S ' = ASCII(83)=1010011

' I ' = ASCII(73)=1001001

1.5.4. Phương pháp Kiểm tra vòng (Cyclic Redundancy Check)

Phương pháp được đặt tên như vậy do nó được thực hiện bằng cách cho các bit đi qua một thanh ghi dịch chuyển vòng có chức năng của phép cộng môđun 2 \oplus . Nó còn được gọi là phương pháp mã đa thức vì có sử dụng khái niệm đa thức đại số.

Một xâu bit bất kì được xem như là một tập các hệ số 0 và 1 của một đa thức đại số. Nếu xâu bit gồm k bit thì đa thức tương ứng sẽ có bậc k - 1, gồm k số hạng từ x^0 đến x^k . Ví dụ: xâu bit 110001 tương đương với đa thức $x^5 + x^4 + 1$.

Để tìm tập bit cần chèn thêm vào (gọi là checksum), các bước tiến hành như sau:

- Chọn trước một đa thức, gọi là đa thức sinh (generator) $G(x)$ với hệ số cao nhất và thấp nhất đều bằng 1 (nghĩa là 2 bit đầu và cuối xâu bit tương ứng đều bằng 1). Gọi bậc của $G(x)$ là r còn xâu bit gốc tương ứng với đa thức $M(x)$ bậc m.

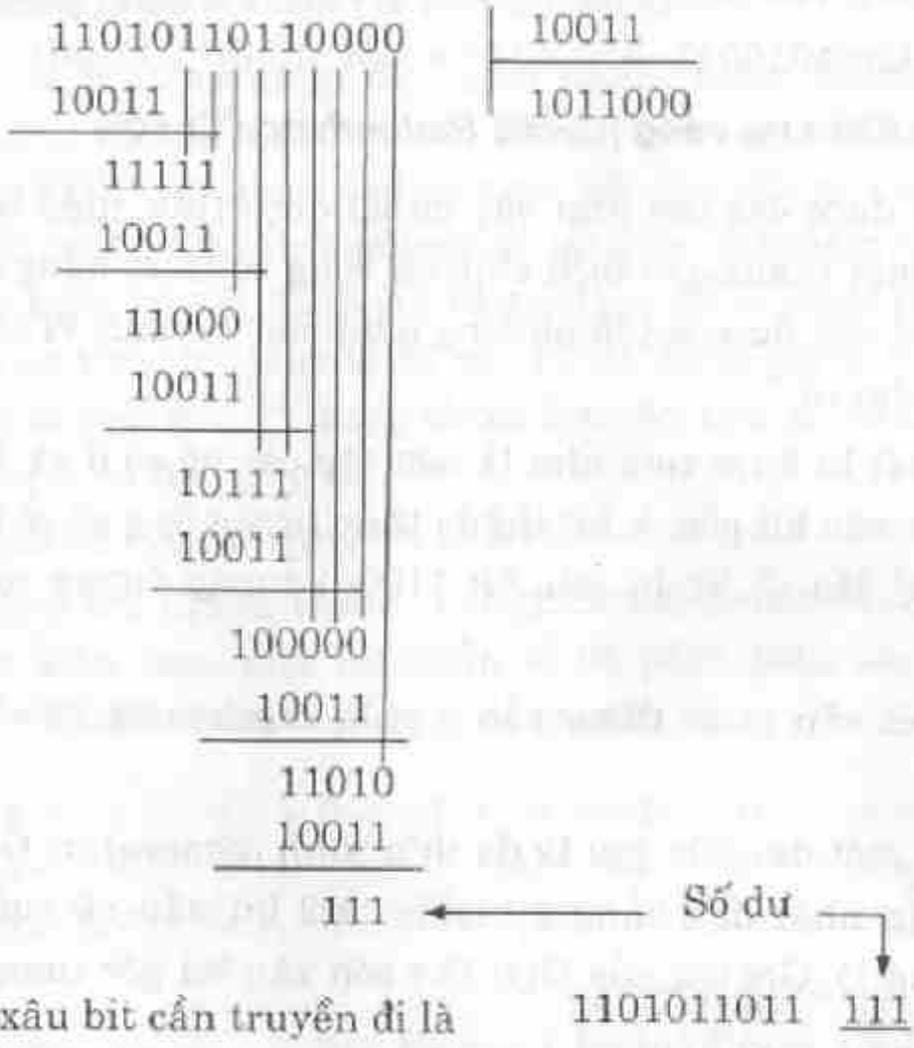
- Thêm r bit 0 vào cuối xâu gốc, xâu ghép có được sẽ tương đương với đa thức $x^r .M(x)$.

- Chia (môđun 2) xâu bit đó cho xâu bit của đa thức sinh $G(x)$. Ta chỉ quan tâm đến số dư của phép chia đó.

- Lấy xâu bit 'bị chia' trừ (môđun 2) đi xâu bit 'dư'. Kết quả chính là xâu bit cuối cùng sẽ được truyền đi (có chứa checksum), tương ứng với đa thức $T(x)$. Rõ ràng là $T(x)$ chia hết cho $G(x)$.

Ví dụ:

Giả sử xâu bit gốc là 1101011011 : $M(x) = x^9 + x^8 + x^6 + x^4 + x^3 + x + 1$



Xâu bit ứng với đa thức sinh (Generator): 10011 tức là $G(x) = x^4 + x + 1$

Thêm 4 bit 0 vào sau xâu bit gốc: 11010110110000

Làm phép chia (phép chia môđun 2 tương đương với phép EXCLUSIVE OR \oplus)

Độ tin cậy

Khi nhận, giả sử xâu bit nhận được đã bị sai lệch và tương đương với đa thức $V(x) = T(x) + E(x)$

Với $E(x)$ là đa thức xuất hiện do nhiễu truyền.

Chia (môđun 2) $V(x)$ cho $G(x)$

$$V(x)/G(x) = T(x)/G(x) + E(x)/G(x) = 0 + E(x)/G(x) = E(x)/G(x)$$

Như vậy nếu kết quả phép chia khác 0 thì có nghĩa là việc truyền tin đã bị lỗi. Nhưng ngược lại (kết quả phép chia = 0) cũng chưa đảm bảo chắc chắn là truyền đúng vì vẫn có thể $E(x)$ chia hết cho $G(x)$.

- *Trường hợp lỗi bit đơn:* chỉ có một bit bị lỗi. Giả sử bit lỗi ở vị trí i , tức là $E(x) = x^i$ ($i < m + r$). Nếu $G(x)$ chứa 2 hoặc nhiều số hạng thì $E(x)$

không thể chia hết cho $G(x)$ được, do đó tất cả các trường hợp lỗi bit đơn đều bị phát hiện.

• Trường hợp 2 lỗi bit đơn rời nhau: Giả sử 2 bit lỗi ở vị trí i, j tức là $E(x) = x^i + x^j = x^j(x^{i-j} + 1)$ với $i > j$. Để cho lỗi kép này bị phát hiện, ta phải chọn $G(x)$ sao cho $(x^k + 1)$ không thể chia hết cho nó với mọi k trong khoảng từ 1 tới $i - j$, tổng quát là tối độ dài cực đại của frame. Chẳng hạn như đa thức $x^{15} + x^{14} + 1$ không phải là ước của mọi đa thức dạng $(x^k + 1) \forall k \leq 32768$.

• Trường hợp $E(x)$ gồm một số lẻ số hạng, tức là số bit lỗi là lẻ: Chúng ta có thể chứng minh được mệnh đề sau: "trong hệ môđun 2, một đa thức với một số lẻ số hạng thì không thể chia hết cho $(x + 1)$ ".

Thật vậy, giả sử $E(x)$ có một số lẻ số hạng và $E(x) = (x + 1).Q(x)$

Suy ra $E(1) = (1 + 1) Q(1)$. Vì $1 + 1 = 0$ (môđun 2) $\Rightarrow E(1) = 0$ (tức là $E(1) = 0 \text{ mod } 2$)

Nhưng mặt khác vì $E(x)$ có một số lẻ số hạng, mỗi số hạng đều có dạng x^i nên khi thay x bằng 1 vào thì chúng đều bằng một. Tổng của một số lẻ giá trị 1 trong hệ môđun 2 thì bằng một (ví dụ: $E(x) = x^{15} + x^{14} + 1$ thì $E(1) = 1 + 1 + 1 = 1$). Đó là điều mâu thuẫn với kết luận lúc trước.

Từ mệnh đề đó, chúng ta chỉ cần chọn $G(x)$ sao cho nó chia hết cho $(x + 1)$. Đơn giản nhất có thể chọn $G(x) = x + 1$, lúc đó ta lại quay về phương pháp kiểm tra chẵn lẻ nêu trên.

• Trường hợp các bit lỗi đứng liền với nhau thành một nhóm, từ vị trí i tới vị trí $i + k$. Khi đó $E(x) = x^i.(x^k + \dots + 1)$, người ta đã chứng minh được rằng với đa thức sinh $G(x)$ bậc r thì mọi lỗi nhóm có độ dài bằng $r + 1$ đều có thể được phát hiện, trong khi các lỗi nhóm có độ dài $\geq r + 1$ vẫn có thể bị lọt lưới.

Hiện nay có 3 đa thức sinh được coi là chuẩn quốc tế, đó là:

CRC-12 = $x^{12} + x^{11} + x^3 + x^2 + x + 1$ dùng cho kí tự 6 bit

CRC-16 = $x^{16} + x^{15} + x^2 + 1$ dùng cho kí tự 8 bit

CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$ dùng cho kí tự 8 bit

Với CRC-16 và CRC-CCITT có thể phát hiện:

- Tất cả các lỗi đơn và kép
- Tất cả các lỗi có số bit lỗi lẻ
- Các lỗi nhóm có độ dài ≤ 16

- 99,997% các lỗi nhóm có độ dài 17 bit
- 99,998 % các lỗi nhóm có độ dài ≥ 18 bit

1.5.4. Phương pháp Mã sửa sai Hamming

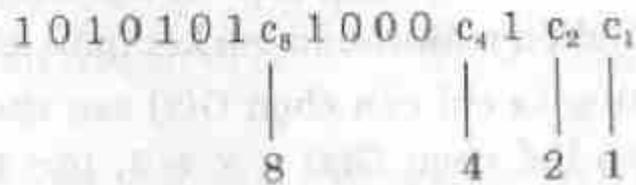
Ta làm như sau: rải đều các bit chẵn lẻ – là các bit được thêm vào chuỗi bit gốc để phát hiện lỗi – lẫn vào các bit dữ liệu theo nguyên lí cân bằng chẵn lẻ để cho chỉ ra vị trí bit lỗi. Nếu ta dùng r bit chẵn lẻ thì sẽ kiểm tra được $2^r - 1$ bit dữ liệu. Các vị trí chèn bit chẵn lẻ là các lũy thừa của 2 như: 1, 2, 4, 8 ... 2^{r-1} . Tổng số bit truyền đi là $r + n$.

Phương pháp này chỉ cho phép phát hiện và sửa được đúng một bit lỗi, có nghĩa là nếu có từ 2 bit lỗi trở lên thì cách làm này không áp dụng được.

Ví dụ:

Chuỗi bit gốc là 10101011001. Các bước thực hiện như sau:

- Chuỗi gốc có 11 bit \Rightarrow cần 4 bit chẵn lẻ gọi là c_8, c_4, c_2, c_1 để chèn vào các vị trí 8, 4, 2, 1



= Cộng môđun 2 tất cả các vị trí khác không trong chuỗi bit vừa thu được. Đó là các vị trí: 15, 13, 11, 9, 7, 3

15	=	1111	
13	=	1101	
11	=	1011	
9	=	1001	\oplus
7	=	0111	
3	=	0011	
		0100	= $c_8 c_4 c_2 c_1$

- Kết quả thu được cho ta giá trị của các bit chẵn lẻ tương ứng, $c_8 = 0, c_4 = 1, c_2 = c_1 = 0$

– Rải các bit chẵn lẻ vừa thu được vào đúng vị trí của chúng, ta có xâu bit truyền đi là 1010101001100.

– Giả sử trên đường truyền, bit thứ 13 bị lỗi. Khi đó giá trị của nó từ 1 bị đổi thành 0.

– Tại trạm thu, sẽ tiến hành lại thao tác cộng môđun 2 tất cả các vị trí khác không trong chuỗi bit vừa nhận được, đó là các vị trí 15, 11, 9, 7, 4, 3.

$$\begin{array}{r}
 15 = 1111 \\
 11 = 1011 \\
 9 = 1001 \quad \oplus \\
 7 = 0111 \\
 4 = 0100 \\
 3 = 0011 \\
 \hline
 1101 = 13
 \end{array}$$

Kết quả thu được 13 chính là vị trí bit lỗi.

1.5.6. Giao thức

Có rất nhiều giao thức được xây dựng cho tầng Liên kết dữ liệu, gọi tắt là DLP (Data Link Protocol). Có thể chia các DLP thành hai loại: DLP đồng bộ và DLP dị bộ. DLP đồng bộ gồm hai nhóm là các giao thức hướng bit (bit oriented) và các giao thức hướng kí tự (character oriented). Sau đây chúng ta sẽ xem xét từng loại DLP đã nêu

• *Các giao thức dị bộ*

Các giao thức này sử dụng phương pháp truyền dị bộ, trong đó sử dụng các kí hiệu đặc biệt START STOP để tách các xâu bit biểu diễn từng kí tự. Gọi là dị bộ vì chúng không cần có sự đồng bộ liên tục giữa bên phát và bên thu. Các giao thức này thường được dùng trong các máy tính, terminal tốc độ thấp.

• *Các giao thức đồng bộ*

Thay vì sử dụng những bit đặc biệt START, STOP để đánh dấu mỗi kí tự như giao thức dị bộ, các giao thức đồng bộ chèn các kí tự đặc biệt như SYN (synchronization), EOT (End Of Transmission) hay một cờ báo để báo cho trạm thu biết dữ liệu đang đến hay đã đến.

• Các giao thức hướng kí tự

Được xây dựng dựa trên một bộ kí tự chuẩn nào đó như ASCII hay EBCDIC, các giao thức hướng kí tự xuất hiện từ những năm 60 thế kỉ trước. Chúng có thể được sử dụng cho các phiên truyền Điểm nối Điểm (Point to Point) hay Phát rộng (multi Point), có thể dùng với các phương thức truyền Đơn công (Simplex), Song công (Full duplex) hay Bán song công (Half duplex). Sau đây chúng ta xem xét một giao thức hướng kí tự rất thông dụng của ISO có tên là Basic Mode dành cho phương thức truyền Bán song công.

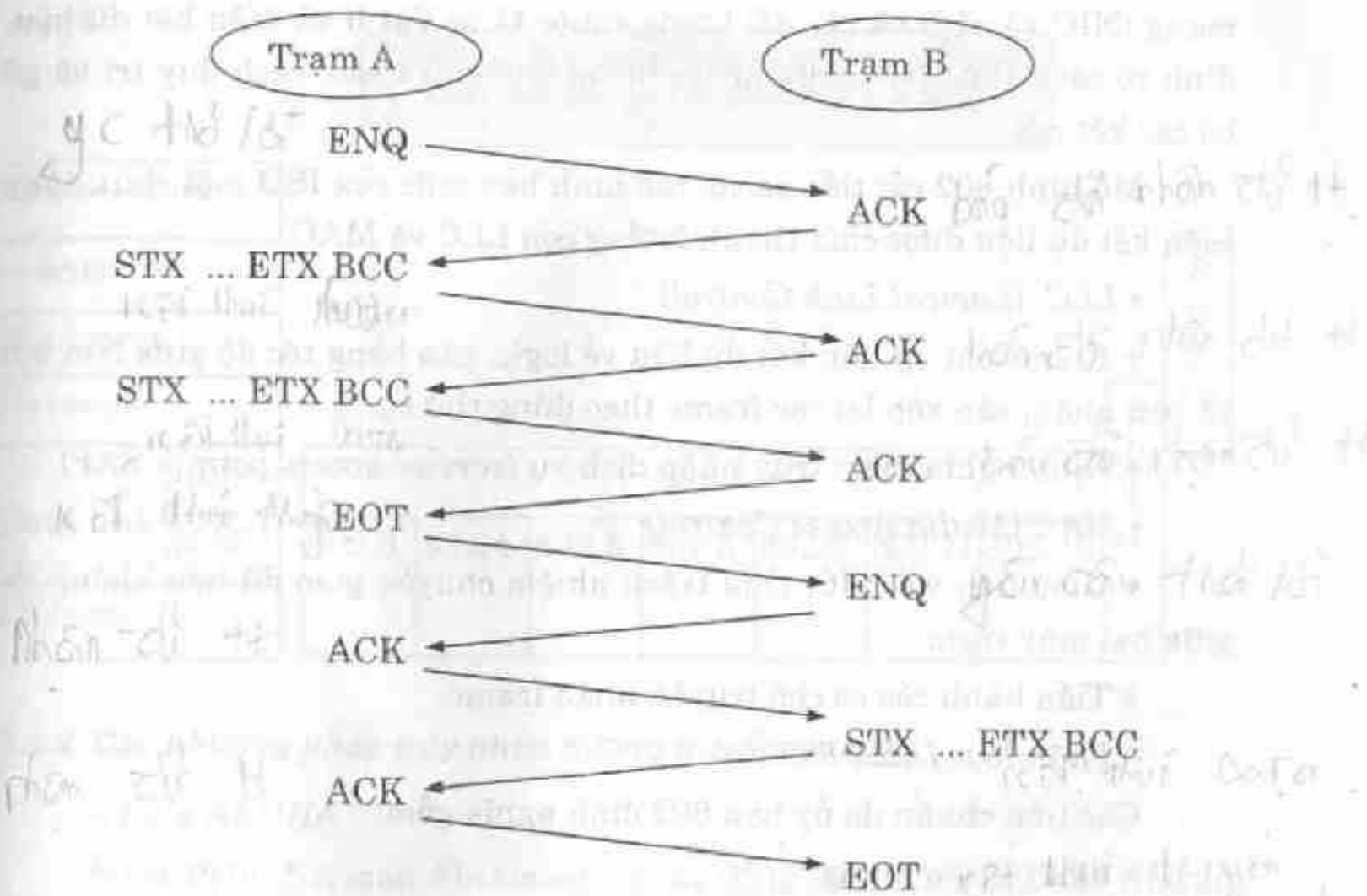
Các kí tự đặc biệt được giao thức Basic Mode sử dụng bao gồm:

- SOH (Start of Header): để chỉ nơi bắt đầu phần Header của một khung tin (frame).
- STX (Start of Text): để chỉ nơi kết thúc phần Header, bắt đầu phần Data.
- ETX (End of Text): chỉ nơi kết thúc phần Data.
- EOT (End of Transmission): báo hiệu kết thúc truyền, cắt đứt liên kết.
- ETB (End of Transmission Block): báo kết thúc truyền một khối. Dữ liệu có thể gồm nhiều khối.
- ENQ (Enquiry): yêu cầu trạm bên kia trả lời.
- DLE (Data Link Escape): thay đổi ý nghĩa các kí tự điều khiển truyền tin.
- ACK (Acknowledge): báo cho trạm phát rằng đã nhận đủ thông tin.
- NAK (Negative Acknowledge): báo cho trạm phát rằng việc nhận đã xảy ra lỗi.
- SYN (Synchronous Idle): tín hiệu đồng bộ, dùng để duy trì sự đồng bộ giữa trạm thu và trạm phát.

Theo quy định của Basic Mode, khung tin có cấu trúc như sau:

SYN	SYN	SOH	Header	STX	Data	ETX	BCC
-----	-----	-----	--------	-----	------	-----	-----

Trong đó SOH là kí tự khởi đầu phần header. Đây là phần chứa những thông tin điều khiển như số thứ tự của frame, địa chỉ trạm đích, ... BCC (Block Check Character) là 8 bit phát hiện lỗi được thành lập theo phương pháp Chẵn lẻ theo chiều dọc VRC để kiểm soát lỗi cho vùng Data.



- Các giao thức hướng bit

Tiêu biểu cho loại này là giao thức HDLC (High-level Data Link Control), được ISO xây dựng và có tên gọi là ISO 3309 và ISO 4335. Giao thức này sử dụng cho các phiên truyền Điểm nối Điểm hay Phát rộng. Các phần tử của nó được xây dựng từ các cấu trúc nhị phân và dữ liệu được tiếp nhận theo từng bit một.

1.5.7. Tầng con LLC và MAC

- Bộ tiêu chuẩn IEEE 802

Vào cuối những năm 1970, khi LAN bắt đầu phát triển mạnh, IEEE nhận thấy nhu cầu phải định nghĩa các tiêu chuẩn cho LAN. Nhằm mục đích đó, IEEE đã đề ra mô hình 802, đặt tên theo thời điểm bắt đầu công việc nghiên cứu là tháng 2/1980. Sau đó bộ tiêu chuẩn này được ISO công nhận, lấy làm chuẩn của mình và đặt tên là ISO 8802.

Mô hình 802 định nghĩa các tiêu chuẩn cho các thành phần vật lí của

mạng (NIC và cáp) và các đối tượng thuộc tầng Vật lý và Liên kết dữ liệu, định rõ cách thức NIC truy nhập đường truyền ra sao, cách duy trì và gỡ bỏ các kết nối.

Mô hình 802 cải tiến so với mô hình bảy mức của ISO một chút, tầng Liên kết dữ liệu được chia thành 2 tầng con LLC và MAC.

- *LLC: (Logical Link Control)*

- + Kiểm soát sự liên kết dữ liệu về logic, cân bằng tốc độ giữa bên gửi và bên nhận, sắp xếp lại các frame theo đúng thứ tự.

- + Định nghĩa điểm truy nhập dịch vụ (service access point – SAP)

- *MAC (Media Access Control)*

- + Giao tiếp với NIC, chịu trách nhiệm chuyển giao dữ liệu không lỗi giữa hai máy trạm.

- + Tiến hành các cơ chế truyền nhận frame.

- *Phân loại IEEE 802*

Các tiêu chuẩn do ủy ban 802 định nghĩa gồm:

- + 802.1: Liên mạng

- + 802.2: Tầng LLC

- + 802.3: Mạng Ethernet

- + 802.4: Mạng Token Bus

- + 802.5: Mạng Token Ring

- + 802.6: Mạng MAN

- + 802.7: Kỹ thuật băng tần rộng (broadband)

- + 802.8: Cáp quang

- + 802.9: Mạng tiếng nói (voice/data network)

- + 802.10: An toàn trên mạng (network security)

- + 802.11: Mạng vô tuyến

- + 802.12: 100 Base VG–Any LAN

Trong đó: nhóm 802.1 và 802.2 liên quan đến tầng LLC, còn 802.3, 802.4, 802.5 quy định các giao thức thuộc tầng MAC và Vật lý.

So sánh chức năng các tầng của mô hình OSI với các phân mục Project 802

Presentation									8 0 2. 10
→Session									
Transport									
Network									8 0 2. 1
Data link	LLC	802.2							
	MAC	802.3	802.4	802.5	802.6	802.9	802.11	802.12	
Physical									

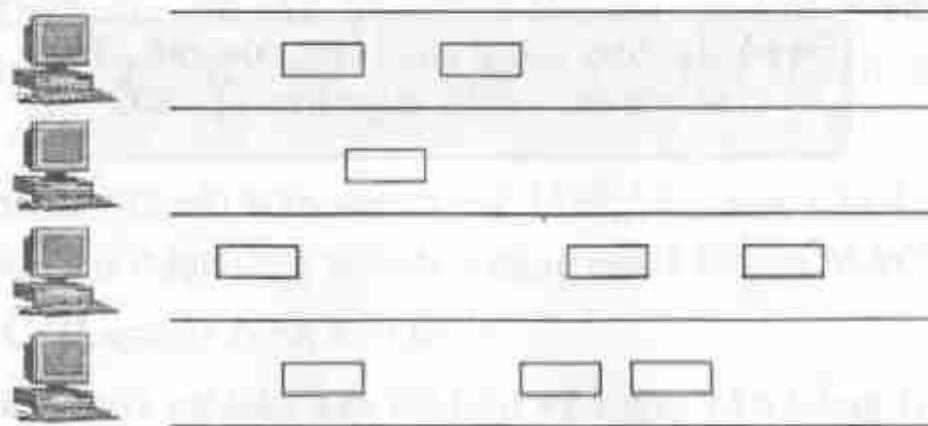
1.5.8. Các phương pháp truy nhập đường truyền chung

– Pure ALOHA

Năm 1970, Norman Abramson và các đồng sự trường Đại học Hawaii đã đề xuất một phương pháp chia sẻ kênh chung gọi là ALOHA cho phép nhiều trạm cùng tham gia truyền thông trên một kênh đơn duy nhất. Để phân biệt với những phiên bản cải tiến sau này, ALOHA đầu tiên của Abramson còn được gọi là ALOHA chuẩn – Pure ALOHA.

Ý tưởng của Pure ALOHA rất đơn giản. Bất cứ trạm nào có nhu cầu đều được gửi ngay dữ liệu lên mạng. Như vậy ắt xảy ra đụng độ giữa các gói tin và chúng bị hủy, nhưng nhờ có tín hiệu phản hồi mà các trạm có thể biết chính xác những gói tin nào gửi đi đã bị va chạm. Chú ý rằng trên mạng LAN thông tin phản hồi đến tức thì nhưng trên mạng WAN sử dụng vệ tinh nó phải mất 270ms mới tới được trạm phát.

Khi biết được gói tin gửi đi không thành công, trạm phát sẽ đợi một khoảng thời gian ngẫu nhiên rồi phát lại. Do vậy thời điểm phát của các trạm là hoàn toàn tùy ý



Chúng ta cùng xem xét hiệu suất truyền của Pure ALOHA. Gọi thời gian cần thiết để truyền một gói tin là T . Giả sử trong khoảng thời gian T những người sử dụng tạo ra trung bình S gói dữ liệu mới. Cũng giả thiết rằng trong khoảng thời gian T đó, các trạm phải truyền đi trung bình là G gói tin. Trong số này có S gói mới phát sinh và $G-S$ gói cũ phải truyền lại, do đó $G \geq S$.

Trong trường hợp đường truyền rảnh rỗi tức là $S \approx 0$, va chạm hầu như không xảy ra và ta có $G \approx S$.

Tổng quát ta có số gói tin được truyền thành công là $K = G.P_0$ với P_0 là xác suất một gói truyền thành công. Người ta đã chứng minh được rằng* trong mạng Pure ALOHA xác suất truyền thành công là:

$$K = G.e^{-2G}$$

Tính ra, K đạt giá trị cực đại là $\frac{1}{2e} \approx 0,184$ tại $G = 0,5$, có nghĩa là tỉ lệ truyền thành công tối đa của mạng Pure ALOHA là khoảng 18%, một tỉ lệ tương đối thấp.

- Slotted ALOHA

Năm 1972, Roberts công bố một phương pháp mới cho phép tăng gấp đôi hiệu năng của ALOHA, có tên là Slotted ALOHA. Ý tưởng cơ bản của phương pháp này là chia đồng thời gian thành những đoạn rời rạc gọi là slot, mỗi slot có chiều dài đúng bằng T – thời gian cần để truyền một gói tin. Các trạm không được phát tin bất cứ lúc nào mà chỉ được phát vào thời điểm đầu mỗi slot mà thôi.

Tại sao làm như vậy lại tăng gấp đôi hiệu năng truyền của hệ thống

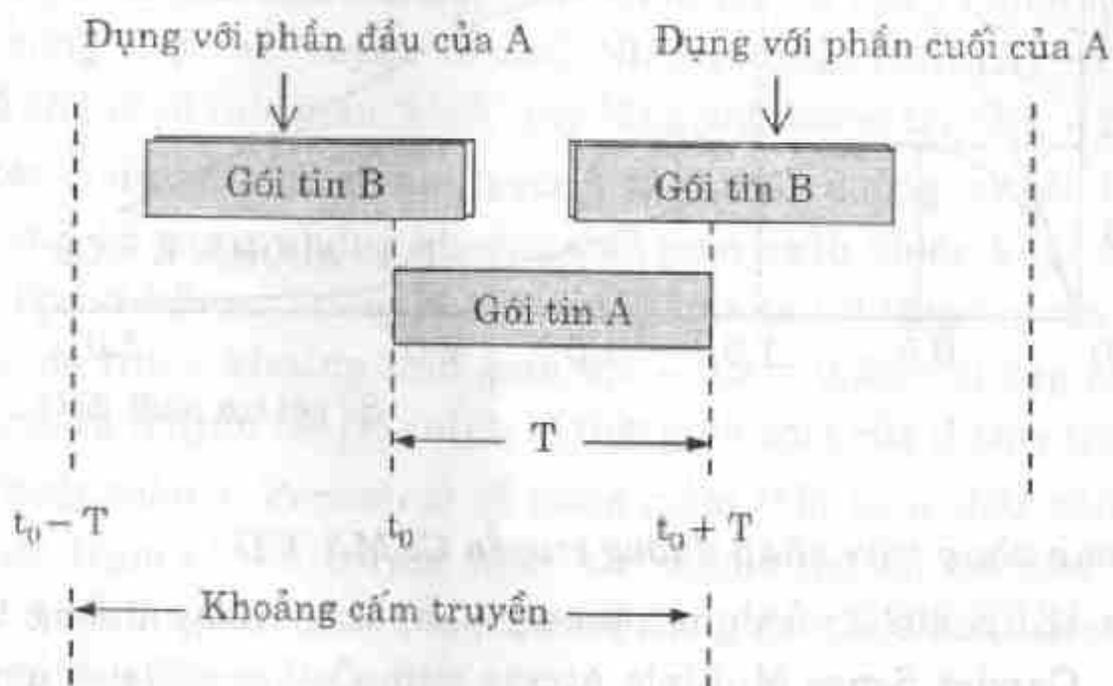
* Với giả thiết S và G tuân theo phân phối Poisson

ALOHA? Để trả lời câu hỏi này trước hết chúng ta quay lại tìm hiểu xem trên mạng Pure ALOHA một gói tin bị va chạm trong điều kiện như thế nào.

Xét một gói tin A được phát đi tại thời điểm t_0 . Nếu an toàn nó sẽ đến đích tại thời điểm $t_0 + T$. Rõ ràng là trong khi A chưa đến đích, tức là trong khoảng từ t_0 đến $t_0 + T$, nếu có một gói tin thứ hai B cũng được phát đi thì A và B sẽ đụng độ nhau, những byte cuối của A sẽ đụng với những byte đầu của B.

Một nguyên nhân thứ hai dẫn đến va chạm là trong khoảng thời gian T trước khi A được phát, nghĩa là từ thời điểm $t_0 - T$ đến t_0 , nếu có một gói B nào đó được phát đi thì B sẽ va chạm với A, chính xác là với những bit đầu tiên của A.

Vậy trong khoảng thời gian $2T$, từ thời điểm $t_0 - T$ đến $t_0 + T$, nếu có một gói tin thứ hai được phát thì nó sẽ đụng độ với A. Khoảng thời gian $2T$ này được gọi là khoảng cấm truyền (vulnerable period).



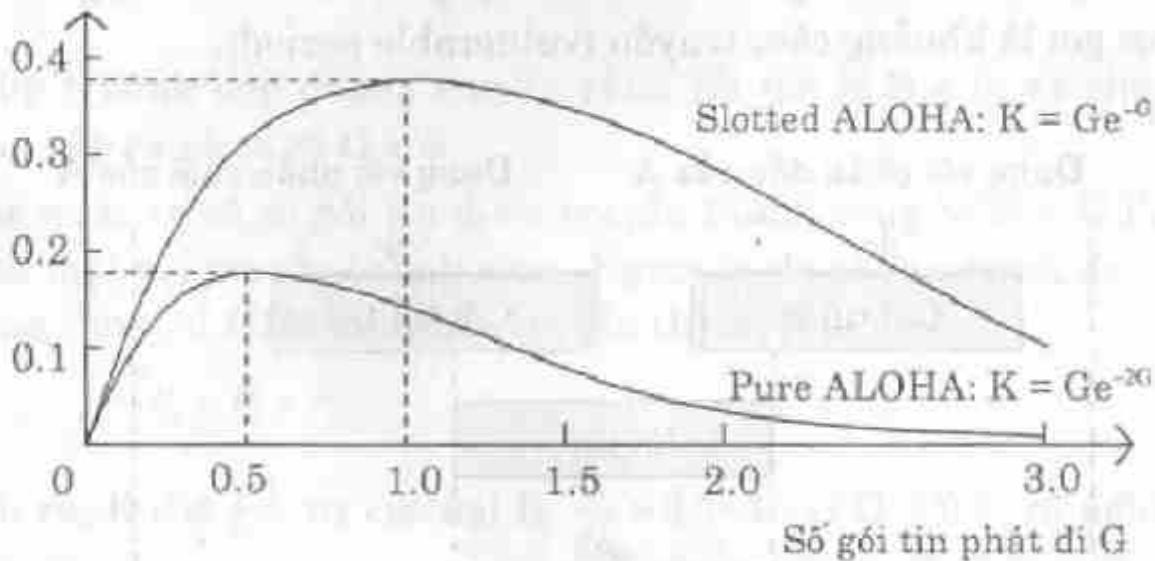
Quay lại xét hệ thống Slotted ALOHA. Vì dòng thời gian đã được chia thành những slot rời rạc nên chỉ những gói tin được phát trong khoảng từ t_0 đến $t_0 + T$, nghĩa là trong cùng một slot như A mới bị va chạm với A (thực ra chúng đều được phát vào thời điểm t_0). Những gói tin phát trong khoảng thời gian T trước khi A được phát, nghĩa là từ thời điểm $t_0 - T$ đến t_0 , thuộc về slot trước và chúng đến đích trước khi A bắt đầu

phát, vì chúng được phát chính xác vào thời điểm $t_0 - T$, nên không đụng độ gì với A. Do đó rõ ràng xác suất va chạm giảm còn một nửa.

$$K = G \cdot e^{-G}$$

Hình vẽ dưới đây chỉ rõ, slotted ALOHA cho hiệu suất truyền cực đại $K = \frac{1}{e} \approx 0,368$ khi $G = 1$. Tại giá trị này của G , người ta tính ra được xác suất khiến slot bị bỏ trống – không có gói nào được truyền trong slot đó – cũng là 0,368. Như vậy trong trường hợp tốt nhất, cơ chế slotted ALOHA sẽ bỏ trống 37% số slot, truyền thành công 37% và 26% còn lại là xảy ra đụng độ.

Xác suất thành công K



- Phương pháp truy nhập đường truyền CSMA/CD

Chuẩn IEEE 802.3 sử dụng phương pháp truy nhập đường truyền CSMA/CD: Carrier Sense Multiple Access with Collision Detection – Đa truy nhập sử dụng sóng mang có phát hiện xung đột.

Phương pháp này được sử dụng cho các giao thức mạng – chẳng hạn như kiểu tuyến tính – mà trong đó các trạm của mạng cùng nối vào và chia sẻ đường truyền chung, do đó rất dễ xảy ra hiện tượng xung đột là hiện tượng xảy ra khi hai hay nhiều trạm đồng thời gửi các gói tin của mình lên đường truyền, chúng va chạm nhau và cùng bị hủy.

CSMA/CD được cải tiến từ phương pháp CSMA- hay còn gọi là LBT

(Listen Before Talk – Nghe trước khi nói). Cơ chế CSMA như sau: một trạm cần truyền dữ liệu trước hết phải "nghe" xem đường truyền đang rỗi hay bận. Nếu đường truyền đang rỗi thì gửi dữ liệu đi, ngược lại đang bận thì trạm thực hiện theo một trong ba thuật toán sau:

- Non Persistent – Thiếu kiên nhẫn. Trạm tạm thời rút lui chờ đợi trong một khoảng thời gian ngẫu nhiên nào đó rồi lại tiếp tục lắng nghe đường truyền.

- p-Persistent – Trạm tiếp tục lắng nghe cho đến khi đường truyền rỗi thì gửi dữ liệu đi với xác suất bằng p xác định từ trước. Ví dụ như $p = 0.05$ tức là trong 100 lần trạm phát hiện đường truyền không bận thì chỉ có 5 lần trạm gửi dữ liệu đi.

- 1-Persistent – Trạm tiếp tục lắng nghe cho đến khi đường truyền rỗi thì gửi dữ liệu đi với xác suất bằng 1 (luôn luôn gửi đi).

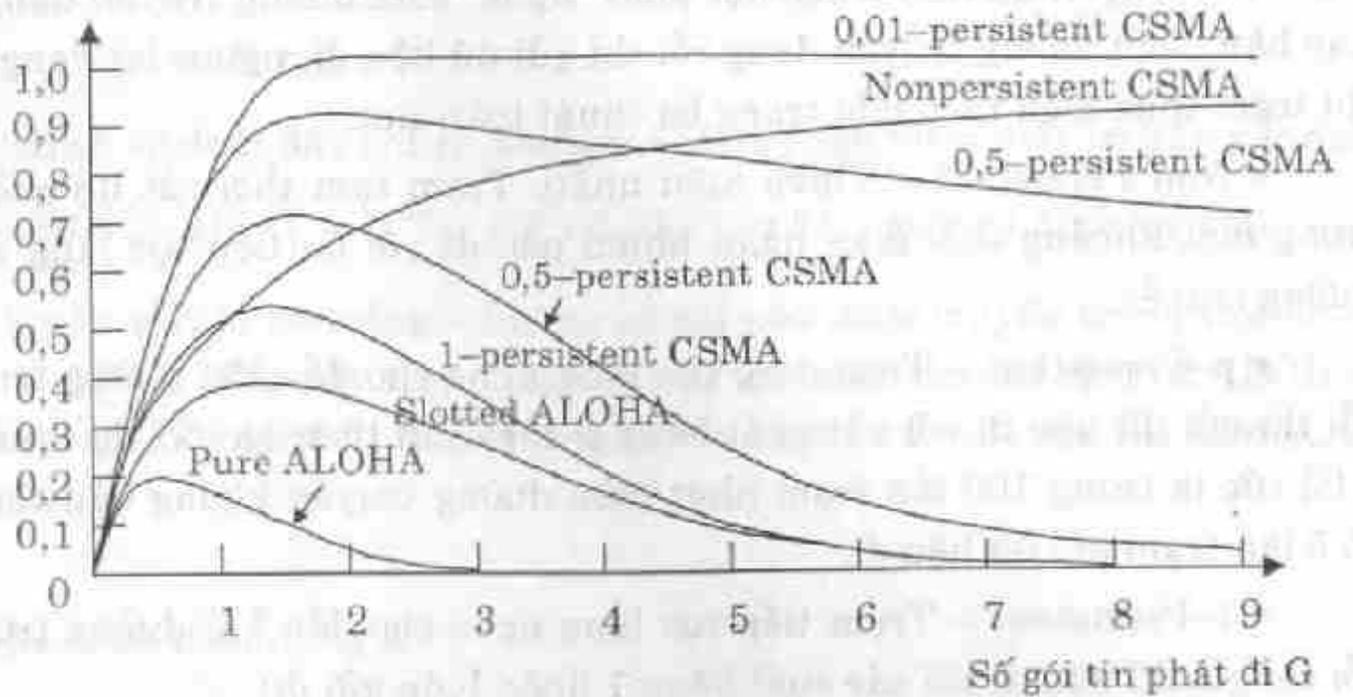
Rõ ràng là thuật toán đầu tiên có hiệu quả trong việc tránh xung đột vì khoảng thời gian mà các trạm rút lui để chờ là ngẫu nhiên nên xác suất chúng cùng tiếp tục truyền là nhỏ. Nhưng thuật toán này có một nhược điểm là có thể có thời gian "chết" gây lãng phí đường truyền.

Xét ví dụ sau: giả sử hai trạm A và B thấy đường truyền bận sẽ cùng rút lui chờ đợi trong những khoảng thời gian ngẫu nhiên khác nhau, A chờ 0,7ms, B chờ 0,5ms. Trong khi đó chỉ 0,2ms sau đường truyền đã trở nên rỗi. Khi đó trong khoảng thời gian $0,5 - 0,2 = 0,3$ ms không có trạm nào lắng nghe và truyền cả. Đó chính là thời gian chết của đường truyền.

Thuật toán 1-Persistent cố gắng giảm thời gian chết bằng cách cho phép một trạm có thể truyền ngay khi đường truyền trở nên rỗi. Nhưng nếu lúc đó có hai hay nhiều trạm cùng đang đợi thì chúng sẽ cùng gửi gói tin đi dẫn đến xảy ra xung đột.

Thuật toán p-Persistent với giá trị p được lựa chọn một cách hợp lý có thể tối thiểu hóa khả năng xảy ra xung đột đồng thời giảm tối đa thời gian chết của đường truyền.

Xác suất thành công K



Thực ra không bao giờ có hai trạm cùng bắt đầu truyền chính xác tại một thời điểm mà luôn chênh lệch ít nhiều. Nguyên nhân xảy ra xung đột là do độ trễ truyền dẫn. Đó là khi một trạm đã truyền dữ liệu cùng sóng mang đi rồi nhưng do độ trễ truyền dẫn nên một trạm khác lúc đó đang lắng nghe vẫn tưởng là đường truyền rỗng mà truyền dữ liệu đi, do đó xảy ra xung đột. Điểm mấu chốt của vấn đề là ở chỗ các trạm chỉ "lắng nghe trước khi nói" mà không "lắng nghe trong khi nói" nên sau khi đã bắt đầu phát tin mà có xảy ra va chạm trên đường truyền thì các trạm cũng không hay biết, vẫn tiếp tục truyền gây ra việc chiếm dụng đường truyền một cách vô ích.

Để khắc phục nhược điểm đó, CSMA/CD (còn gọi là LWT-Listen While Talk: nghe trong khi nói) đã bổ sung thêm một số quy tắc:

- Sau khi bắt đầu truyền, trạm vẫn tiếp tục lắng nghe đường truyền. Nếu phát hiện thấy có xung đột thì ngừng ngay việc phát dữ liệu nhưng vẫn tiếp tục gửi tín hiệu thêm một thời gian nữa để báo động cho các trạm khác về xung đột đã xảy ra.

- Sau đó trạm chờ đợi theo một trong ba thuật toán "kiên nhẫn" nói trên. Thông thường thuật toán 1-persistent hay được dùng hơn cả.

- Sau khi đã chờ một khoảng thời gian ngẫu nhiên rồi truyền lại mà vẫn xảy ra đụng độ thì trạm sẽ xử lý theo thuật toán "Backoff lũy thừa 2" như sau.

Thời gian được chia thành các khoảng nhỏ gọi là lát cắt (slot time) có độ dài bằng khoảng thời gian đủ để tín hiệu truyền tới đầu cáp xa nhất và quay trở về (bằng 2τ như giải thích trong mục 5.9 về Ethernet). Với các giới hạn của Ethernet chuẩn (băng thông 10 Mbps, độ dài cáp xa nhất 2.5 kilômet) thì thời gian đó bằng khoảng $51.2\mu s$.

Sau lần đụng độ thứ nhất, mỗi trạm sẽ chờ 0 hoặc 1 slot trước khi bắt đầu phát lại. Nếu lại có đụng độ lần thứ hai thì mỗi trạm sẽ lấy ngẫu nhiên 0 hoặc 1, 2, 3 slot làm thời gian chờ của mình trước khi bắt đầu lại. Nếu lại đụng độ lần thứ ba (xác suất xảy ra chuyện này = 0,25) thì số slot chờ sẽ được lấy ngẫu nhiên trong khoảng từ 0 đến $2^3 - 1 = 7$.

Tổng quát, sau khi xảy ra đụng độ i lần liên tiếp ($i < 16$) thì số slot chờ sẽ được lấy ngẫu nhiên trong khoảng từ 0 đến $2^i - 1$. Nhưng nếu đụng độ liên tiếp bộ điều khiển sẽ đầu hàng và lỗi được chuyển lên cho tầng trên xử lý.

1.5.9. Ethernet

Lược sử

Vào cuối những năm 60 thế kỉ trước, trường Đại học Hawaii đã xây dựng một mạng diện rộng kết nối các máy tính trong phạm vi của trường và đặt tên là ALOHA. Một trong những đặc điểm của mạng là sử dụng CSMA/CD làm phương pháp truy nhập đường truyền.

Năm 1972, tại Trung tâm nghiên cứu Palo Alto, Robert Metcalfe và David Boggs đứng đầu một nhóm trong Xerox đã xây dựng sơ đồ cáp và lược đồ truyền tín hiệu cho một mạng LAN dựa trên cơ chế cảm nhận sóng mang (CSMA) dài 1km với 100 trạm làm việc, tốc độ truyền 2.49Mbps. Mạng đó được đặt tên là Ethernet, hoàn thành vào ngày 27/5/1973 (Metcalfe sau khi rời Xerox đã lập ra 3COM).

Ethernet được tập đoàn các công ti: DEC, Intel, Xerox đặt thành một chuẩn của mình với tên gọi là DIX (lấy chữ cái đầu tên ba công ti trên).



Năm 1982 DIX version 2.0 ra đời và còn được gọi là Ethenet II. Khi IEEE tiến hành chuẩn hoá LAN, ba công ti trên tiến cử Ethernet như một chuẩn. Đồng thời IBM, dựa trên một mẫu thử nghiệm tại Zurich, cũng đề nghị một chuẩn là Token Ring. Sau này Ethernet trở thành 802.3 và Token Ring trở thành 802.5 trong họ chuẩn của IEEE. Mặc dù chuẩn IEEE 802.3 không hoàn toàn giống với nguyên mẫu Ethernet lúc đầu, nhưng đến nay thuật ngữ Ethernet vẫn được dùng để gọi IEEE 802.3 và những LAN tuân theo IEEE 802.3

Các đặc tính của Ethernet

- Cấu hình truyền thống: bus tuyến tính
- Cấu hình khác: star-bus
- Kiến trúc: based band (băng tần cơ sở – dải gốc)
- Phương pháp truy nhập đường truyền: CSMA/CD
- Thông lượng:
10Mbps /100 Mbps
- Loại cáp: cáp đồng trục (béo/gầy), cáp xoắn (UTP/STP)

frame IEEE 802.3

frame Ethernet II

So sánh khuôn dạng frame IEEE 802.3 và Ethernet II

Như trên đã trình bày, IEEE đã chọn Ethernet II làm chuẩn của mình nhưng cũng tiến hành sửa lại một phần nhỏ. Sau đây là sự khác biệt về khuôn dạng khung tin giữa hai chuẩn này.

Cả 2 frame đều có kích thước tối thiểu là 64 byte, tối đa là 1518 byte.

Frame IEEE 802.3:

- Preamble: phần mở đầu 8 byte gồm toàn các bit 0,1 xen kẽ, kết thúc bằng

Preamble 8B
Destination Address 6B
Source Address 6B
Type 2B
Data 46-1500B
CRC 4B

Preamble 7B
SFD 1B
Destination Address 2/6B
Source Address 2/6B
Length 2B
LLC Data 0-1500B
Pad 0-46B
CRC 4B

10101011. Ở tốc độ 10Mbps phần này tương ứng với thời gian truyền 6.4ms, đủ để hai trạm nhận và gửi đồng bộ hóa với nhau.

- Des Add 6 byte, trong đó 3 byte đầu là mã của nhà sản xuất do IEEE cấp cho, 3 byte sau là mã của từng thiết bị (3 byte đủ để phân biệt hơn 16 triệu chiếc). Có ba loại địa chỉ:

- + Unique Add: địa chỉ MAC của một nút nhất định.
- + Multicast Add: địa chỉ MAC của một nhóm nút.
- + Broadcast Add: gửi cho tất cả mọi nút trên mạng.

Khi đó Des Add = FF FF FF FF FF FF. Bit đầu tiên (LSB – Least Significant Bit) = 0: Unique / 1: Multicast

- Type: loại dữ liệu, cho biết giao thức của lớp trên, chẳng hạn như

8137H: frame IPX (netware)

0800H: frame IP (internet)

0600H: frame của mạng 3COM

.....

Trên mạng IEEE 802.3, cơ chế nhận dữ liệu do trạm nhận tiến hành diễn ra theo các bước sau:

- Kiểm tra độ dài frame, nếu độ dài nhỏ hơn 64 byte thì coi là không hợp lệ và bỏ qua.

- Kiểm tra Des Add và đối chiếu với địa chỉ của mình.

- Tính lại mã CRC từ tất cả các phần trừ Preamble và so sánh với CRC.

- Kiểm tra độ dài frame, nếu lớn hơn 1518 byte thì bỏ qua

- Tách lấy Data và gửi lên tầng trên.

Frame Ethernet II:

- SFD (Start Frame Delimiter: báo hiệu khởi đầu frame, là 8 bit 10101011). Chú ý: preamble 802.3 + SFD = preamble Ethernet II

- Length: độ dài của phần LLC Data. Thông tin về tipe do các tầng trên cung cấp.

- PAD: các bit đệm thêm vào để đạt kích thước tối thiểu 64 byte.

Ta thấy rằng cả IEEE 802.3 và Ethernet II đều quy định kích thước frame hợp lệ phải lớn hơn 64 byte. Tại sao vậy? Chúng ta hãy xét tình huống sau:



Thời điểm xuất phát: 0



Xảy ra đụng độ: $\tau - \epsilon$
 ϵ rất bé so với τ



Tiếng nổ vọng về tới A: 2τ

Giả sử trên mạng có hai trạm A và B truyền tin với nhau. Trạm A gửi một frame X tới trạm B ở đầu kia của cáp. Gọi thời gian frame đi từ A tới B là τ . Ngay trước khi tới B, tại thời điểm $\tau - \epsilon$, thì trạm B cũng bắt đầu phát đi một frame. Tất nhiên hai frame va chạm nhau và cùng bị hủy. B phát hiện ra đụng độ giữa hai frame vào thời điểm τ khi nó nhận thấy cường độ sóng mang tăng lên đột ngột. B lập tức ngừng phát frame và gửi đi một gói tin 48 bit (gọi là 'tiếng nổ') để báo động cho toàn mạng về đụng độ đó. Tiếng nổ vọng về tới A tại thời điểm 2τ . Nếu như vào lúc đó A vẫn còn đang phát frame X thì nó biết rằng X đã bị va chạm và sẽ rút lui, nghe ngóng đường truyền để phát lại X vào lúc khác. Nhưng nếu như lúc đó A đã phát xong X, tức là tổng thời gian để phát X là nhỏ hơn 2τ thì khi nhận được tiếng nổ, A đã phát xong và coi như X không gặp sự cố gì trong khi thực tế là X đã bị đụng độ và phá hủy.

Để tránh tình trạng trên, mọi frame phải đủ dài để thời gian phát $\geq 2\tau$. Đối với mạng LAN Ethernet 802.3 chuẩn 10 Mbps, tổng chiều dài không vượt quá 2500 mét với 4 repeater thì giá trị 2τ là 51.2ms, tương đương với chiều dài frame là 64 byte.

Ta thấy rằng, với sự phát triển của mạng hiện nay, thông lượng ngày càng tăng, tốc độ phát ngày càng nhanh thì để tránh sai sót trên, độ dài tối thiểu của frame phải tăng theo hoặc độ dài cáp cực đại phải giảm xuống để tiếng nổ kịp vọng về trước khi phát xong frame. Với LAN 2500m, thông lượng 1 Gbps thì độ dài tối thiểu của frame phải là 6400 byte, còn nếu là 640 byte thì cáp không vượt quá 250 mét.

1.6. Tầng Mạng

Chức năng của tầng mạng là:

- Chọn đường đi tốt nhất để phát các gói tin lên mạng.
- Điều phối đường truyền, tránh quá tải, đồng thời tận dụng tối đa công suất đường truyền.
- Chia cắt hay tổ hợp dữ liệu. Dồn kênh và phân kênh.

1.6.1. Chọn đường

Chức năng quan trọng nhất của tầng Mạng là *chọn đường* (routing). Đó là tìm kiếm, lựa chọn một con đường tốt nhất để truyền một *datagram* (tên đơn vị dữ liệu trên tầng mạng) từ trạm phát tới trạm thu. Một kĩ thuật chọn đường phải thực hiện được hai công việc sau:



- Tìm đường đi tốt nhất cho gói tin.
- Cập nhật liên tục những thông tin dùng để chọn đường như: khoảng cách giữa các trạm, vị trí những trạm mới xuất hiện, tình trạng tắc nghẽn hay thông suốt của các tuyến đường hiện thời...

Việc định nghĩa thế nào là một đường truyền tốt nhất cũng không phải là bất biến mà có thể do người quản trị mạng, người thiết kế mạng đặt ra. Các tiêu chuẩn để đánh giá đường truyền thường là:

- Chi phí truyền.
- Thời gian truyền.
- Độ an toàn, chắc chắn của mạng truyền thông.

.....

Hiện nay có rất nhiều kĩ thuật chọn đường khác nhau. Có thể phân loại chúng dựa trên các yếu tố sau:

- Việc chọn đường do tất cả các trạm tự làm – kĩ thuật chọn đường phân tán – hay chỉ do một số trung tâm điều khiển mạng đảm nhiệm – kĩ thuật chọn đường tập trung.
- Việc tìm đường có lưu ý đến những thay đổi, biến động của các tuyến đường hay không. Nói cách khác, việc chọn đường có được điều chỉnh liên tục để thích nghi với mọi sự biến đổi của mạng hay không. Từ đó chúng ta có kĩ thuật chọn đường *thích nghi* và kĩ thuật chọn đường *tĩnh*.

Trong kĩ thuật chọn đường tập trung, có một trung tâm điều khiển mạng chịu trách nhiệm lựa chọn đường đi tốt nhất. Sau đó các bảng chọn đường (routing table) được gửi cho các trạm để chúng phát dữ liệu theo các con đường định sẵn trong đó.



Edsger W. Dijkstra

Như vậy thông tin cần cho việc chọn đường chỉ được lưu giữ tại trung tâm mạng. Trái lại, trong kĩ thuật chọn đường phân tán, không tồn tại các trung tâm tìm đường đi trên mạng. Các máy trạm phải tự quyết định đường đi cho các gói tin của chúng. Điều này đòi hỏi các trạm phải thường xuyên trao đổi thông tin trạng thái và thông tin về đường truyền với nhau.

Sau đây chúng ta sẽ tìm hiểu một thuật toán dành cho kĩ thuật chọn đường tập trung, thuật toán **Dijkstra** (1959).

Mạng ARPANET của Bộ Quốc phòng Mỹ, tiền thân của mạng Internet hiện nay, đã chọn một phiên bản cải tiến của thuật toán Dijkstra để tìm đường đi cho các datagram. Trong phần trình bày sau đây, ta coi mạng như một đồ thị có hướng, mỗi trạm tương ứng với một nút, mỗi cạnh có một trọng số đặc trưng cho độ tốt xấu của đường truyền.

Giả thiết: Trọng số không âm, đường đi một chiều.

Mục đích: Tìm đường đi ngắn nhất từ đỉnh s tới các đỉnh khác.

Thuật toán gán cho các đỉnh các nhãn tạm thời, nhãn là một cặp hai thành phần phần, thứ nhất 'độ dài' từ s tới đỉnh đó và thứ hai là đỉnh ngay trước nó. Mỗi vòng lặp có một nhãn trở thành cố định – tức là tìm thêm được đường đi ngắn nhất tới một đỉnh.

PROCEDURE Dijkstra;

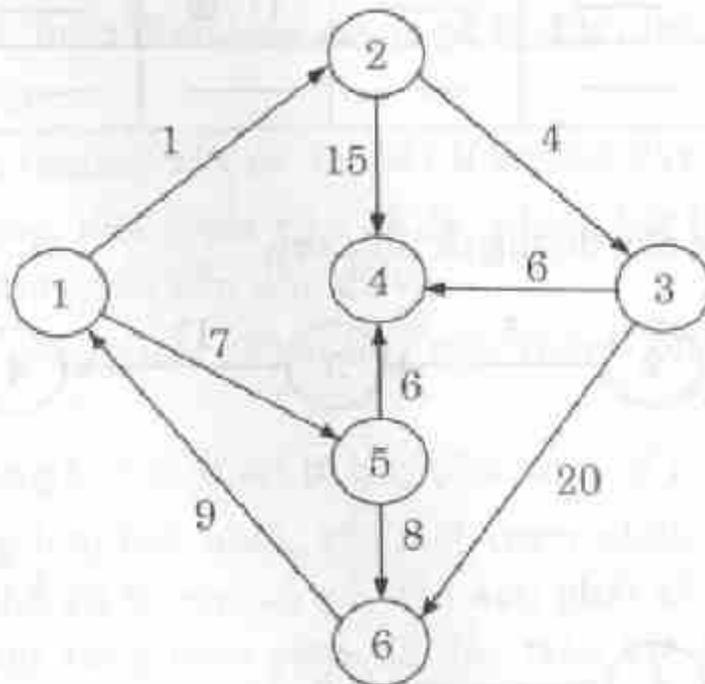
{ đầu vào: đồ thị có hướng $G=(V,E)$. V : tập các đỉnh, E : tập các cung. Đỉnh s : đỉnh xuất phát. Ma trận cung $A: a[i,j]$ độ dài cung nối hai đỉnh i và j , $a[i,j] \geq 0 \forall i,j$.

$d[v]$: độ dài đường đi từ đỉnh xuất phát s tới đỉnh v

$Truoc[v]$: đỉnh trước v trên đường nối từ s tới v .

```
}  
BEGIN  
  { khởi tạo}  
  for  $v \in V$  do  
    begin  
       $d[v] := a[s, v];$   
       $Truoc[v] := s;$   
    end;  
 $d[s] := 0; T := V \setminus \{s\};$  {  $T$ : tập các đỉnh có nhãn tạm thời}  
  { Lặp}  
  while  $T \neq \emptyset$  do  
    begin  
      Tìm đỉnh  $u \in T$  thỏa mãn:  $d[u] = \min\{d[z] : z \in T\};$   
       $T := T \setminus \{u\};$  { Cố định nhãn của đỉnh  $u$ }  
      for  $v \in T$  do { gán lại nhãn cho các đỉnh trong  $T$ }  
        if  $d[v] > d[u] + a[u, v]$  then  
          begin  
             $d[v] := d[u] + a[u, v];$   
             $Truoc[v] := u;$   
          end;  
    end;  
  end;  
END;
```

Ví dụ



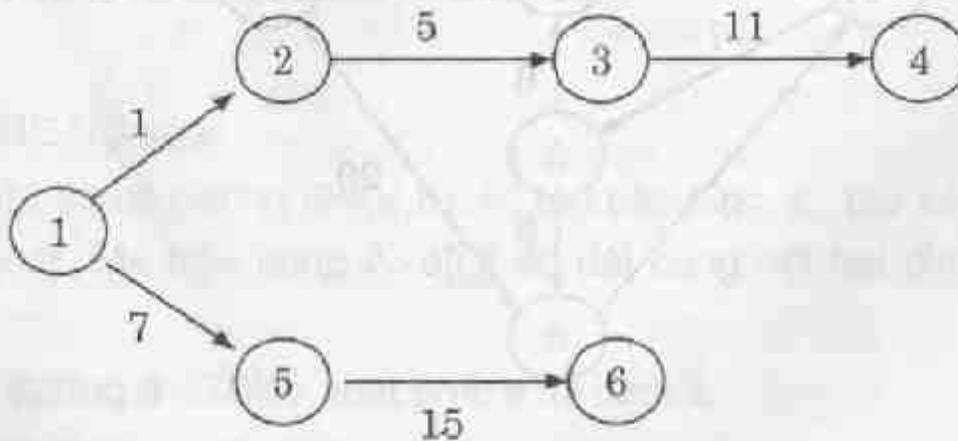
Ma trận trọng số A

I \ J	1	2	3	4	5	6
1	1				7	
2			4	15		
3				6		20
4						
5				6		8
6	9					

Kết quả tính toán theo các bước, đỉnh đánh dấu * là đỉnh được chọn để cố định nhân ở bước lập đang xét, nhân của nó không đổi ở những bước sau và được kí hiệu là —. Hai thành phần của nhân viết theo thứ tự (d[v], Truoc[v]). Sau đây là các bước tiến hành thuật toán:

Bước	Đỉnh 1	Đỉnh 2	Đỉnh 3	Đỉnh 4	Đỉnh 5	Đỉnh 6
Khởi tạo	0, ①	1*, ①	∞ , ①	∞ , ①	7, ①	∞ , ①
1	—	—	5*, ②	16, ②	7, ①	∞ , ①
2	—	—	—	11, ③	7*, ①	25, ③
3	—	—	—	11*, ③	—	15, ⑤
4	—	—	—	—	—	15*, ⑤

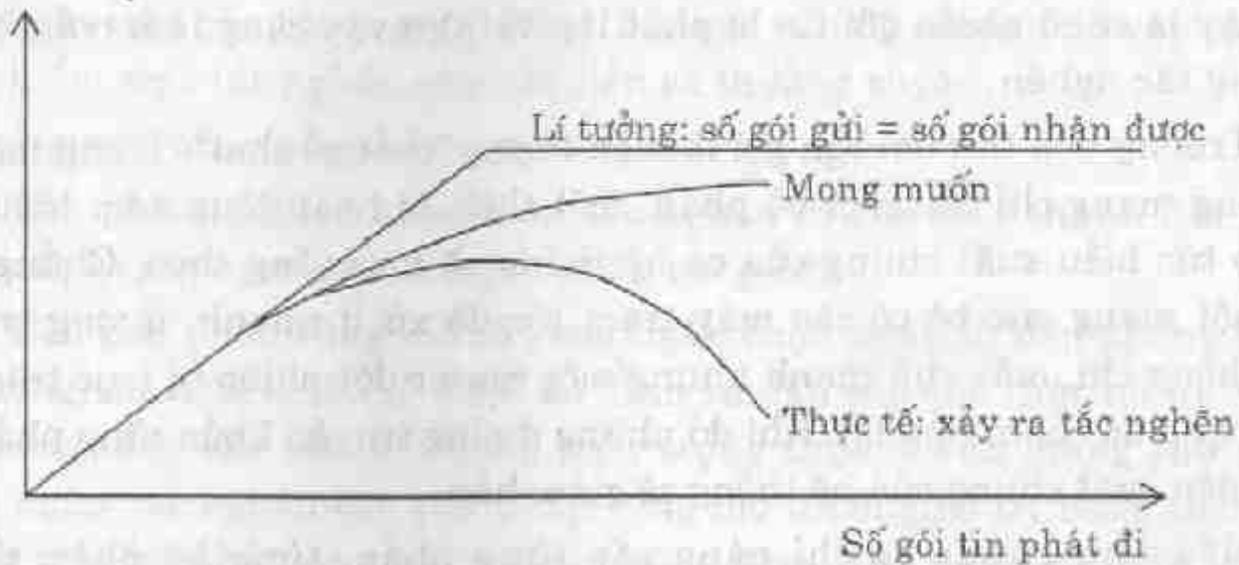
Từ đó ta thu được cây đường đi như sau



1.6.2. Hiện tượng tắc nghẽn

Mạng máy tính cũng tương tự như một hệ thống giao thông công cộng, khi có quá nhiều xe cộ thì phải xảy ra ùn tắc. Hiện tượng này làm suy giảm nghiêm trọng, thậm chí dừng hẳn hoạt động của mạng.

Số gói tin thực sự tới đích



Trong hình vẽ trên ta thấy, nếu số gói tin gửi lên đường truyền nhỏ hơn hoặc gần bằng khả năng vận chuyển của mạng thì tất cả chúng sẽ được chuyển đến đích, trừ một tỉ lệ nào đó bị lỗi. Nhưng nếu số gói bắt đầu bằng và vượt quá khả năng chuyển tải thì mạng không thể đảm đương nổi. Một số gói tin không thể chuyển đi được, một số bị thất lạc. Nếu số gói vẫn tiếp tục tăng lên, hoạt động của mạng sẽ bị đình trệ và có thể ngừng hẳn.

Nguyên nhân

Tắc nghẽn thường xảy ra do mấy lí do sau đây:

- Trên mạng, một trạm nào đó đột nhiên trở thành trung tâm chú ý, gói tin từ các trạm khác dồn dập đổ về.
- Bộ xử lí của router chậm hay một thành phần nào đó của mạng có công suất kém.
- Có sự hỏng hóc về thiết bị hay phá hoại cố ý.

Xét trường hợp thứ nhất, khi một trạm nhận được nhiều gói tin hơn mức mà nó có thể xử lí, những gói đến sau phải xếp hàng trong một vùng đệm*. Nhưng nếu vùng đệm cũng đã đầy tràn mà các gói tin vẫn tiếp tục tới thì chúng sẽ bị hủy. Có thể nhầm tưởng rằng chỉ cần tăng kích thước

* Xem lại chương 2, mục 2.1.1 về vùng đệm

vùng đệm là giải quyết được vấn đề này. Nhưng vấn đề lại phức tạp hơn thế nhiều. Ta giả sử rằng bằng cách nào đó ta thu xếp được cho các trạm một vùng đệm vô hạn, như vậy là các gói tin đến sau cứ việc vào vùng đệm và chờ đến lượt xử lí mà không bị hủy nữa. Nhưng thời gian chờ đó lại vượt quá thời gian quy định, trạm phát không nhận được tín hiệu phản hồi rằng gói tin đã đến đích, nó sẽ tưởng rằng gói tin bị thất lạc và phát lại. Như vậy là sẽ có nhiều gói tin bị phát lặp và như vậy càng làm trầm trọng thêm sự tắc nghẽn.

Trường hợp thứ hai còn gọi là hiện tượng "thắt cổ chai". Trong toàn bộ hệ thống mạng chỉ cần một bộ phận, một thiết bị hoạt động kém hiệu quả thì lập tức hiệu suất chung của cả hệ thống sẽ hạ xuống theo. Chẳng hạn như một mạng cục bộ có các máy trạm tốc độ xử lí nhanh, đường truyền băng thông lớn, máy chủ mạnh nhưng một router đột nhiên bị trục trặc, các gói tin qua đó chậm hẳn lại. Khi đó những đường truyền khác cũng phải chờ và cả hiệu suất chung của hệ thống sẽ giảm hẳn.

Nếu như chúng ta chỉ nâng cấp từng phần, từng bộ phận thì cổ chai chỉ dời từ chỗ nọ sang chỗ kia mà thôi, hiệu năng chung của cả hệ thống không thể cải thiện được. Mọi thành phần của hệ thống mạng phải hoạt động với công suất cân bằng nhau thì mới tránh khỏi hiện tượng thắt cổ chai.

1.6.3. Kiểm soát tắc nghẽn

Trước hết cần phân biệt hai khái niệm: *kiểm soát tắc nghẽn* và *kiểm soát dòng*. Kiểm soát dòng chỉ quan tâm đến liên lạc giữa hai trạm nhằm đảm bảo không có sự chênh lệch về tốc độ thu và phát. Kiểm soát tắc nghẽn mang tính toàn cục hơn, nó theo dõi hoạt động của mọi thiết bị trong mạng như máy trạm, router, đường truyền ... nhằm duy trì hoạt động bình thường của mạng và tránh xảy ra tắc nghẽn.

Xét ví dụ sau: một mạng cục bộ có đường truyền tốc độ cao, băng thông có thể lên đến 1 Gbps. Máy server, là một siêu máy tính tốc độ rất cao, đang cố gắng truyền dữ liệu cho một máy trạm – có bộ xử lí Intel 486 – với tốc độ 100 Mbps. Rõ ràng ở đây không có vấn đề tắc nghẽn mạng vì băng thông của đường truyền đủ rộng, nhưng chức năng kiểm soát dòng dữ liệu cần phải hoạt động để giảm tốc độ phát của server xuống cho máy trạm theo kịp.

Hãy xét một trường hợp khác. Hai phân đoạn mạng (segment), mỗi

phân đoạn có khoảng 100 máy trạm có cấu hình tương đương nhau, kết nối bằng đường truyền băng thông 10 Mbps. Hầu hết các trạm của phân đoạn thứ nhất đang cố gắng truyền với tốc độ 1 Mbps sang một trạm nào đó thuộc phân đoạn thứ hai. Trong trường hợp này, khả năng thu phát của các máy trạm là xấp xỉ nhau nên chức năng kiểm soát dòng gôn như không cần thiết. Vấn đề là băng thông của kênh truyền (10 Mbps) quá nhỏ so với nhu cầu của các trạm ($100 \times 10 \text{ Mbps} = 1000 \text{ Mbps}$), do vậy các hoạt động kiểm soát tắc nghẽn sẽ phải diễn ra thường xuyên.

Nguyên tắc chung của việc kiểm soát tắc nghẽn

Các phương pháp kiểm soát tắc nghẽn có thể chia thành hai nhóm: các giải pháp vòng mở và các giải pháp vòng kín.

Các giải pháp vòng mở cố gắng ngăn chặn ngay từ đầu không để xảy ra tắc nghẽn. Các thiết kế được ấn định từ đầu sao cho thật tối ưu và sau đó không thay đổi nữa bất chấp hiện trạng thực tế của mạng sau đó. Để ngăn ngừa tắc nghẽn các giải pháp vòng mở thường bố trí băng thông của đường truyền, khả năng lưu trữ của vùng đệm, khả năng xử lý dữ liệu của CPU và router vượt hơn so với yêu cầu.

Ngược lại, các giải pháp vòng kín được triển khai để ứng phó với các tắc nghẽn trước và trong khi nó đang xảy ra, mục đích nhằm hiệu chỉnh hệ thống để khắc phục sự cố. Đó là:

- Tìm cách phát hiện tắc nghẽn xảy ra khi nào và ở đâu trên mạng.
- Hủy bỏ những gói tin đã bị tắc nghẽn (tại một vùng đệm nào đó) quá thời hạn định trước.
- Hạn chế số gói tin lưu thông trên mạng
- Chặn đường lên mạng khi xảy ra tắc nghẽn

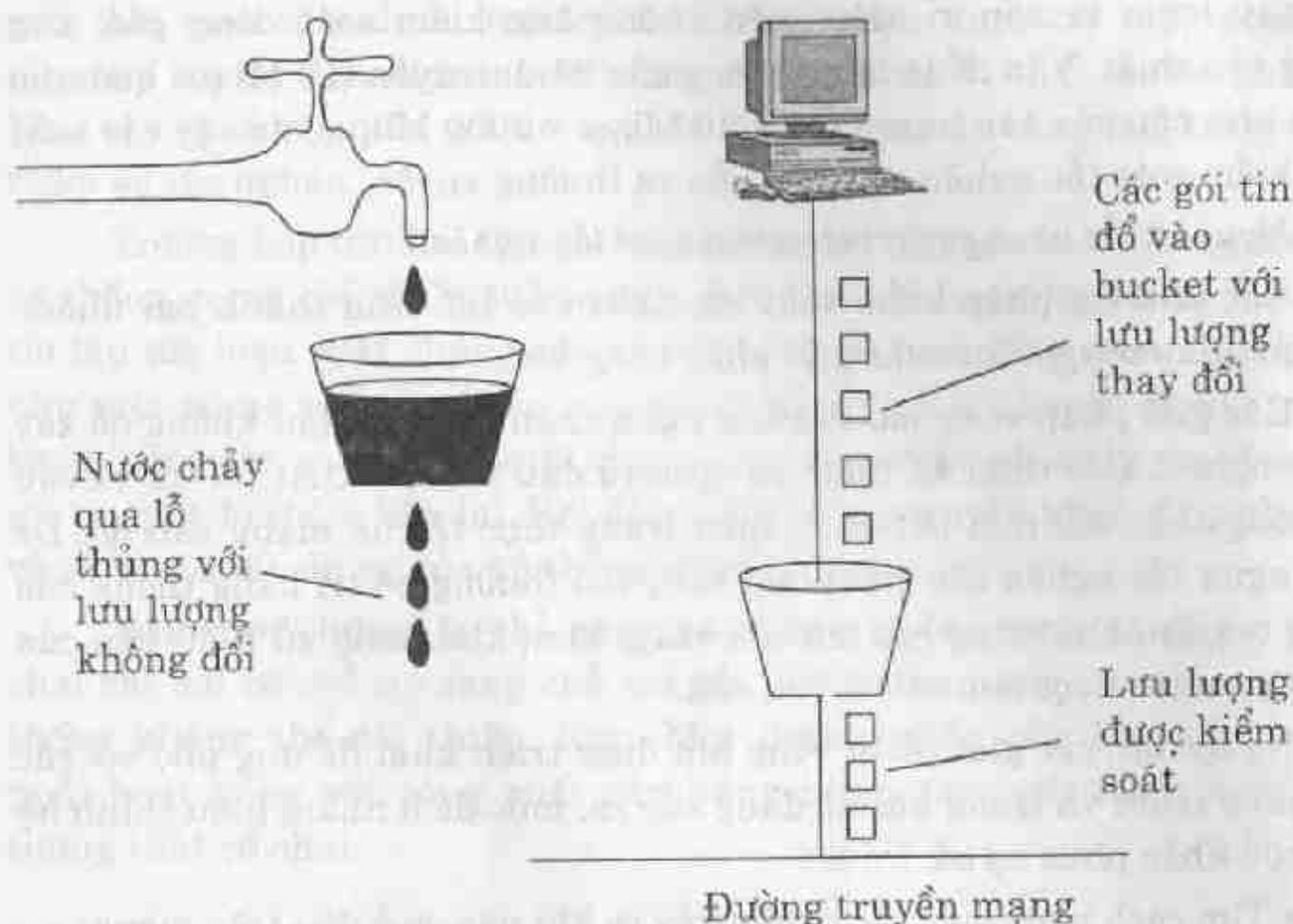
Thuật toán Cái xô thủng (Leaky Bucket)

Turner đề xuất thuật toán này năm 1986 với nội dung như sau:

Vấn đề: Dòng dữ liệu từ các trạm xuất ra không đều, lúc nhiều lúc ít khiến cho dòng dữ liệu trên mạng tăng giảm không ổn định, những lúc có nhiều trạm đồng thời đổ nhiều dữ liệu vào sẽ gây tắc nghẽn mạng. Cần phải điều hòa luồng dữ liệu trên mạng để đạt tới một lưu lượng ổn định, muốn vậy cũng phải điều hòa luồng dữ liệu từ mỗi trạm xuất ra đường truyền.

Giải pháp: Hãy hình dung một cái xô dựng nước có một lỗ thủng dưới đáy. Khi xô có nước, lượng nước chảy ra qua lỗ với lưu lượng gần như không đổi. Khi xô đầy mà nước vẫn chảy thêm vào, lượng nước thừa sẽ bị

tràn đi mất. Ở đây cái xô tượng trưng cho một vùng đệm đặt giữa CPU và đường truyền. Như vậy dù dữ liệu từ CPU vào thất thường, lúc nhiều lúc ít thì luồng dữ liệu ra (chảy từ đáy xô) vẫn đều đặn.



Chú ý rằng, nếu xô đã đầy rồi mà nước vẫn chảy vào thì sẽ bị tràn ra ngoài, tức những gói tin đến sau khi vùng đệm đã đầy sẽ bị hủy bỏ.

Nếu các đơn vị dữ liệu trên mạng có cùng kích thước – chẳng hạn như các gói tin trong mạng cell ATM – thì có thể căn cứ vào đơn vị đếm là số gói tin để biết xô đã đầy hay chưa và lưu lượng nước chảy qua lỗ thủng là bao nhiêu. Nhưng nếu các gói tin có kích thước không đồng đều thì phải cài đặt thêm một bộ đếm (theo đơn vị byte) để tính lượng nước chảy vào xô là bao nhiêu, xô đã đầy hay chưa và lưu lượng nước chảy qua lỗ thủng là bao nhiêu.

Thuật toán Token bucket:

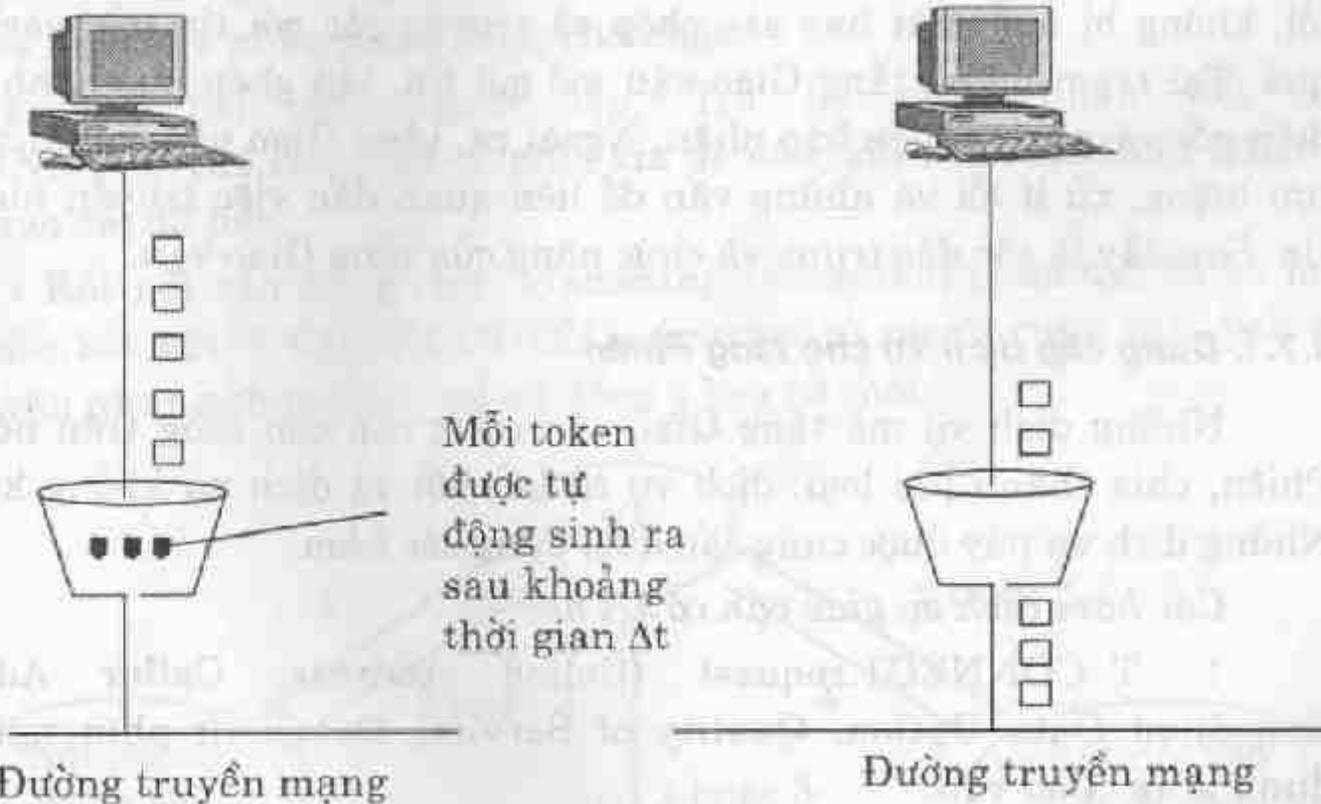
Trong thuật toán Cái xô thủng nêu trên có một điểm chưa được linh hoạt, đó là dữ liệu chỉ được xuất ra từ trạm một cách đều đều, do đó không

đáp ứng được những thời điểm trạm muốn truyền ngay một lượng lớn dữ liệu. Ta hãy xét một thuật toán linh hoạt hơn gọi là Token bucket.

Trong thuật toán này, xô không chứa các gói tin mà chứa các token* (thẻ truyền tin), các token này được sinh ra một cách đều đặn, cứ sau một khoảng thời gian Δt nào đó lại có một token được sinh ra. Trong xô có bao nhiêu token thì trạm được phép truyền cùng lúc bấy nhiêu đơn vị dữ liệu, và sau khi truyền thì số token trong xô bị trừ một số lượng tương ứng với số đơn vị dữ liệu đã truyền. Cũng giống như thuật toán Leaky bucket trên, đơn vị dữ liệu ở đây có thể tính theo số gói tin hoặc theo tổng kích thước (byte) của chúng.

Trạng thái trước ...

.. và sau đợt truyền



Những lúc trạm rỗi, truyền ít thì số token còn dư được lưu lại như một khoản cho vay (với thuật toán Leaky bucket thì khoản này không được tính). Với cơ chế này, khi trạm rỗi là lúc nó dễ dàng giành quyền được gửi để về sau có thể gửi cùng lúc một lượng lớn dữ liệu.

*Tất nhiên là vẫn phải có một vùng đệm ở đầu đó để chứa các gói tin chưa được gửi đi

1.7. Tầng Giao vận

Trong bảy tầng của mô hình OSI, nhóm bốn tầng thấp (Vật lý, Liên kết dữ liệu, Mạng, Giao vận) lo việc truyền dữ liệu trên đường truyền đảm bảo không lỗi, đúng địa chỉ và an toàn. Còn nhóm thứ hai gồm ba tầng trên (Phiên, Trình diễn, Ứng dụng) tập trung đáp ứng yêu cầu của người sử dụng và các trình ứng dụng. Tầng Giao vận là tầng cao nhất trong nhóm dưới, chức năng của nó là cung cấp các dịch vụ truyền dữ liệu sao cho những chi tiết cụ thể về cơ chế truyền thông bên dưới trở nên trong suốt đối với nhóm trên. Nói cách khác tầng Giao vận như một bức màn che phủ toàn bộ hoạt động bên dưới nó.

Cụ thể là tại tầng Giao vận các thông điệp được đóng gói, những thông điệp lớn được chia thành nhiều gói nhỏ, các thông điệp ngắn được gộp lại trong một gói. Tầng Giao vận phải bảo đảm truyền gói không phạm lỗi, không bị mất mát hay sao chép và truyền các gói tin một cách hiệu quả. Tại trạm nhận, tầng Giao vận mở gói tin, lắp ghép lại thành thông điệp gốc và gửi tín hiệu báo nhận. Ngoài ra, tầng Giao vận còn kiểm soát lưu lượng, xử lý lỗi và những vấn đề liên quan đến việc truyền nhận gói tin. Sau đây là các đặc trưng và chức năng của tầng Giao vận.

1.7.1. Cung cấp dịch vụ cho tầng Phiên

Những dịch vụ mà tầng Giao vận cung cấp cho tầng trên nó, tầng Phiên, chia thành hai loại: dịch vụ có kết nối và dịch vụ không kết nối. Những dịch vụ này được cung cấp dưới dạng các hàm.

Các hàm dịch vụ giao vận có kết nối

1. T-CONNECT.request (Called Address, Caller Address, Expedited Data Option, Quality of Service, Data): từ phía người sử dụng tầng Giao vận.

2. T-CONNECT.indication (Called Address, Caller Address, Expedited Data Option, Quality of Service, Data): từ phía người cung cấp dịch vụ Giao vận.

3. T-CONNECT.response (Quality of Service, Responding address, Expedited Data Option, Data): từ phía người sử dụng tầng Giao vận.

4. T-CONNECT.confirm (Quality of Service, Responding address, Expedited Data Option, Data): từ phía người cung cấp dịch vụ Giao vận.

5. T-DISCONNECT.request (Data): từ phía người sử dụng tầng Giao vận.

6. T-DISCONNECT.indication (Data): từ phía người cung cấp dịch vụ Giao vận.

7. T-DATA.request (Data): từ phía người sử dụng tầng Giao vận.

8. T-DATA.indication (Data): từ phía người cung cấp dịch vụ Giao vận.

9. T-EXPEDITED-DATA.request (Data): từ phía người sử dụng tầng Giao vận.

10. T-EXPEDITED-DATA.indication (Data): từ phía người cung cấp dịch vụ Giao vận.

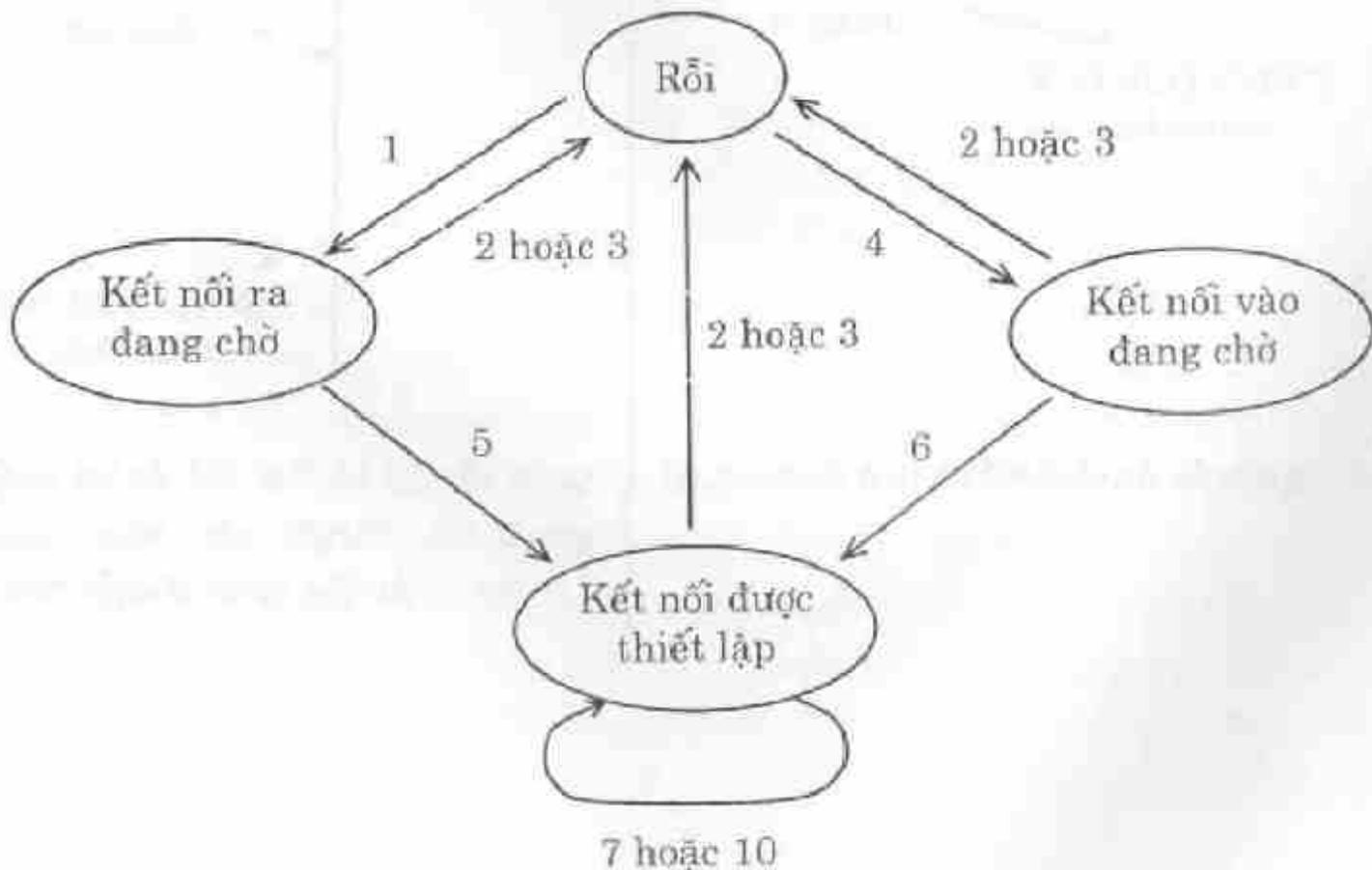
Các trạng thái thiết lập kết nối

- Rỗi (Idle): kết nối chưa được thiết lập, sẵn sàng chấp nhận cả hai kết nối đi và đến.

- Kết nối ra đang chờ (Outgoing connection pending): Người sử dụng tầng Giao vận đã gửi đi một yêu cầu kết nối T-CONNECTION.request, trả lời từ phía kia chưa nhận được, đang chờ nhận.

- Kết nối được thiết lập: Trả lời chấp nhận kết nối T-CONNECTION.response từ phía kia đã đến, kết nối được thiết lập, bắt đầu trao đổi dữ liệu.

- Kết nối vào đang chờ: (Incoming connection pending) đã có một yêu cầu kết nối T-CONNECTION.indication từ người cung cấp dịch vụ Giao vận nhưng chưa được trả lời đồng ý hay từ chối.



Ta thấy từ trạng thái "Rỗi" chuyển sang "Kết nối được thiết lập" có thể thông qua "Kết nối ra đang chờ" hoặc "Kết nối vào đang chờ". Đó là trường hợp yêu cầu kết nối do chính người sử dụng tại trạm để xuất hay do trạm kia gửi đến.

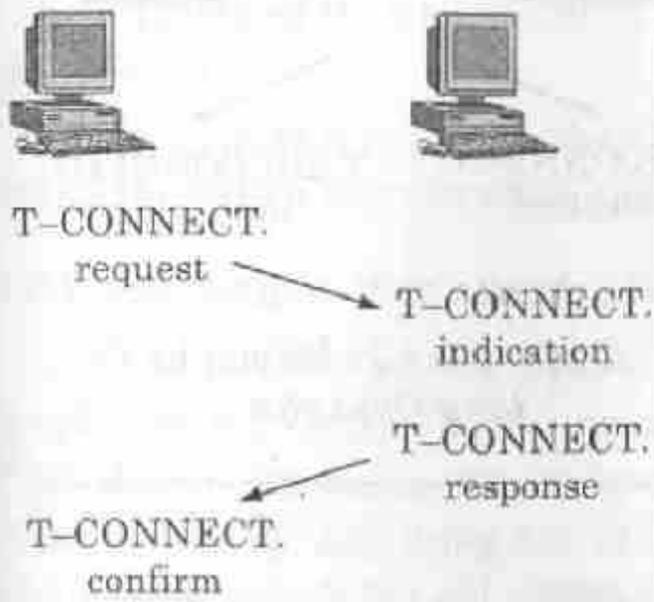
Sau khi kết nối được thiết lập, có hai cách để quay lại trạng thái Rỗi tương ứng với việc yêu cầu hủy kết nối do người sử dụng tăng Giao vận hay do bản thân tăng Giao vận. Trường hợp sau có thể là trạm bên kia muốn hủy kết nối hoặc người cung cấp dịch vụ chủ động hủy.

Các hàm dịch vụ giao vận không kết nối

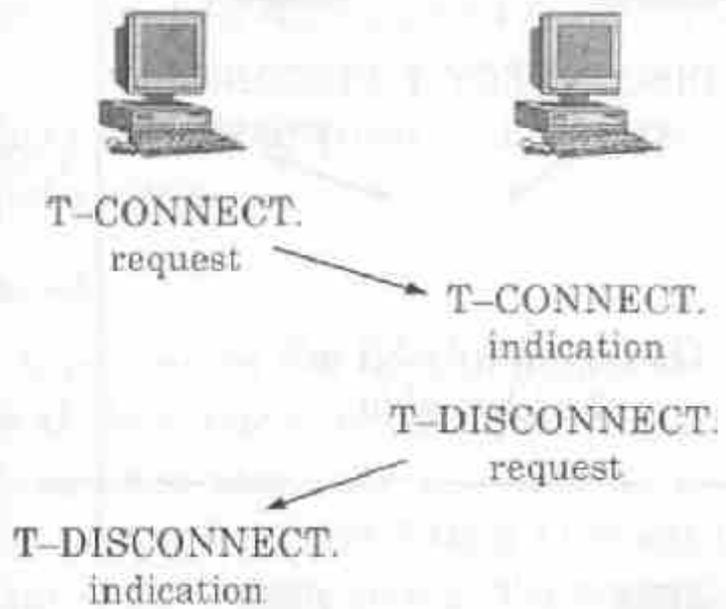
- T-UNITDATA.request (Source Address, Destination Address, Quality of Service, TS-data).
- T-UNITDATA.indication (Source Address, Destination Address, Quality of Service, TS-data).



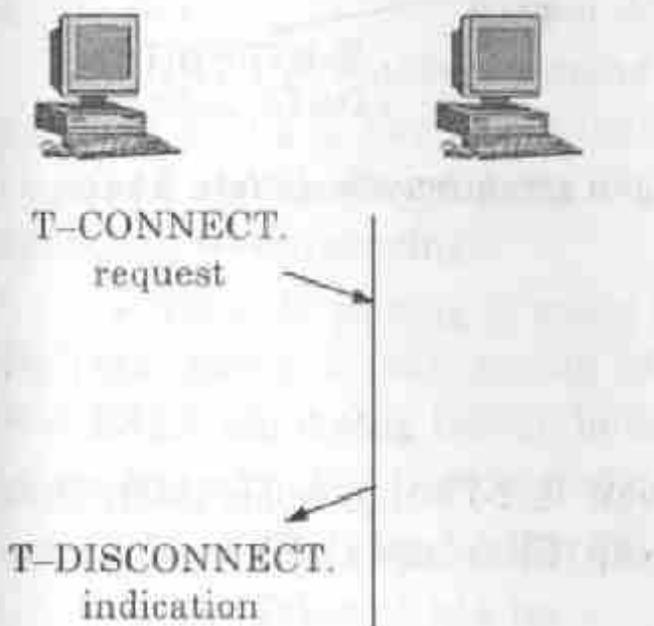
Quá trình kết nối, truyền dữ liệu và hủy kết nối dựa trên các hàm dịch vụ giao vận



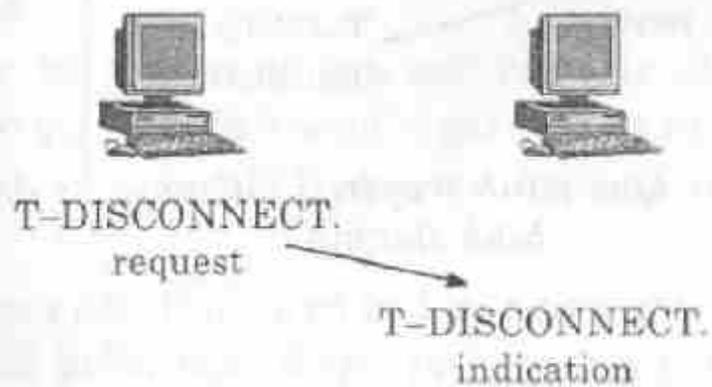
Quá trình kết nối thành công



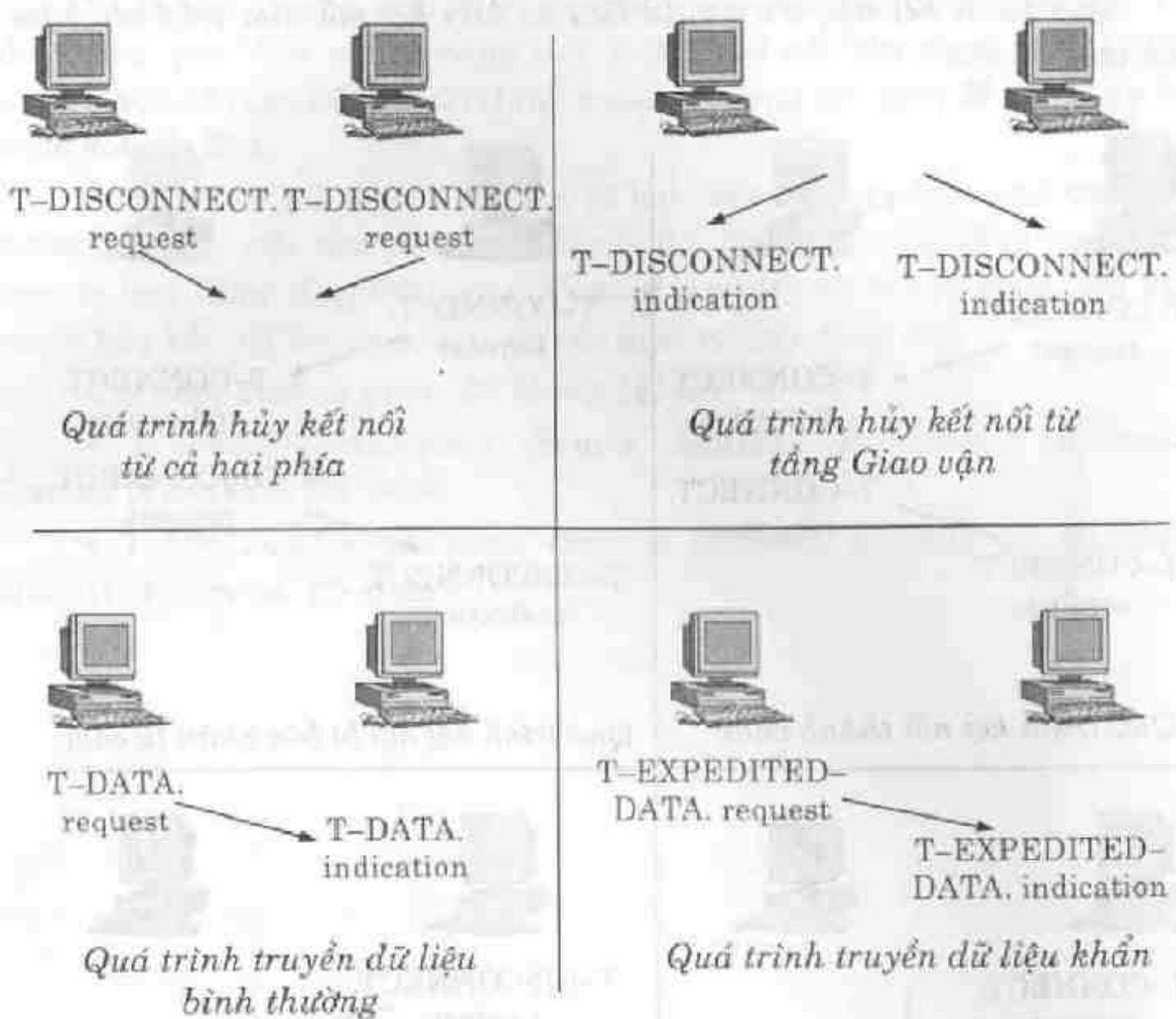
Quá trình kết nối bị bên nhận từ chối



Quá trình kết nối bị lỗi do tầng Giao vận, do Người sử dụng hoặc Người cung cấp dịch vụ



Quá trình hủy kết nối bình thường



1.7.2. Tăng cường chất lượng dịch vụ

Chức năng cơ bản của tầng Giao vận là bổ sung, hoàn thiện chất lượng những dịch vụ do tầng Mạng cung cấp. Chất lượng dịch vụ được đặc trưng bởi các thông số sau:

- Thời gian thiết lập liên kết, tức là thời gian từ khi gửi yêu cầu kết nối đi cho đến lúc kết nối được thiết lập.
- Xác suất thiết lập liên kết thành công.
- Tỷ lệ thông tin bị lỗi do truyền.
- Lưu lượng đường truyền tính theo số byte hữu ích.
- Thời gian hủy kết nối tính từ khi người sử dụng phát yêu cầu hủy cho đến khi kết nối thật sự bị hủy bỏ.

- Xác suất không thành công khi hủy kết nối trong thời gian lớn nhất.
- Khả năng bảo vệ, tức là mức độ người sử dụng cấm các trạm bên ngoài chen vào đường truyền.
- Thông số ưu tiên xác định quyền ưu tiên của người sử dụng đối với một kết nối.
- Thông số hủy bỏ cho phép tầng Giao vận tự quyết định hủy kết nối khi có tắc nghẽn hay các sự cố khác trên mạng.

1.7.3. Các lớp giao thức của tầng Giao vận

Ở tầng Liên kết dữ liệu, hai trạm truyền tin trực tiếp qua đường truyền vật lý do tầng Vật lý cung cấp. Ở tầng Giao vận, đường truyền vật lý được thay bằng mạng con (subnet), sự khác nhau này kéo theo sự khác nhau trong việc xây dựng các thủ tục, chẳng hạn như ở tầng Liên kết dữ liệu phải xác định địa chỉ nhận, ở tầng Giao vận thì không. Tại tầng Giao vận, chúng ta quan tâm đến các dịch vụ cung cấp bởi tầng Mạng hơn là các tính chất vật lý của đường truyền. Các dịch vụ cung cấp bởi tầng Mạng phụ thuộc vào mạng đó thuộc loại nào. CCITT và ISO đã chia mạng thành ba nhóm sau:

- Nhóm A: thường là mạng cục bộ, truyền dữ liệu một cách tin cậy, gần như không có lỗi, các gói tin được giả thiết là không bị mất, do đó tầng Giao vận không cần cung cấp các dịch vụ phục hồi (recovery) hay sắp xếp lại thứ tự (resequencing).

- Nhóm B: thường là mạng đường dài. Gói tin có khả năng bị mất, bị lỗi trên đường truyền nhưng có thể kiểm soát được. Phải gọi thủ tục N-RESET khi đường truyền bị tắc nghẽn hay có trục trặc thiết bị. Đối với mạng loại này tầng Giao vận có nhiệm vụ:

- Thiết lập lại liên kết
- Đồng bộ hóa lại
- Theo dõi những yêu cầu khởi động lại của người dùng

- Nhóm C: thường là mạng đường dài, không liên kết, gồm nhiều mạng con. Tỷ lệ lỗi cao hơn mức chấp nhận được, do đó nhiệm vụ của tầng Giao vận là phức tạp. Nó phải có khả năng phục hồi lỗi, sắp xếp lại thứ tự các gói tin.

Chất lượng dịch vụ do tầng Mạng cung cấp càng kém thì giao thức của tầng Giao vận bên trên càng phức tạp. CCITT và ISO đã định nghĩa

5 lớp giao thức cho tầng Giao vận để thích ứng với 3 nhóm mạng kể trên như sau:

Lớp giao thức tầng Giao vận	Loại mạng tương ứng	Đặc trưng
0	A	Các thủ tục đơn giản vì dịch vụ ở lớp mạng có chất lượng đảm bảo
1	B	Phải kiểm tra lỗi
2	A	Thực hiện dồn kênh
3	B	Kiểm tra lỗi và dồn kênh
4	C	Phát hiện, phục hồi lỗi và dồn kênh

• *Lớp 0 (mạng loại A)*

Các giao thức lớp 0 tương đối đơn giản, cho phép thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết. Chúng có khả năng phát hiện và báo hiệu lỗi, nhưng không có khả năng phục hồi lỗi. Nếu tầng Mạng phát hiện và báo lên một lỗi cho tầng Giao vận thì tầng này sẽ hủy kết nối tương ứng và thông báo cho người sử dụng biết.

• *Lớp 1 (mạng loại B)*

Ngoài các tính chất như lớp 0, các giao thức lớp 1 còn có thêm các chức năng sau:

- Khởi động lại mạng sau khi tầng mạng thực hiện thủ tục N-RESET, sau đó tái đồng bộ và tái thiết lập kết nối.
- Báo nhận (Acknowledgement) và truyền dữ liệu khẩn.
- Phục hồi lỗi.

• *Lớp 2 (mạng loại A)*

Là phiên bản cải tiến của lớp 0 bổ sung thêm việc ghép kênh, tức là dồn một số kết nối ở tầng Giao vận vào một liên kết duy nhất ở tầng Mạng, đồng thời kiểm soát luồng để tránh tắc nghẽn. Tuy nhiên các giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi nên chúng chỉ hoạt động trên nền mạng tin cậy loại A.

• *Lớp 3 (mạng loại B)*

Đây là sự tổ hợp các giao thức lớp 1 và lớp 2 với các chức năng sau:

- Dồn kênh.
- Khởi động lại.
- Kiểm soát dòng dữ liệu.
- Phát hiện và phục hồi lỗi.

• **Lớp 4 (mạng loại C)**

Những giao thức lớp này có hầu hết những khả năng của các lớp trước, chúng có thể:

- Giải quyết vấn đề gói tin bị mất, bị lỗi.
- Khởi động lại.
- Kiểm soát việc truyền dữ liệu tránh tắc nghẽn.

1.8. Tầng Phiên

Như phần 1.7 đã trình bày, mô hình 7 tầng OSI có thể chia thành hai nhóm theo đặc trưng về chức năng của chúng. Tầng Phiên là tầng thấp nhất trong nhóm các tầng trên gồm: tầng Phiên, tầng Trình diễn và tầng Ứng dụng. Nhóm này tập trung phục vụ các yêu cầu của người sử dụng bằng cách tổ chức các phân mềm mạng để triển khai các ứng dụng truyền thông tin thông qua sự phục vụ của nhóm bốn tầng dưới.

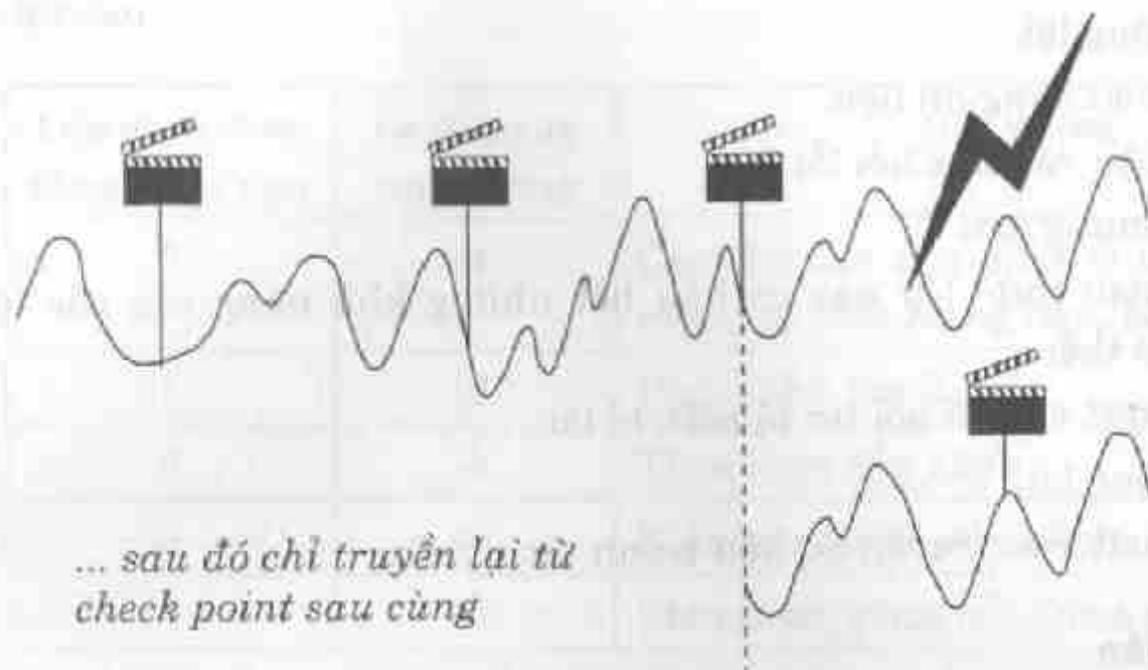
1.8.1. Nhiệm vụ của tầng Phiên

- Điều phối việc trao đổi dữ liệu giữa các trình ứng dụng bằng cách thiết lập và giải phóng các phiên làm việc.
- Tổ chức các điểm đồng bộ hóa để kiểm soát việc trao đổi dữ liệu.
- Cung cấp cơ chế lần lượt nắm quyền trong trao đổi dữ liệu.

Việc trao đổi thông tin trên mạng có thể diễn ra theo một trong ba phương pháp: Song công, Bán song công và Đơn công. Trong phương pháp Bán song công hai trạm thay phiên nhau làm chủ đường truyền, trạm này phát thì trạm kia thu. Ở đây tầng Phiên có nhiệm vụ báo cho mỗi trạm khi đến lượt nắm quyền điều khiển đường truyền.

Các điểm đồng bộ hóa – checkpoint and restart – do tầng Phiên đặt trong dòng dữ liệu cho phép khôi phục nhanh nhất một khi xảy ra gián đoạn truyền thông. Khi đó chỉ cần truyền lại bắt đầu từ điểm check – point gần nhất chứ không phải truyền từ đầu.

Xảy ra sự cố làm gián đoạn



Tầng Phiên còn có nhiệm vụ duy trì các liên kết Phiên tương ứng với các liên kết Giao vận. Có thể nhiều liên kết Phiên phân chia cùng một liên kết Giao vận hoặc ngược lại, một liên kết Phiên sử dụng nhiều liên kết Giao vận.

1.8.2. Các dịch vụ của tầng Phiên

Các dịch vụ tầng Phiên cung cấp cho người sử dụng nhằm các mục tiêu sau:

- Thiết lập một liên kết Phiên với một người sử dụng khác, trao đổi dữ liệu, cuối cùng hủy bỏ liên kết khi không dùng đến nữa.
- Quản lý việc sử dụng và chuyển giao token. Ở đây token là khái niệm khác với thẻ bài token của mạng Token Ring tuy cơ chế hoạt động cũng tương tự như nhau. Khi áp dụng cơ chế sử dụng token, chỉ có trạm đang giữ token mới được quyền thực hiện thao tác. Việc cấp token cho bên nào, việc quản lý và thu hồi token ra sao là một chức năng của tầng Phiên.

Trong phần sau chúng ta sẽ làm rõ hơn khái niệm và cơ chế hoạt động của token.

- Thiết lập các điểm đồng bộ hóa – check point – trong cuộc truyền, khi xảy ra sự cố tiến hành khôi phục và truyền lại bắt đầu từ check point gần nhất.

Sau đây là mô tả chi tiết các dịch vụ tầng Phiên cho từng giai đoạn: thiết lập kết nối, truyền dữ liệu và cuối cùng hủy kết nối.

Tên dịch vụ	Chức năng
<i>Nhóm dịch vụ thiết lập liên kết Phiên</i>	
Session Connection	Thiết lập kết nối, đàm phán về quyền sử dụng token và các tham số truyền, chẳng hạn như chất lượng dịch vụ.
<i>Nhóm dịch vụ truyền dữ liệu</i>	
Normal Data Transfer	Cho phép truyền các đơn vị dữ liệu qua một liên kết Phiên theo phương thức Song công hay Bán song công.
Expedited Data Transfer	Truyền các đơn vị dữ liệu khẩn qua liên kết Phiên mà không phải chịu các ràng buộc về token cũng như các dịch vụ kiểm soát luồng dữ liệu khác.
Tiped Data Transfer	Truyền các đơn vị dữ liệu qua liên kết Phiên độc lập với việc gán token, do vậy dữ liệu có thể ngược với luồng dữ liệu hiện hành.
<i>Nhóm dịch vụ quản lý token</i>	
Give Token	Trao lại quyền sử dụng token cho trạm khác
Please Token	Cho phép một người sử dụng yêu cầu một token cụ thể đang được một người khác sử dụng
Give Control	Trao lại tất cả các token cho một người khác
<i>Nhóm dịch vụ đồng bộ hóa</i>	
Minor Synchronization Point	Cho phép người sử dụng đặt điểm đồng bộ hóa phụ trong dòng dữ liệu đang truyền. Người đó có thể yêu cầu sự xác nhận tương minh rằng người sử dụng bên kia đã đồng ý công nhận điểm đồng bộ phụ đó.

Major Synchronization Point	Xác định các điểm đồng bộ hóa chính trong dòng dữ liệu đang truyền. Các điểm này sẽ tách biệt một đơn vị dữ liệu khỏi các đơn vị dữ liệu được truyền trước và sau đó.
Resynchronization	Thiết lập lại liên kết bắt đầu từ một điểm đồng bộ trước đó, nhưng không lùi xa hơn điểm đồng bộ chính cuối cùng
<i>Nhóm dịch vụ dành cho Activity</i>	
Activity Start	Thông báo rằng một Activity mới được đưa vào.
Activity Resume	Thông báo rằng một Activity đã bị ngắt trước đây nay được khởi động lại
Activity Interrupt	Cho phép một Activity được kết thúc một cách bất thường, kết quả được bảo lưu
Activity Discard	Cho phép một Activity được kết thúc một cách bất thường, kết quả không được bảo lưu và bị hủy bỏ
Activity End	Kết thúc một Activity
<i>Nhóm dịch vụ hủy liên kết Phiên</i>	
Orderly Release	Hủy bỏ liên kết Phiên sau khi toàn bộ dữ liệu đã được tiếp nhận.
User Initiaed Abort	Hủy bỏ một Phiên, xóa bỏ luôn các yêu cầu chưa được giải quyết nên có thể mất các đơn vị dữ liệu chưa phân phối.

1.8.3. Khái niệm Token, điểm đồng bộ chính và phụ, Activity

- Token

Chúng ta quay lại cơ chế token. Trong khi hai trạm tương tác với nhau, điều quan trọng là không để xảy ra tình trạng cả hai cùng thực hiện một thao tác, một cơ chế kiểm soát (giống như hai người đi ngược chiều tránh nhau, nếu cả hai luôn tránh về cùng một phía thì sẽ va vào nhau). Token là một thuộc tính được gán tạm thời cho một người sử dụng và đảm

bảo cho người đó quyền được gọi các dịch vụ nhất định. Ai có token sẽ có quyền truyền dữ liệu.

ISO định nghĩa bốn loại token:

- Data token: dùng để quản lý một liên kết Bán song công.
- Synchronize Minor Token: dùng để điều khiển việc đặt các điểm đồng bộ hóa phụ.
- Major/Activity Token: dùng để điều khiển việc đặt các điểm đồng bộ hóa chính và quản lý các Activity.
- Release Token: quản lý việc hủy bỏ liên kết.

Một token luôn ở trong một trong hai trạng thái sau:

+ Not Available: trong trường hợp data token và release token, trạng thái này có nghĩa là các dịch vụ tương ứng – truyền dữ liệu và hủy bỏ liên kết – là khả dụng đối với cả hai người sử dụng liên kết. Trong trường hợp Synchronize Minor Token và Major/Activity Token trạng thái này có nghĩa là dịch vụ tương ứng – đồng bộ hóa và activity – là không sử dụng được đối với cả hai người sử dụng.

+ Available: token sẽ được gán cho một trong hai người sử dụng và người đó sẽ có quyền gọi các dịch vụ tương ứng.

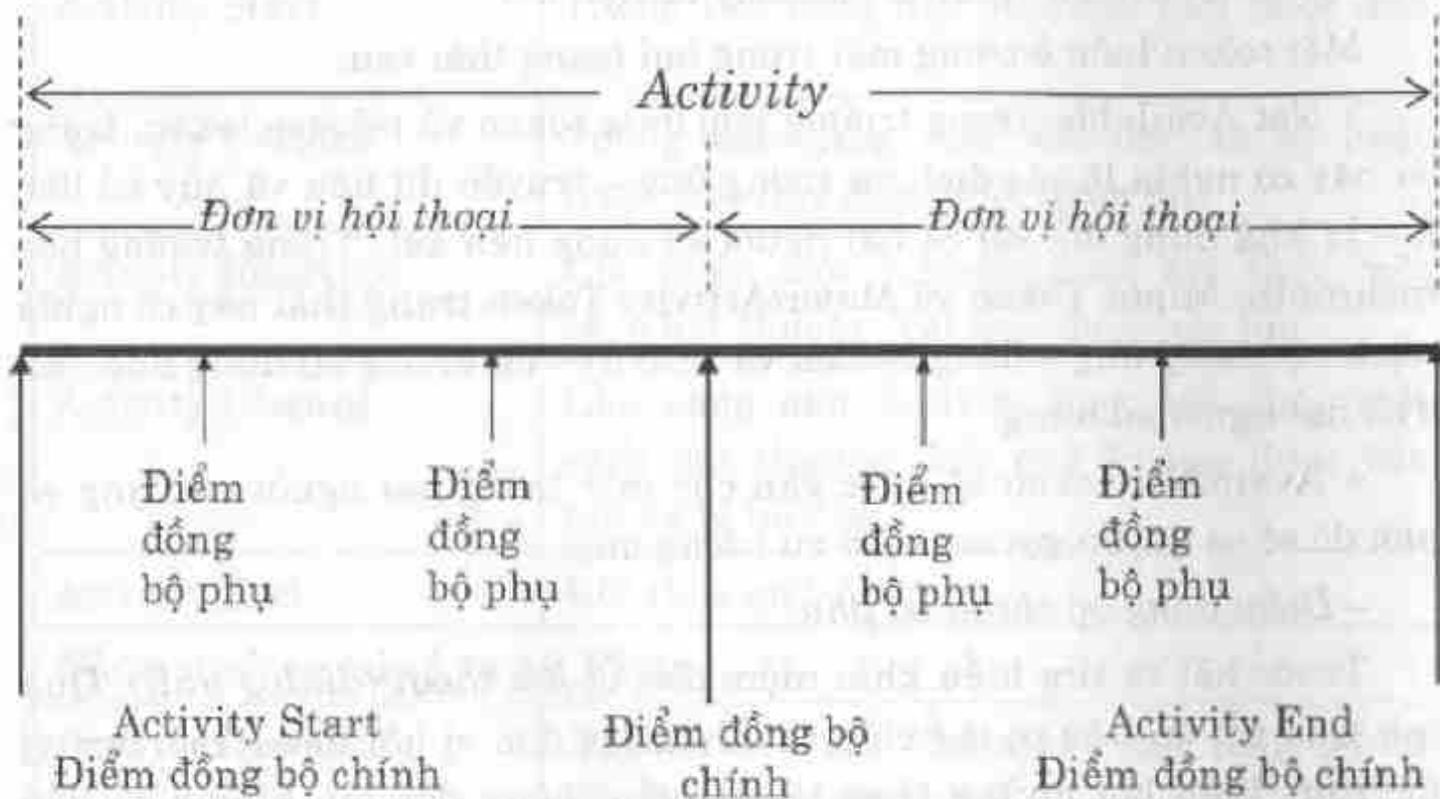
– *Điểm đồng bộ chính và phụ*

Trước hết ta tìm hiểu khái niệm đơn vị hội thoại (*dialog unit*). Quá trình trao đổi dữ liệu có thể chia thành nhiều đơn vị hội thoại, mỗi đơn vị được thực hiện bởi những thao tác truyền thông độc lập không có liên quan gì đến những đơn vị hội thoại trước và sau đó. Một đơn vị hội thoại có thể bị ngắt giữa chừng, sau đó khôi phục lại nhờ các điểm đồng bộ hóa.

Điểm đồng bộ hóa (check point) có hai chức năng. Một là để phân tách các phần của một cuộc hội thoại, hai là để khôi phục cuộc thoại khi có lỗi xảy ra. *Điểm đồng bộ chính (major check point)* dùng để chia quá trình trao đổi dữ liệu thành một chuỗi các đơn vị hội thoại. Mỗi điểm đồng bộ chính phải được xác nhận (confirmation) đồng ý từ phía người sử dụng bên kia. Chưa có xác nhận thì người sử dụng chỉ được gọi một số dịch vụ hạn chế, chẳng hạn không được gửi thêm dữ liệu.

Điểm đồng bộ hóa phụ được dùng để chia nhỏ một đơn vị hội thoại, chúng không nhất thiết phải được xác nhận và có thể dùng để khởi động lại quá trình trao đổi dữ liệu.

Cuối cùng là khái niệm *Activity*. Một *Activity* (hoạt động) bao gồm một hoặc nhiều đơn vị hội thoại, đó là việc thực hiện một tập hợp các nhiệm vụ có liên quan với nhau, ví dụ như truyền một tệp gồm nhiều phần, mỗi phần tương ứng với một đơn vị hội thoại. Tại mỗi thời điểm chỉ có một *Activity* trên một liên kết Phiên, nhưng nó có thể bị ngắt và sau đó khôi phục lại ở một liên kết Phiên khác. Do đó một *Activity* có thể diễn ra (từng phần nối tiếp) trên nhiều liên kết Phiên, và ngược lại trong thời gian tồn tại của một liên kết Phiên có thể diễn ra nhiều *Activity* (từng phần hay hoàn chỉnh).



1.9. Tầng Trình diễn

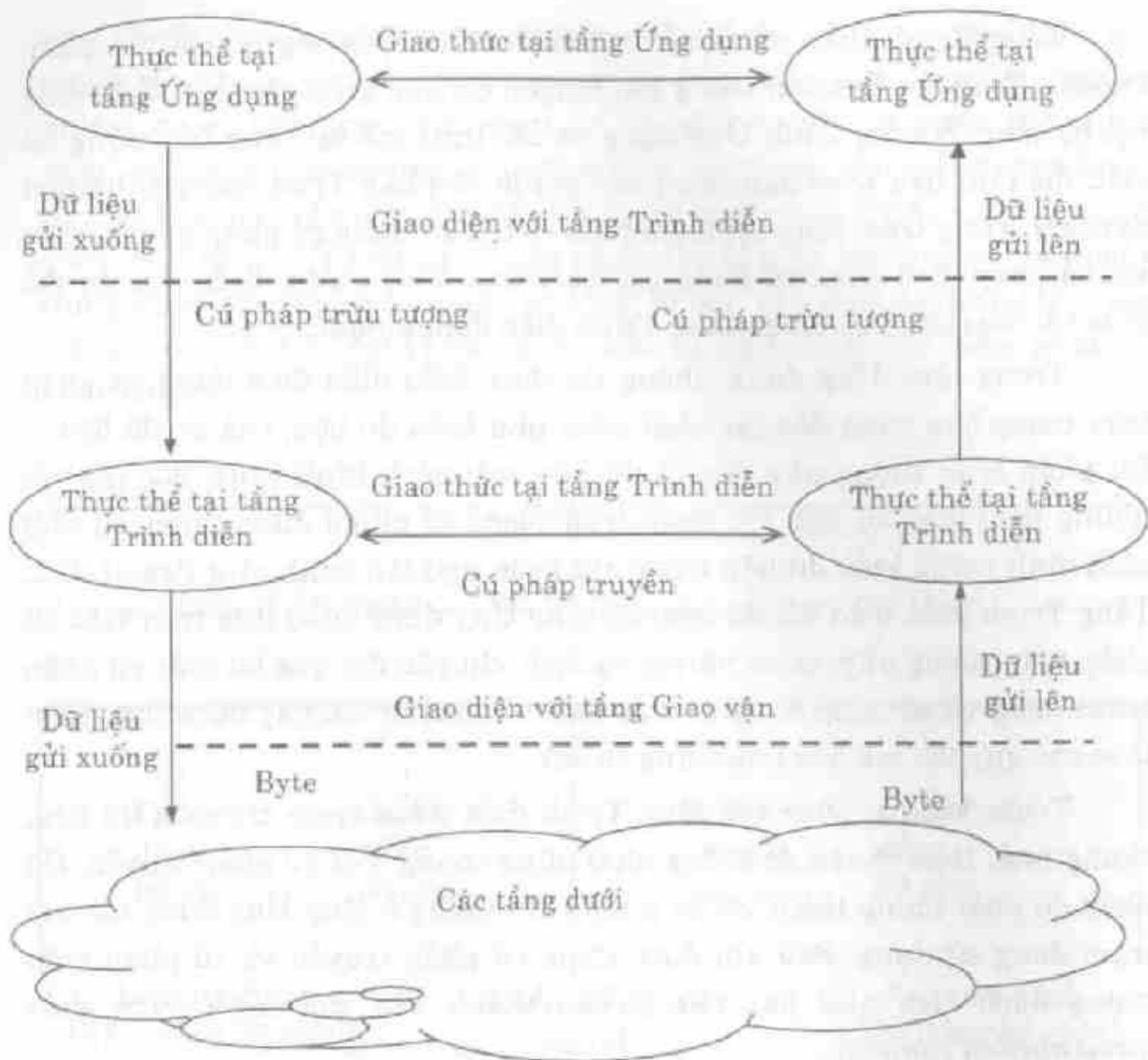
Không như một số người hiểu lầm, tầng Trình diễn không liên quan đến việc hiển thị dữ liệu là phần việc của tầng Ứng dụng bên trên mà nó đảm bảo cho các trạm có thể trao đổi dữ liệu với nhau mặc dù chúng sử dụng các dạng biểu diễn dữ liệu khác nhau.

Khi dữ liệu truyền qua ranh giới giao diện giữa tầng Trình diễn và tầng Phiên thì có một sự thay đổi quan trọng về mặt biểu diễn dữ liệu. Từ tầng Phiên trở xuống, dữ liệu được đặc tả dưới dạng nhị phân trong khi tầng Ứng dụng lại sử dụng những cấu trúc thông tin gắn gũi với con người như văn bản (text), bản ghi (record)... Do đó tầng Trình diễn có nhiệm vụ chuyển đổi cú pháp trình diễn dữ liệu giữa hai kiểu trên.

Tầng Trình diễn sử dụng một loại cú pháp riêng gọi là Cú pháp truyền (Transfer Syntax) trong khi truyền dữ liệu giữa các thực thể trong nội bộ tầng. Nhưng trình Ứng dụng và các thực thể tại tầng ứng dụng lại biểu diễn dữ liệu theo dạng cú pháp gọi là cú pháp Trừu tượng (Abstract Syntax). Tầng Ứng dụng tại trạm phát có thể sử dụng cú pháp nguồn khác với cú pháp đích được sử dụng tại trạm thu. Việc phiên dịch, chuyển đổi giữa các loại cú pháp đó do tầng Trình diễn đảm nhiệm.

Trong tầng Ứng dụng, thông tin được biểu diễn dưới dạng cú pháp trừu tượng liên quan đến các khái niệm như Kiểu dữ liệu, Giá trị dữ liệu ... Cú pháp trừu tượng này đặc tả dữ liệu một cách hình thức, độc lập với những biểu diễn cụ thể. Cú pháp trừu tượng có nhiều điểm tương tự như cách định nghĩa kiểu dữ liệu trong các ngôn ngữ lập trình như Pascal, C ... Tầng Trình diễn trao đổi dữ liệu với tầng Ứng dụng cũng dựa trên kiểu cú pháp trừu tượng này, nó có nhiệm vụ dịch, chuyển đổi qua lại giữa cú pháp trừu tượng và cú pháp truyền. Việc dịch và chuyển đổi này được thực hiện theo các quy tắc mã hóa (encoding rules).

Trước khi hai thực thể tầng Trình diễn ở hai trạm trao đổi dữ liệu, chúng phải thỏa thuận để thống nhất dùng chung một cú pháp truyền. Cú pháp đó phải tương thích với cú pháp trừu tượng ở tầng Ứng dụng mà hai trạm đang sử dụng. Sau khi được chọn, cú pháp truyền và cú pháp trừu tượng được xem như hai yếu tố cấu thành nên *Bối cảnh trình diễn (presentation context)*.



1.10. Tầng Ứng dụng

Tầng Ứng dụng định nghĩa các giao thức và chức năng cần thiết giúp người sử dụng thực hiện việc trao đổi thông tin qua mạng. Các chức năng cơ bản của tầng này là:

- Xây dựng các giao thức cung cấp dịch vụ tập tin từ xa như mở, đóng, đọc ghi, truy cập file đồng thời.
- Cung cấp dịch vụ truyền file, truy cập cơ sở dữ liệu từ xa.
- Cung cấp dịch vụ xử lý thông điệp cho các ứng dụng như e-mail, chat ...
- Cung cấp dịch vụ thư mục toàn cục để định vị tài nguyên trên mạng.
- Thi hành các tác vụ từ xa như Điều khiển từ xa (remote control).

1.11. An toàn thông tin trên mạng (network security)

Trong thời kì đầu của mạng máy tính, khi chỉ có vài chục người trong nội bộ công ti hay cơ quan nối mạng để dùng chung máy in thì vấn đề bảo mật và an ninh mạng chưa được chú ý. Nhưng hiện nay, khi hàng triệu người cùng tham gia với những công việc mang tầm quan trọng lớn lao như thanh toán ngân, hàng, chính phủ điện tử... thì an ninh mạng bị vi phạm, thậm chí bị một vài nhóm người sử dụng như là vũ khí để thực hiện những ý đồ của họ.

<i>Nhóm người ...</i>	<i>... lợi dụng mạng với ý đồ</i>
Sinh viên	Tô mò, trêu chọc, tự chứng tỏ bản thân.
Doanh nhân	Thăm dò, tìm hiểu chiến lược kinh doanh của đối thủ cạnh tranh. Cản trở công việc của đối thủ nếu cần.
Nhân viên thất nghiệp	Trả thù công ti cũ vì bị sa thải
Nhân viên kế toán	Biến thủ tiền công quỹ
Người buôn cổ phiếu	Phủ nhận một giao dịch với khách hàng khiến anh ta bị lỗ
Hacker	Phá phách những hệ thống bảo mật của người khác để tự thử sức hay ăn cắp dữ liệu, lấy trộm thẻ tín dụng.
Gián điệp	Tim hiểu những bí mật của đối phương
Kẻ theo chủ nghĩa khủng bố	Lấy trộm những bí mật có thể là mấu chốt gây xung đột.

Những hành động xâm hại an ninh mạng thực chất đều nhằm vào đối tượng là thông tin trên mạng, phương thức có thể là chủ động hay bị động. Với phương thức bị động, thông tin gốc không bị biến đổi mà chỉ bị nghe hay đọc trộm. Ngược lại phương thức phá hoại chủ động còn nhằm làm sai lệch nội dung, thứ tự hay làm trễ thông tin gốc, hoặc vô hiệu hóa các chức năng phục vụ của người dùng trên mạng. Hiện nay, nói chung những hành vi xâm hại theo kiểu bị động thường khó phát hiện nhưng lại có thể ngăn chặn một cách hiệu quả. Ngược lại những hành vi chủ động

rất dễ phát hiện – chẳng hạn như một Web site bị "dội bom" làm tê liệt trong nhiều giờ đồng hồ – nhưng rất khó ngăn chặn.

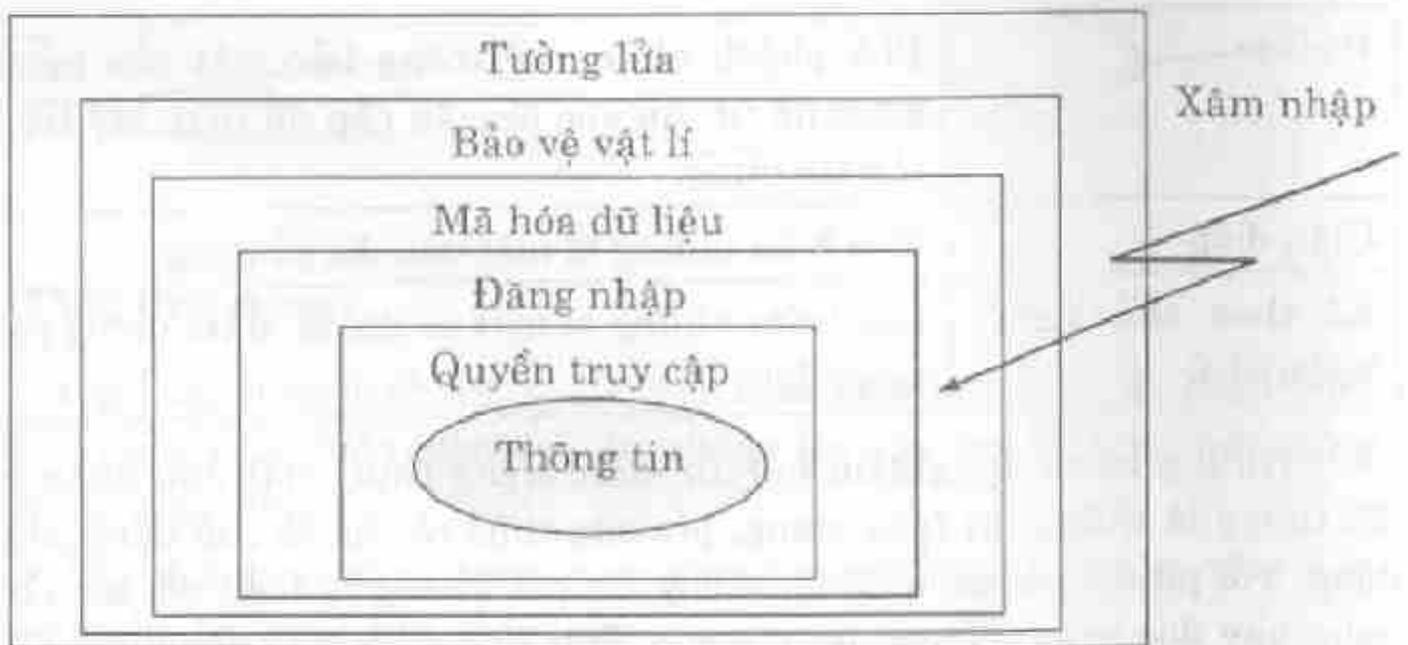
Trước khi tìm hiểu các chiến lược bảo vệ an ninh mạng, chúng ta cần chú ý rằng không có chiến lược nào là hoàn hảo cả. Một hệ thống bảo mật dù có mức độ an toàn cao đến mấy vẫn có điểm yếu có thể bị lợi dụng. Chỗ sơ hở có thể nằm ngay trong cơ chế thiết kế hoặc trong khi vận hành mới bộc lộ, chẳng hạn do nhân viên cũ bị sa thải tiết lộ.

1.11.1. Các lớp bảo mật

Bảo mật trên mạng nhằm:

- Bí mật (Secrecy): Ngăn cản những người không có quyền truy nhập
- Xác nhận (Authentication): Xác định đối tác trước khi thực hiện một giao dịch trên mạng.
- Tính không thể phủ nhận (Nonrepudiation): Xác minh nguồn gốc của một thông tin trên mạng.
- Điều khiển toàn vẹn (Integrity control): Quản lý được toàn bộ việc trao đổi thông tin trên mạng.

Các hệ thống an ninh mạng thường bao gồm nhiều lớp để chống lại các kiểu xâm phạm khác nhau. Sau đây là sơ đồ các lớp bảo mật thông dụng hiện nay:



Lớp bảo vệ trong cùng nhằm kiểm tra, giới hạn Quyền truy cập (Access right) của các đối tượng sử dụng tài nguyên mạng. Quyền truy cập quy định người sử dụng có thể truy cập vào tài nguyên gì và được phép thực hiện những thao tác nào trên đó.

Lớp tiếp theo, Đăng nhập (Login), yêu cầu mỗi cá nhân khi bước vào mạng phải xuất trình Tên (User name) và Mật khẩu (Password). Đây là một cơ chế đơn giản và ít tốn kém nhưng rất hiệu quả góp phần hạn chế ngay từ ngoài những truy nhập trái phép. Mỗi người sử dụng hợp lệ đều phải có một cặp Tên – Mật khẩu, dựa vào đó hệ thống nhận biết anh ta được sử dụng những tài nguyên nào và thao tác gì trên những tài nguyên ấy.

Các phương pháp mã hóa chủ yếu dành cho các thông tin truyền trên mạng để tránh bị nghe trộm, nhưng chúng cũng được áp dụng cho việc bảo mật tại chỗ. Dữ liệu được biến đổi từ dạng tự nhiên (dễ dàng đọc hiểu) sang dạng mã hóa (không thể nhận thức được) để gửi đi, còn tại trạm nhận lại diễn ra quá trình ngược lại – giải mã.

Các cơ cấu bảo vệ vật lý nhằm ngăn chặn những thao tác sử dụng trái phép trên hệ thống. Đó là các biện pháp như: kiểm soát người ra vào phòng điều hành mạng trung tâm, lắp ổ khóa trên máy tính, sử dụng các máy trạm không có ổ đĩa để chống sao chép thông tin ...

Để bảo vệ cho mạng nội bộ, thông thường hiện nay các hệ thống mạng thường sử dụng các phần mềm Fire wall (Tường lửa). Chức năng của Fire wall là ngăn chặn những truy nhập trái phép từ môi trường mạng bên ngoài vào hệ thống nội bộ, lọc bỏ những gói tin, cấm những truy nhập trái phép theo một danh sách được quy định trước.

1.11.2. Các phương pháp mã hóa

Từ "Cryptography" (mật mã) có nguồn gốc từ các từ Hy Lạp là "crypto" (ẩn giấu) và "graphein" (viết). Các cơ chế mã hóa và giải mã có một lịch sử từ xa xưa, thời La Mã đã sử dụng những mệnh lệnh được viết bằng mật mã trong quân đội.



Giả sử: M là văn bản gốc

C là văn bản sau khi mã hóa (Ciphertext – văn bản mật mã)

E là hàm mã hóa (Encryption Function)

D là hàm giải mã (Decryption Function)

Khâu mã hóa chính là đem hàm mã hóa E tác động lên văn bản gốc M để thu được văn bản mật mã C

$$C = E(M)$$

Còn tại trạm thu diễn ra quá trình giải mã nhờ hàm giải mã D để lấy lại văn bản gốc M từ C

$$M = D(C) = D(E(M))$$

Trước đây các hàm mã hóa và giải mã được xây dựng theo hệ thống mã đối xứng hay còn gọi là hệ một khóa, trong đó khóa để làm công việc mã hóa và giải mã là như nhau. Nếu biết nắm được cách mã hóa thì cũng biết cách giải mã, do đó khóa mã hóa phải giữ bí mật tuyệt đối. Tuy nhiên hệ thống khóa như vậy tỏ ra bất tiện và hiện nay người ta thường sử dụng hệ thống khóa công khai (Public key). Trong hệ thống Public, khóa mã hóa và giải mã là khác nhau, không cái nào có thể suy ra từ cái nào. Do đó khóa mã hóa được công khai để mọi người đều có thể mã hóa và gửi dữ liệu, nhưng chỉ đúng người nhận mới giải mã nổi.

Như vậy các hệ thống mã hóa đã có được xây dựng theo một trong bốn phương pháp chủ yếu sau:

- Phương pháp chuyển dịch (Transposition Ciphers)
- Phương pháp thay thế (Substitution Ciphers)
- Phương pháp sử dụng chuẩn mật mã (DES)
- Phương pháp sử dụng khóa công khai (Public key)

1.11.3. Phương pháp chuyển dịch (Transposition Ciphers)

Trong phương pháp này, các kí tự trong văn bản gốc được dịch chuyển, sắp xếp lại để tạo ra văn bản mã hóa. Có nhiều cách dịch chuyển như sau.

– Đảo ngược toàn bộ văn bản

Chẳng hạn văn bản gốc là "HEN GAP VAO CHU NHAT TAI NHA HAT LON" được đổi thành "NOL TAH AHN IAT TAHN UHC OAV PAG NEH" không tính các khoảng trống.

Sắp xếp lại theo mẫu hình học

Ta viết lại văn bản gốc trên theo dạng bảng 4x7

Cột Dòng	1	2	3	4	5	6	7
1	H	A	O	N	T	H	T
2	E	P	C	H	A	A	L
3	N	V	H	A	I	H	O
4	G	A	U	T	N	A	N

Sau đó ta lấy các kí tự ra theo hàng ngang và thứ tự cột là 1, 4, 7, 3, 5, 2, 6 thì được văn bản mật mã là:

“HNTOTAHEHLCAPAAOHIVHGTNUNAAOTAH”

Hoán vị theo chu kì cố định

Giả sử $f()$ là một hàm hoán vị của n phần tử thì văn bản gốc gồm $2n$ kí tự

$a_1 a_2 a_3 \dots a_n a_{n+1} a_{n+2} a_{n+3} \dots a_{2n}$

sẽ được mã hóa thành

$a_{f(1)} a_{f(2)} \dots a_{f(n)} a_{n+f(1)} a_{n+f(2)} \dots a_{n+f(n)}$

Chẳng hạn, với $n = 4$ và $f(1, 2, 3, 4) = (4, 1, 3, 2)$ thì văn bản gốc “DIEN TOAN” sẽ chuyển thành “NDEI NTAO” theo bảng dưới đây

Vị trí	Kí tự gốc	Vị trí hoán vị	Kí tự mã hóa
1	D	4	N
2	I	1	D
3	E	3	E
4	N	2	I
5	T	$4 + 4 = 8$	N
6	O	$4 + 1 = 5$	T
7	A	$4 + 3 = 7$	A
8	N	$4 + 2 = 6$	O

1.11.4. Phương pháp thay thế

Dạng đơn giản nhất của phương pháp này là thay thế mỗi kí tự trong văn bản gốc bằng một kí tự trong văn bản mật mã. Như vậy là có một song ánh 1-1 giữa tập chữ của bản gốc và tập chữ của bản mật mã. Nếu biết được quy luật ánh xạ này ta sẽ nắm được cách lập mã và giải mã.

Giả sử A là bộ chữ của văn bản gốc, gồm n chữ theo thứ tự sau

$$A = \{ a_0, a_1, a_2, \dots, a_n \}$$

Gọi C là bộ chữ mật mã thì phép mã hóa chính là ánh xạ

$$f: A \rightarrow C$$

$$a_i \rightarrow f(a_i)$$

Một ví dụ nổi tiếng của phương pháp thay thế là mật mã Caesar được Julius Caesar sử dụng từ thời La Mã. Trong phép mã hóa đó, tập chữ mật mã C trùng với tập các chữ cái A. Ánh xạ f() chẳng qua chỉ là phép dịch chuyển vị trí kí tự trong bảng chữ cái với khoảng xê dịch là 3. Cụ thể, với a là một chữ cái thì kí tự mật mã tương ứng với nó được tính như sau:

$$f(a) = (a+3) \bmod n$$

với n là số chữ của bảng chữ A. Ví dụ với bảng chữ cái tiếng Anh gồm 26 chữ cái

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

thì bảng chữ mật mã Caesar tương ứng là

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Hai phương pháp mà chúng ta vừa khảo sát tương đối đơn giản và dễ bị phá khóa. Giả sử có một nhà phân tích cố gắng phá một bản mật mã theo phương pháp thay thế hay chuyển dịch. Ông ta bắt đầu bằng cách thống kê tần suất xuất hiện của các chữ trong những văn bản mật mã mà ông ta thu trộm được. Chẳng hạn ông ta thấy chữ X xuất hiện nhiều nhất. Nếu văn bản gốc là tiếng Anh thì thống kê cho thấy trong tiếng Anh chữ E xuất hiện nhiều nhất. Như vậy nhà phân tích sẽ thử thay X bằng E và cứ như vậy cho các chữ có tần suất nhỏ hơn. Còn một công cụ dò tìm nữa, đó là việc có một số từ thông dụng cũng có tần suất xuất hiện lớn, chẳng hạn từ "the" trong tiếng Anh. Như vậy là 3 chữ cái T, H, E thường đi với nhau. Điều này có nghĩa là trong văn bản mật mã, nếu gặp một từ gồm 3 chữ cái mà chữ cuối cùng là X thì nhiều khả năng đó chính là từ "the" và quan trọng hơn là hai kí tự đầu là mã hóa của chữ T và H

$$X = E, "YZX" = "THE" \Rightarrow Y = T, Z = H$$

Còn một phương pháp bẻ khóa khác là dự đoán cả một từ hay câu. Giả sử cần giải mã văn bản kế toán sau đây của một công ty tài chính

CTBMN BYCTC BTJDS QXBNS GSTJC BTSWX CTWTZ CWVUJ
QJSGS TJQSS MNQJS VLNSX VSZJU JDSTS JQUUS JUBXZ DSKSU
JSNTK BGAQJ ZBGYQ TLCTZ BNYBN QJSW

Chúng ta đều biết rằng một từ hay gặp trong chuyên môn kế toán là "FINANCIAL". Trong từ đó chữ I xuất hiện hai lần cách nhau 4 vị trí. Nhìn vào văn bản mật mã ở trên, ta thấy có 12 trường hợp trong đó một chữ cái xuất hiện hai lần cách nhau 4 vị trí. Đó là các chữ thứ 6, 15, 27, 31, 42, 48, 56, 66, 70, 71, 76, và 82. (Ví dụ như chữ B thứ 6 và S thứ 15 được in đậm ở trên). Ta lại tiếp tục nhận xét rằng trong từ "FINANCIAL", sau chữ I mà ta đang để ý là chữ N được lặp lại hai lần cách nhau một vị trí. Nhưng trong các trường hợp vừa được phát hiện chỉ có cụm thứ 31 và 42 là có tính chất này. Tiếp tục cách làm đó, ta thấy trong bản gốc chữ A cũng lặp hai lần, lần đầu nó xuất hiện giữa hai chữ N. Chỉ có cụm 31 là thỏa mãn điều này và ta có kết luận cuối cùng :

$$XCTWTZCWV = FINANCIAL$$

Do đó $X = F, C = L, T = N \dots$

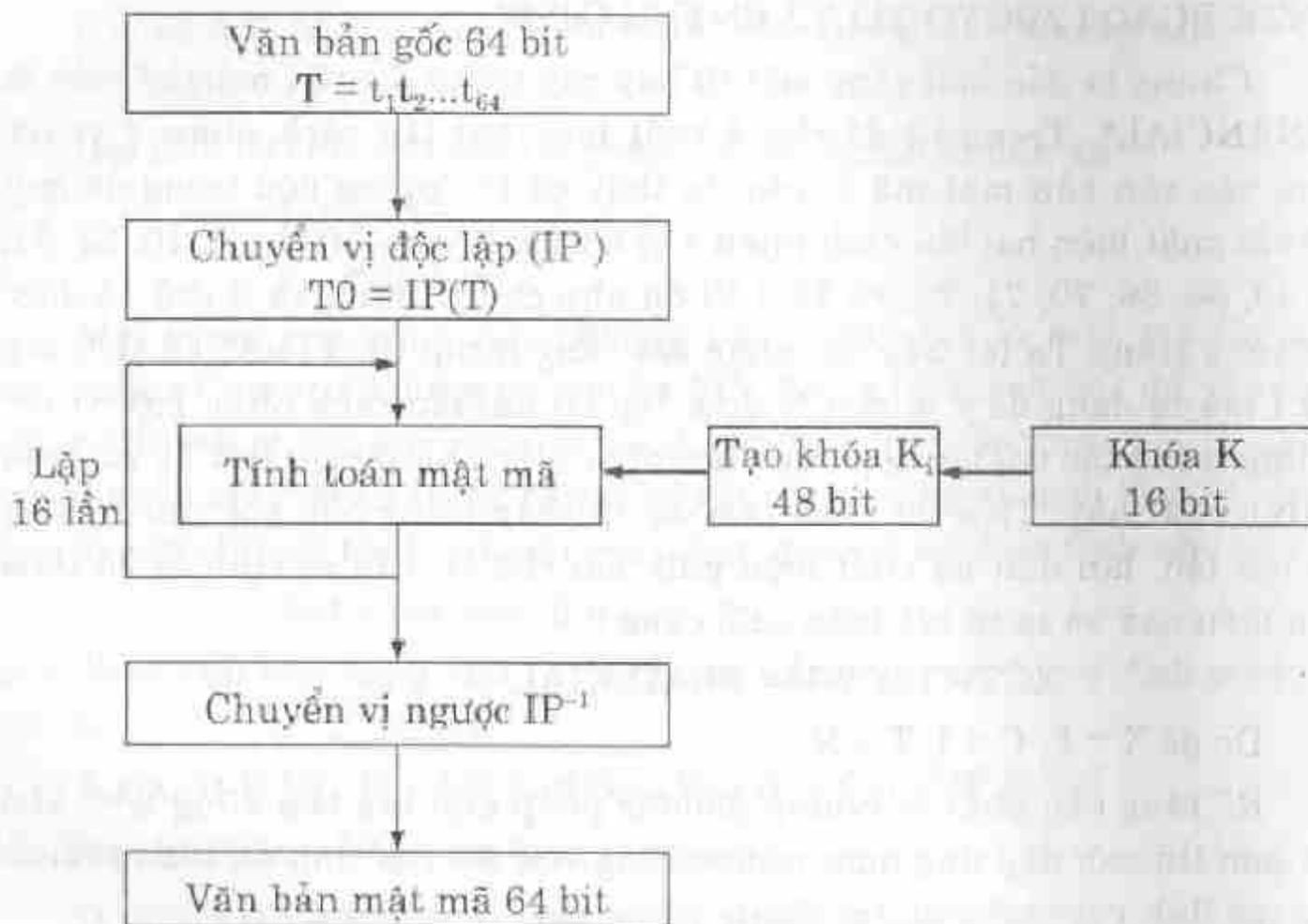
Rõ ràng cần phải có những phương pháp mật mã bền vững hơn, khó phá hơn thì mới đáp ứng được những công việc đòi hỏi tính an toàn rất cao như các lĩnh vực quân sự, tài chính, ngoại giao ...

1.11.5. Phương pháp sử dụng chuẩn mật mã (DES)

Vào tháng 1/1977, văn phòng tiêu chuẩn của Mỹ (U.S. National Bureau of Standards) công bố lấy DES làm chuẩn mã hóa dữ liệu trong các cơ quan chính phủ liên bang. DES (Data Encrypting Standard – Chuẩn mật mã dữ liệu) được phát triển bởi IBM dựa trên mật mã LUCIFER của Feistel.

Thuật toán DES mã hóa các khối 64 bit của văn bản gốc thành 64 bit mật mã dưới tác dụng của một khóa. Khóa cũng gồm 64 bit trong đó 56 bit được sử dụng trực tiếp bởi thuật toán mã hóa và 8 bit còn lại dùng để kiểm soát lỗi. Quá trình mã hóa gồm 19 công đoạn phân biệt. Bước đầu tiên là chuyển vị độc lập (IP-Initial Permutation-hoán vị khởi đầu) khóa trên văn bản gốc 64 bit. Bước cuối cùng (19) là đảo ngược chuyển vị này. Bước

18 chuyển đổi 32 bit cực trái với 32 bit cực phải. 16 bước còn lại có chức năng như nhau, thực chất chúng là các bước lặp của một hàm $f()$ bao gồm cả kĩ thuật đổi chỗ và thay thế. Thuật toán được thiết kế để cho phép việc giải mã được thực hiện cùng với khóa khi lập mật mã với các bước theo thứ tự ngược với lúc mã hóa.



Tuy DES được áp dụng rộng rãi không chỉ tại các văn phòng chính phủ Mỹ mà còn ở nhiều lĩnh vực như ngân hàng, tài chính... nhưng độ tin cậy của nó không thật đảm bảo. Có những ý kiến cho rằng độ dài 56 bit là quá ngắn. Thiết kế gốc của IBM là 128 bit đã bị chính phủ Mỹ rút lại còn 56 bit để NSA (National Security Agency – Cơ quan an ninh quốc gia) có thể phá khóa khi thấy cần thiết.

Năm 1977, hai nhà nghiên cứu mật mã là Diffie và Hellman đã thiết kế máy bẻ khóa DES và phỏng tính chi phí cho nó khoảng 20 triệu đô la, thời gian tìm ra khóa trong không gian khóa 2^{56} mất gần một ngày. Đến năm 1994, Wiener giới thiệu thiết kế chi tiết cho một máy như vậy với chi phí chỉ 1 triệu đô la, thời gian phá khóa rút xuống còn 4 giờ.

Nói chung, có hai phương pháp phá khóa thường được áp dụng là:

- Phân tích mã vi phân (Differential cryptanalysis) – do Biham và Shamir đề xuất năm 1993. Phương pháp này có thể dùng để tấn công một kĩ thuật mật mã bất kì bằng cách đưa vào các văn bản gốc chỉ khác nhau một chút và so sánh, tìm hiểu sự khác nhau trên các văn bản mật mã, từ đó tìm ra xác suất xuất hiện và các phép lập mã.

- Phân tích mã tuyến tính (Linear cryptanalysis) – do Matsui đề xuất năm 1994. Phương pháp này áp dụng toán tử XOR giữa một số bit văn bản gốc với các bit đã mã hóa. Chỉ với 2^{49} mẫu văn bản gốc thử nghiệm nó có thể bẻ khóa DES.

1.11.6. Phương pháp khóa công khai (Public – key)

Các hệ thống mật mã cổ điển (còn gọi là Hệ một khóa) có nhược điểm là khóa lập mã và khóa giải mã trùng nhau hoặc có thể dễ dàng suy ra cái nọ từ cái kia. Điều đó có nghĩa là nếu khóa lập mã bị lộ thì mọi thông điệp sẽ bị giải mã, do đó cần phải giữ bí mật khóa lập mã cũng như khóa giải mã. Nhưng trong một môi trường nhiều người sử dụng như hệ thống rút tiền tự động đặt ở nơi công cộng, điều đó rất khó thực hiện và bất tiện.

Năm 1976, hai nhà nghiên cứu ở trường Đại học Stanford là Diffie và Hellman đã đề xuất một kiểu mật mã mới trong đó khóa lập mã và khóa giải mã là hoàn toàn khác nhau, không thể suy diễn lẫn nhau được, do đó khóa lập mã có thể công khai cho mọi người biết. Về nguyên lí, khóa lập mã E và khóa giải mã D phải đáp ứng ba tiêu chuẩn sau:

- $D(E(P)) = P$
- Từ E suy ra D cực kì khó. E không thể bị bẻ khóa theo phương pháp Phân tích mã vi phân.

Một thuật toán mật mã như thế gọi là *Mật mã khóa công khai*, cơ chế áp dụng nó như sau. Ông A muốn liên hệ với nhiều người và muốn những thông điệp với họ phải được giữ bí mật. Ông ta xây dựng 2 khóa, khóa lập mã E và khóa giải mã D, rồi công bố công khai E, còn D giữ bí mật. Bằng cách đó tất cả những người muốn gửi thông điệp cho A sẽ dùng E để mã hóa thông điệp của mình rồi gửi cho A và đảm bảo rằng không ai giải mã nổi vì không biết D.

Tiện lợi của thuật toán khóa công khai ở chỗ, nếu như E được công bố

trên Internet chẳng hạn, thì bất kì ai cũng có thể mã hóa thông điệp của mình để gửi cho A mà không cần phải gặp gỡ trao đổi gì với A trước đó, và A cũng không cần phải yêu cầu mọi người giữ bí mật một khóa nào cả.

Thuật toán RSA

Một đại diện tiêu biểu của mã khóa công khai, RSA, do nhóm ba nhà phát minh của MIT đề xuất. Đó là Rivest, Shamir và Adleman và RSA là tên ghép ba chữ cái đầu tên của họ. Thuật toán dựa trên nhận xét sau đây: cho biết hai số nguyên tố thì có thể dễ dàng tìm ra tích của chúng, nhưng làm điều ngược lại – tức là phân tích một số thành tích hai thừa số nguyên tố – thì cực kì khó khăn nếu như hai số nguyên tố ban đầu rất lớn.



Leonard Adleman

Phương pháp RSA có thể tóm tắt như sau:

1. Chọn 2 số nguyên tố lớn p và q (thường lớn hơn 10^{100})
2. Tính $n = p \times q$ và hàm Öle $\Phi(n) = (p - 1) \times (q - 1)$
3. Chọn một số k nguyên tố cùng nhau với $\Phi(n)$
4. Tính số D sao cho $E \times D = 1$ (môđun $\Phi(n)$). Có thể dùng giải thuật Oclid thực hiện việc này không mấy khó khăn.

Với các tham số đã tính sẵn này, ta có thể bắt đầu quá trình lập và giải mã. Chọn K làm khóa công khai cùng với n còn D là khóa bí mật. Biểu diễn văn bản gốc dưới dạng một dãy số nguyên nằm trong đoạn $[1, n-1]$. kí hiệu dãy số đó là P thì văn bản mật mã C được tạo ra theo công thức

$$C = PE \text{ (môđun } n)$$

Quá trình giải mã tiến hành ngược lại. Khi nhận được C , ta tính

$$P = CD \text{ (môđun } n)$$

Ví dụ:

Chọn hai số nguyên tố $p = 5, q = 7$.

Tính $n = pq = 35$

Tính $\Phi(n) = (p - 1).(q - 1) = 24$

Chọn $E = 5$ vì $(5, 24) = 1$

$D = E^{-1} \bmod 24 = 5$

Giả sử văn bản gốc $P = 2$. Lập mật mã: $C = PE \bmod n = 2^5 \bmod 35 = 32$

Giải mã. Tính $P = CD \bmod n = 32^5 \bmod 35 = 2$. Ta lại thu được bản gốc P .

Thuật toán Balô

Đây cũng là một mật mã khóa công khai, tuy không nổi tiếng và mạnh như RSA. Thuật toán này được hai tác giả Merkle và Hellman công bố năm 1978. Ý tưởng chính của nó tương tự như bài toán xếp balô. Một người có một số lớn đồ vật với trọng lượng khác nhau, để lập mã chủ nhân chọn lựa một số đồ vật trong đó và xếp vào balô. Tổng trọng lượng balô được công khai, còn danh sách các đồ vật được giữ bí mật.



Ron Rivest



Ralph Merkle

Nhà phát minh ra thuật toán, Ralph Merkle, quả quyết rằng không thể phá khóa mật mã này được và đặt giải thưởng 100 USD cho ai làm được điều đó. Adi Shamir (người ứng với chữ S trong RSA) phá được và lấy giải. Không nhụt chí, Merkle cải tiến lại cho mật mã khó hơn và treo giải 1000 USD. Ron Rivest (chữ R trong RSA) lại bẻ được khóa và lĩnh giải. Cuối cùng Merkle đã không đặt giải 10 000 USD cho phiên bản tiếp theo nữa và "A" (Leonard Adleman) mất vận may.

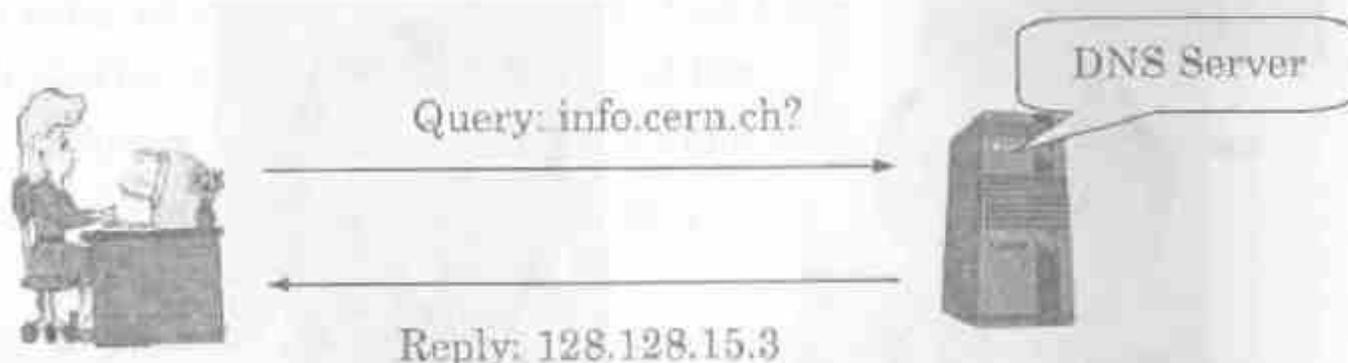
1.11.7. Hệ thống tên miền DNS (Domain Name System)

Trên những mạng diện rộng, như Internet chẳng hạn, số máy trạm lên đến hàng triệu cái và việc quản lí tên của chúng trở thành một vấn đề.

Người ta đã sử dụng DNS để giải quyết vấn đề này.

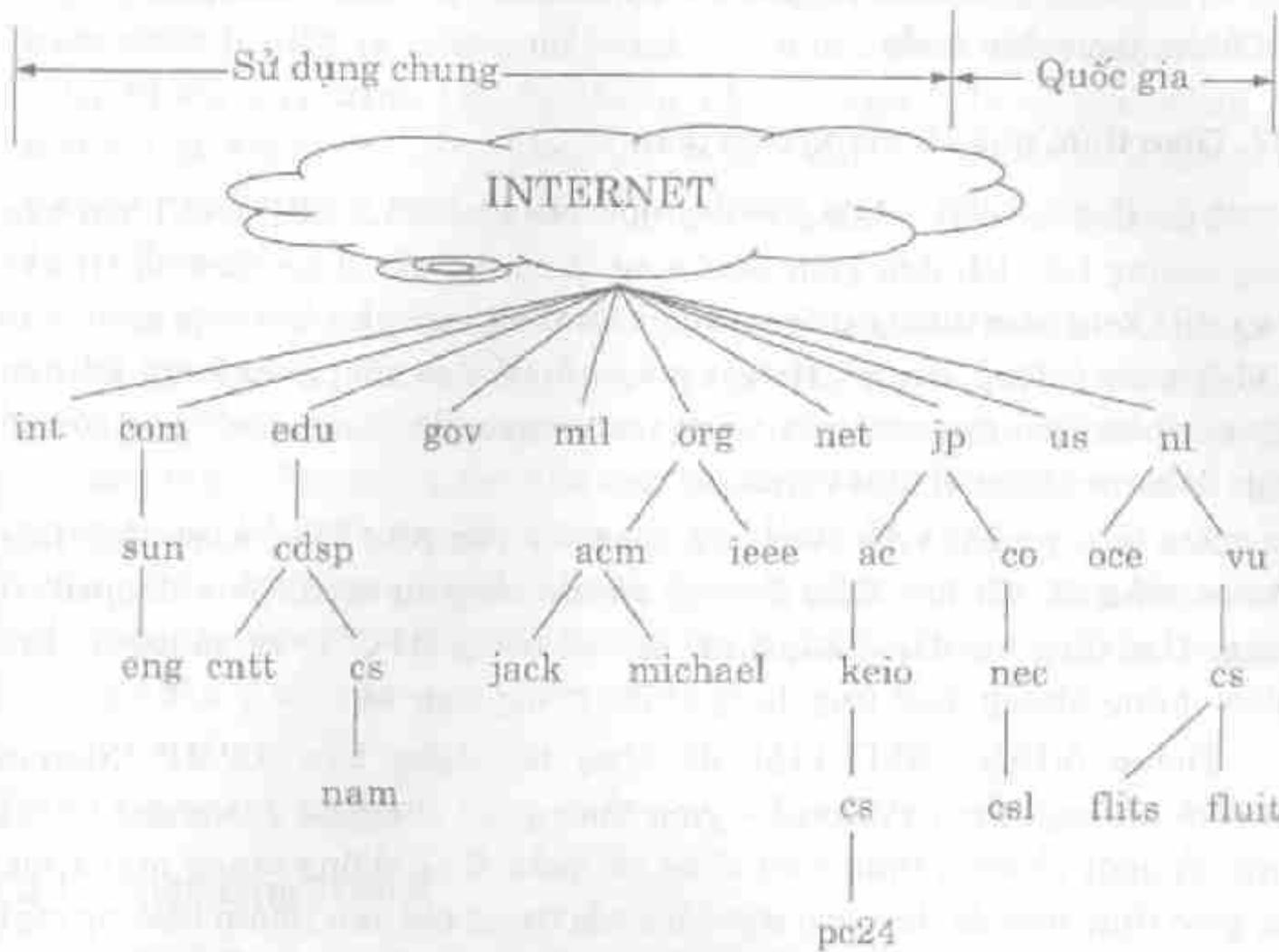
Bản chất hệ thống tên miền DNS là một hệ phân cấp, một sơ đồ đặt tên có tính kế thừa dựa trên miền và một cơ sở dữ liệu phân tán để lưu trữ sơ đồ này trên nhiều máy gọi là DNS server. DNS được ưu tiên sử dụng để ánh xạ tên các trạm và các địa chỉ nhận e-mail vào tập các địa chỉ IP và còn được dùng cho một số mục đích khác.

Cơ chế hoạt động của DNS có thể tóm tắt như sau. Để ánh xạ một tên máy trạm thành một địa chỉ IP, một chương trình ứng dụng gọi một thủ tục thư viện tên là resolver với tham số chính là tên trạm. Resolver gửi thông báo đến một DNS Server – là nơi chứa một bản sao của cơ sở dữ liệu tên miền. Server này dò tìm tên trạm trong cơ sở dữ liệu và trả lại địa chỉ IP tương ứng.



Không gian tên miền

Trong ngành bưu chính, việc quản lý tên yêu cầu các lá thư, bưu kiện gửi hàng ... phải ghi rõ địa chỉ người gửi cũng như người nhận theo hệ thống phân cấp hành chính như: Tên quốc gia, tên tỉnh, huyện, xã, thôn, tên người. Không gian tên miền cũng vậy. Hãy lấy Internet làm ví dụ. Hệ thống tên của mạng Internet gồm nhiều cấp, cấp trên cùng chia thành hàng trăm miền, mỗi miền lại chứa các miền con và cứ phân chia như vậy. Ta hình dung hệ thống này như một cây, các lá tận cùng tượng trưng cho một trạm hoặc cho một mạng nội bộ công ti với nhiều trạm.



Các tên miền quốc gia đại diện cho từng đất nước, chẳng hạn như vn cho Việt Nam, jp cho Nhật Bản..., được quy định rõ trong bộ chuẩn ISO 3166.

Các tên miền sử dụng chung (generic) gồm

- int (certain international organization): các tổ chức quốc tế
- com (comercial): các tổ chức, cơ quan, công ti.
- edu (education institution): các cơ quan giáo dục, viện, trường đại học
- gov (government): các tổ chức, văn phòng cơ quan chính phủ
- net (network provider): những công ti, nhà cung cấp dịch vụ mạng
- org (non profit organization): tổ chức, cơ quan

Mỗi miền được đặt tên dựa trên đường dẫn từ lá đến gốc, các thành phần ngăn cách nhau bởi dấu chấm. Ví dụ tên miền của phòng kĩ thuật công ti Sun Microsystem là **eng.sun.com**.

Các tên miền có thể là tuyệt đối (kết thúc bởi dấu chấm như ví dụ trên) hoặc là tương đối (không có dấu chấm cuối). Các tên miền tương đối

phải đi kèm với ngữ cảnh để phân biệt. Chữ hoa và chữ thường có ý nghĩa như nhau trong tên miền.

1.12. Giao thức quản lí mạng đơn giản

Vào thời kì đầu, những mạng quy mô nhỏ như ARPANET chỉ cần dùng những tiện ích đơn giản như *ping* là có thể xác định được vị trí xảy ra sự cố. Ví dụ như đường truyền đứt, một thiết bị mạng hay một trạm nào đó không hoạt động, các gói tin mà *ping* gửi đến sẽ không được trả lời, căn cứ vào nhân thời gian mà các trạm trung gian đã đánh dấu cũng có thể phán đoán ra phạm vi khu vực có sự cố.

Khi mạng phát triển lên quy mô toàn cầu như hiện nay, cách làm trên rõ ràng đã bất lực. Cần phải có những công cụ mạnh hơn để quản lí mạng. Hai công cụ đầu tiên, được mô tả trong RFC 1028 và 1067, tuy nhiên chúng không được ứng dụng nhiều trong thực tế.

Tháng 5/1990, RFC 1157 đã công bố phiên bản *SNMP* (*Simple Network Management Protocol – giao thức quản lí mạng đơn giản*) nhằm cung cấp một phương thức điều động và quản lí hệ thống mạng máy tính. Các giao thức này đã được cài đặt rộng rãi trong các sản phẩm thương mại và trở thành một tiêu chuẩn thực tế cho việc quản lí mạng. Sau đó, phiên bản *SNMPv2* tiếp theo – được định nghĩa trong RFC 1441 đến 1452 – đã đưa *SNMP* trở thành chuẩn cho Internet.

Mô hình SNMP

Theo mô hình *SNMP*, mạng chia thành các thành phần:

- Các nút được quản lí
- Các trạm làm công việc theo dõi, điều hành mạng
- Những thông tin phục vụ cho việc điều hành mạng
- Các giao thức quản lí mạng

Các nút được quản lí có thể là các trạm đầu cuối, các máy trạm, router, bridge, máy in mạng ... Nói chung đó là bất kì thiết bị mạng nào có khả năng nhận biết và báo cáo những thông tin về trạng thái hoạt động của chính mình. Để được quản lí bởi hệ thống *SNMP*, thiết bị đó phải có khả năng chạy một phần mềm quản lí gọi là *SNMP agent*. Mỗi agent sẽ theo dõi và duy trì một cơ sở dữ liệu về trạng thái hoạt động của thiết bị mà nó theo dõi.

Việc quản lý mạng được thực hiện bởi các Management station – trạm quản lý. Đây là những máy tính có cài đặt phần mềm quản lý SNMP chứa nhiều quá trình truyền thông với các agent đang hoạt động trên mạng. Các agent báo cáo thông tin trạng thái về trạm quản lý, trạm này theo dõi tình trạng hoạt động và ra những mệnh lệnh cần thiết cho các agent thi hành.

Có một vấn đề là các thiết bị hoạt động trên mạng có thể có rất nhiều nguồn gốc, do nhiều hãng khác nhau sản xuất. Để chúng có thể giao tiếp được với trạm quản lý, phải có những giao thức quy định khuôn dạng thông tin và những lĩnh vực hoạt động của từng thành phần trong hệ thống quản lý mạng. SNMPv2 đã sử dụng một ngôn ngữ định nghĩa đối tượng chuẩn tên là ASN-1 (Abstract Syntax Notation 1) để chuẩn hóa việc trao đổi thông tin giữa các thành phần trong hệ thống quản lý mạng.

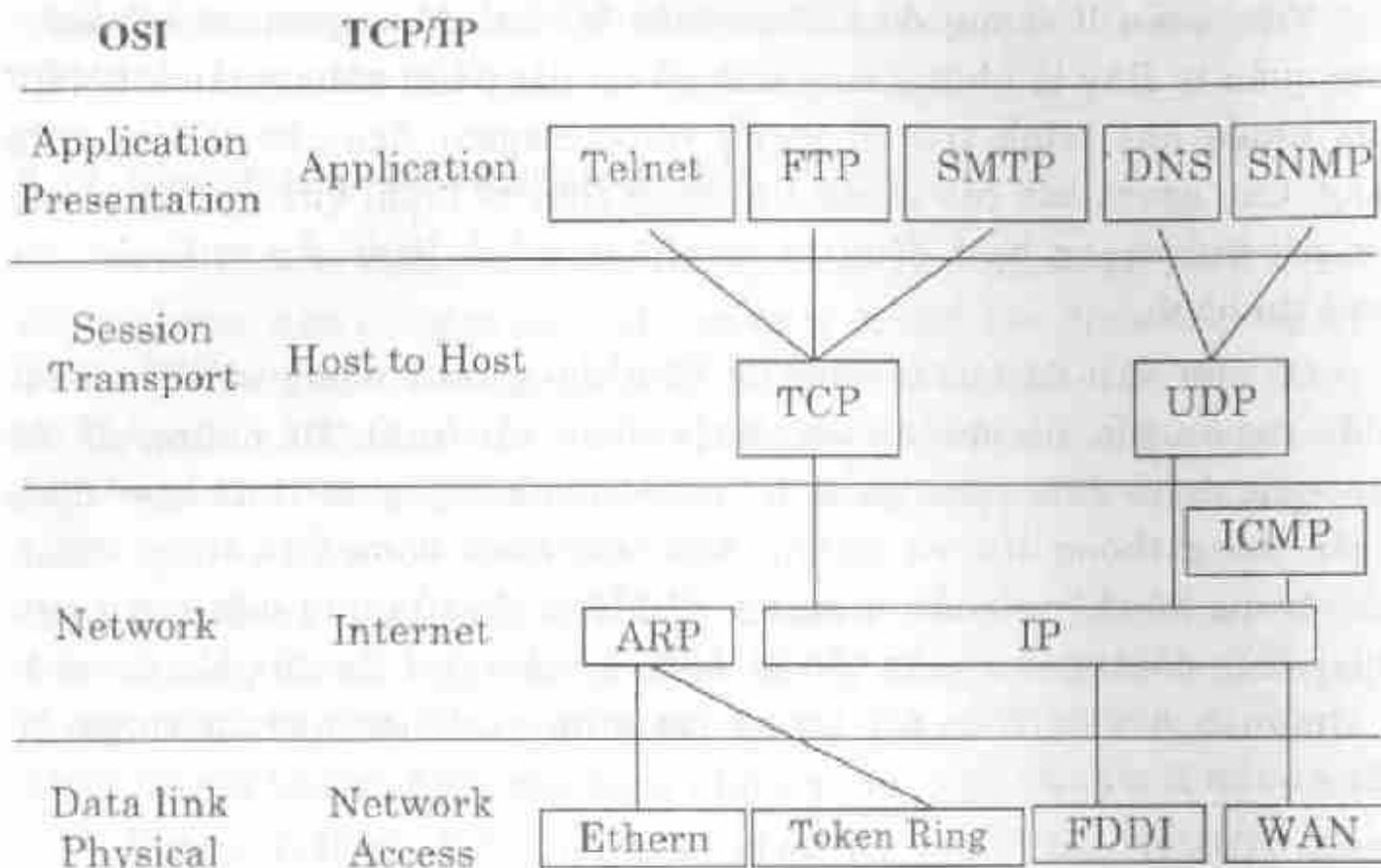
2. MÔ HÌNH TCP/IP

2.1. Phân tầng TCP/IP

Ngày nay chúng ta đều biết đến mạng Internet. Giao thức chủ yếu được sử dụng trên Internet là TCP/IP và lịch sử ra đời của Internet và TCP/IP gắn liền với Bộ Quốc phòng Mỹ nên mô hình TCP/IP đôi khi còn được gọi là DoD (Department of Defense).

Hình vẽ sau đây cho ta thấy sự tương đương về chức năng giữa các tầng trong hai mô hình: OSI và TCP/IP.

Mô hình TCP/IP gồm bốn tầng. Tầng dưới cùng là Network Access (tầng truy nhập mạng). Tầng này đại diện cho các bộ phận kết nối vật lý như cáp, bộ chuyển đổi transceiver, NIC, các giao thức truy nhập mạng như CSMA/CD hay Token Ring...



Tầng Internet chịu trách nhiệm cung cấp một địa chỉ logic cho giao diện vật lý của mạng. Giao thức được sử dụng trong tầng này là IP (Internet Protocol). Tầng này hỗ trợ một ánh xạ giữa địa chỉ logic và địa chỉ vật lý do tầng trên cung cấp bằng cách sử dụng các giao thức ARP (Address Resolution Protocol: giao thức phân giải địa chỉ) và RARP (Reverse Address Resolution Protocol: giao thức phân giải địa chỉ đảo). Các vấn đề như thông tin chẩn đoán lỗi, các tình huống bất thường liên quan đến giao thức IP được thống kê và báo cáo thông qua giao thức ICMP (Internet Control Message Protocol: giao thức điều khiển thông điệp Internet). Tầng Internet cũng tham gia vào việc định tuyến các gói tin giữa các host trên mạng.

Tầng phía trên, Host to Host hay còn gọi là tầng Transport, thực hiện việc kết nối hai host trên mạng. Hai giao thức tại tầng này là TCP (Transmission Control Protocol: Giao thức điều khiển việc truyền dữ liệu) và UDP (User Datagram Protocol: Giao thức đối với gói tin). TCP chịu trách nhiệm về độ tin cậy, tính đồng thời và kết nối song công. Độ tin cậy được TCP đảm bảo bằng cách yêu cầu truyền lại khi phát hiện lỗi. Ngoài ra TCP còn hỗ trợ những kết nối đồng thời, nhiều kết nối TCP có thể được

thiết lập tại một host và dữ liệu được truyền đồng thời, song song và độc lập trên những kết nối đó.

Giao thức UDP là giao thức thiếu tin cậy và không kết nối. Nó không mạnh như TCP và được sử dụng bởi những ứng dụng không đòi hỏi tính tin cậy cao như TCP.

Tầng ứng dụng Application chứa tất cả các giao thức bậc cao hơn và hỗ trợ các ứng dụng sử dụng những giao thức của tầng Host to Host, ví dụ như FTP – File Transfer Protocol: ứng dụng truyền các file, TE – Terminal Emulation: giả lập thiết bị đầu cuối, SMTP – Simple Mail Transfer Protocol : thư điện tử, Telnet: cho phép người sử dụng ngồi tại một trạm và đăng nhập vào một trạm khác ở xa để làm việc.

2.2. Bộ giao thức TCP/IP

Các giao thức TCP/IP được định nghĩa bởi RFC (Request for Comments: yêu cầu khuyến nghị) và số hiệu chuẩn (Standard number). Trong đó không phải tất cả RFC đều là các định nghĩa mà một số chỉ là các chuẩn thử nghiệm, khuyến nghị. Các hãng sản xuất phải tuân theo các chuẩn Internet chính thức, vào thời điểm 1997 RFC mô tả danh sách chuẩn Internet chính thức là RFC 1600. Sau đây là một số chuẩn quan trọng trong đó.

Tên chuẩn	Số hiệu chuẩn	RFC	Tầng TCP/IP
File Transfer Protocol (FTP)	9	959	Application
Telnet Protocol (TELNET)	8	854,855	Application
Trivial File Transfer Protocol (TFTP)	33	1350	Application
Simple Mail Transfer Protocol (SMTP)	10	821	Application
Simple Network Management Protocol (SNMP)	15	1157	Application
Domain Name System (DNS)	13	1034, 1035	Application
Transmission Control Protocol (TCP)	7	793	
User Datagram Protocol (UDP)	6	768	
Internet Protocol (IP)	5	791	

CÂU HỎI CUỐI CHƯƠNG

1. Vì sao phải xây dựng bộ tiêu chuẩn mạng?
2. Những nguyên lý của kiến trúc phân tầng là gì?
3. Nêu vai trò, chức năng của tầng Vật lý. Phân biệt hai khái niệm DTE và DCE.
4. Nêu vai trò, chức năng của tầng Liên kết dữ liệu.
5. Trình bày phương pháp phát hiện lỗi Chẵn lẻ, Kiểm tra vòng, mã Hamming.
6. Trình bày về Ethernet, so sánh khuôn dạng frame Ethernet II với IEEE 802.3.
7. Nêu vai trò, chức năng của tầng Mạng.
8. Phân biệt và so sánh kỹ thuật chọn đường Phân tán và Tập trung.
9. Trình bày, so sánh các phương pháp truy nhập đường truyền ALOHA, CSMA/CD.
10. Hiện tượng tắc nghẽn: nguyên nhân và các phương pháp kiểm soát.
11. Nêu vai trò, chức năng của tầng Giao vận.
12. Nêu vai trò, chức năng của tầng Phiên.
13. Tóm tắt các dịch vụ được cung cấp ở tầng Phiên.
14. Phân biệt khái niệm Điểm đồng bộ chính và phụ.
15. Nêu vai trò, chức năng của tầng Trình diễn.
16. Nêu vai trò, chức năng của tầng Ứng dụng.
17. Nêu những hình thức xâm hại an ninh mạng chủ yếu.
18. Tóm tắt ý tưởng chính của các phương pháp mã hóa.
19. Thế nào là không gian tên miền? Giải thích thuật ngữ SNMP.
20. Phân biệt và so sánh hai mô hình OSI và TCP/IP.

Điền từ (cụm từ) thích hợp vào chỗ trống

1. Trong mô hình kiến trúc phân tầng, mỗi tầng cung cấp dịch vụ cho tầng và che giấu những chi tiết về cách thực hiện dịch vụ đó.
2. Tại mỗi tầng, gói dữ liệu được bổ sung thêm thông tin định dạng hay

3. Mỗi tầng hoạt động như thế nó đang giao tiếp trực tiếp với tầng nguồn..... trên máy tính đầu bên kia.
4. Ở trạm phát, tầng trình diện..... diễn dịch dữ liệu từ tầng Ứng dụng gửi xuống sang Transfer syntax.
5. Tầng truyền..... quyết định đường đi của gói dữ liệu từ trạm nguồn đến trạm đích.
6. Tầng Liên kết dữ liệu gửi chúng đi..... từ tầng Network xuống tầng Vật lí.
7. Tầng vật lí..... quy định cáp được gắn vào NIC như thế nào.
8. Mô hình 802 chia tầng dữ liệu..... của mô hình OSI thành hai tầng con LLC và MAC.
9. Tầng con MAC..... giao tiếp trực tiếp với NIC và chịu trách nhiệm chuyển dữ liệu không lỗi giữa hai trạm.
10. Phần thông tin trong khung dữ liệu cho biết loại khung, đường đi và thông tin về vị trí phân đoạn.
11. Phân mục IEEE bao gồm các tiêu chuẩn mạng cục bộ cho Ethernet.

1. ...
 2. ...
 3. ...
 4. ...
 5. ...
 6. ...
 7. ...
 8. ...
 9. ...
 10. ...
 11. ...
 12. ...
 13. ...
 14. ...
 15. ...
 16. ...
 17. ...
 18. ...
 19. ...
 20. ...

21. ...
 22. ...
 23. ...
 24. ...
 25. ...

Chương 4

GIAO THỨC

Chương này mô tả khái niệm giao thức (protocol) trong các hoạt động của mạng; tập trung giải thích vai trò của giao thức và mô tả phương thức hoạt động của các giao thức.

1. CHỨC NĂNG CỦA GIAO THỨC

Ta xem xét một thế giới bao gồm rất nhiều những quốc gia khác nhau, mỗi quốc gia hoạt động theo một thể chế khác nhau, để các quốc gia này tiếp xúc được với nhau cần phải có những quy tắc chung về giao tiếp trong các hoạt động ngoại giao. Mạng máy tính cũng vậy, mỗi máy tính (quốc gia) có thể hoạt động với những hệ điều hành (thể chế) khác nhau giao tiếp với nhau trên mạng phải tuân thủ những quy tắc thống nhất, từ khuôn dạng (cú pháp, ngữ nghĩa) của dữ liệu đến các thủ tục gửi nhận, kiểm soát, xử lý lỗi, ... *Giao thức mạng (protocol)* là tập hợp những quy tắc, quy ước điều khiển sự giao tiếp và tương tác giữa các máy tính trong mạng.

Trong phần trước, khi nghiên cứu về mô hình OSI chúng ta đã biết rằng hoạt động truyền dữ liệu trên mạng phải được chia làm nhiều bước tách biệt trong một hệ thống thống nhất. Tại mỗi bước một số hoạt động nhất định phải diễn ra và hoạt động đó chỉ diễn ra ở bước đó chứ không lặp lại ở một bước nào khác. Mỗi bước đều có giao thức riêng, hoạt động theo trình tự nhất quán trên mỗi máy tính trong mạng. Tại máy tính gửi các bước được thực hiện theo trình tự các tầng từ trên xuống, tại máy tính nhận các bước được thực hiện theo trình tự ngược lại. Ví dụ, ta xem xét các hoạt động cụ thể truyền dữ liệu giữa hai máy tính, một máy gửi còn máy kia nhận.

• Máy gửi

Giao thức quy định:

- Nhận dữ liệu từ chương trình ứng dụng.
- Chia dữ liệu thành các gói.

- Thêm thông tin vào gói, mỗi tầng thêm thông tin xử lý cho tầng đó.

- Chuyển gói dữ liệu lên cấp mạng qua NIC.

• **Máy nhận**

Giao thức quy định:

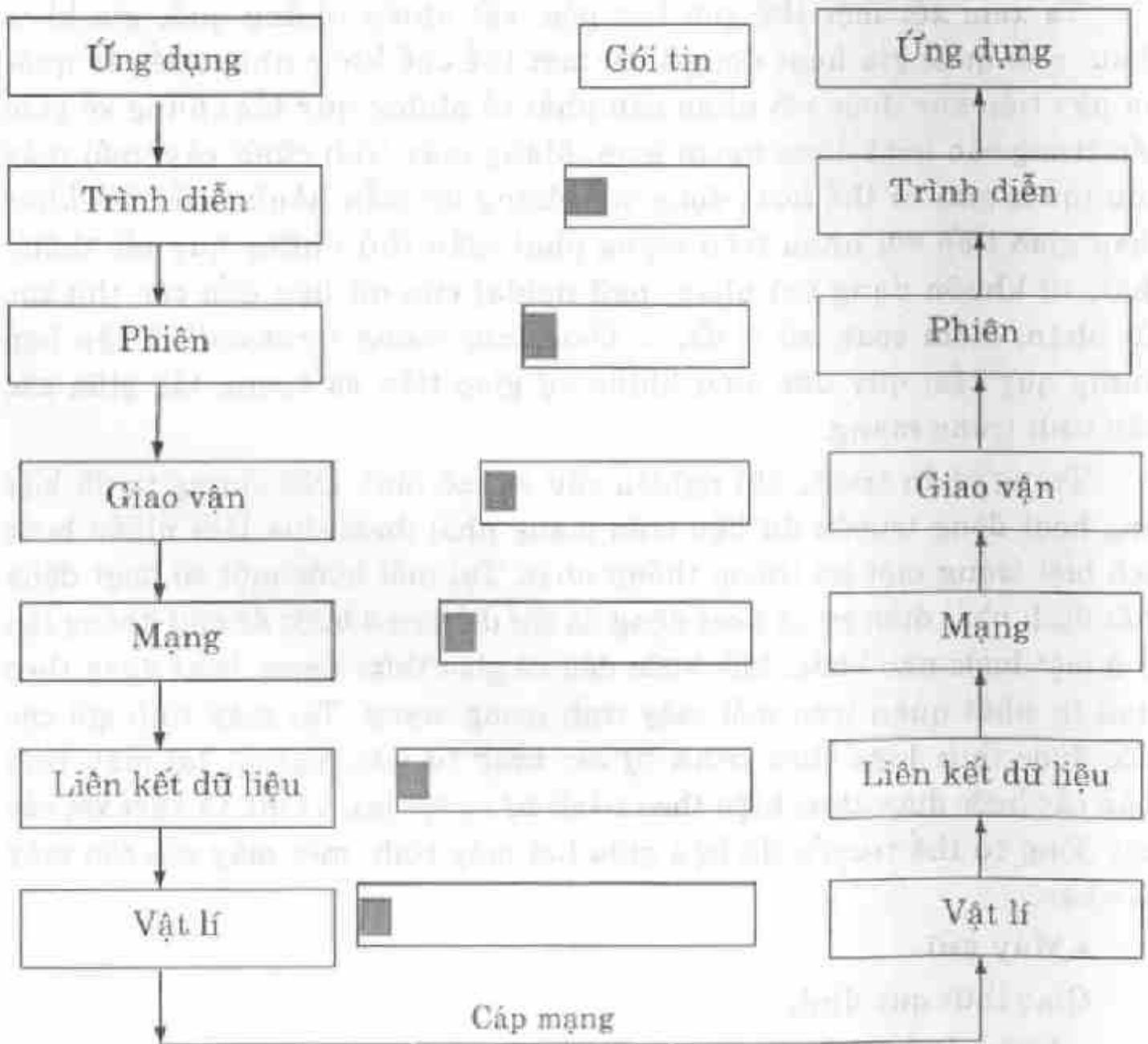
- Lấy gói dữ liệu từ cấp mạng qua NIC.

- Tước bỏ thông tin trong gói tương ứng với từng phần.

- Lắp ghép các gói thành dữ liệu gốc.

- Chuyển dữ liệu cho chương trình ứng dụng.

Các thủ tục ở máy gửi và máy nhận đều được thực hiện theo cùng một quy tắc để đảm bảo dữ liệu nhận được không thay đổi so với dữ liệu gốc.



Hình 4.1. Lược đồ truyền dữ liệu giữa 2 máy

Trên mạng máy tính có nhiều loại giao thức, mỗi giao thức cho phép thực hiện một loại giao tiếp cơ bản, có mục đích khác nhau và thi hành những tác vụ khác nhau. Mỗi giao thức đều có những ưu, nhược điểm riêng của chúng.

Một số giao thức hoạt động ở nhiều tầng khác nhau. Tại mỗi tầng chức năng của giao thức được hoạt động ở tầng đó quy định. Chẳng hạn, một giao thức nào đó hoạt động ở tầng Vật lý có nghĩa là tại tầng này giao thức đảm bảo cho gói dữ liệu đi qua NIC lên đường truyền và ngược lại.

Nhiều giao thức có thể hoạt động phối hợp với nhau, chúng được tập hợp với nhau thành một dãy (suite) hay còn gọi là một *chồng giao thức (protocol stack)*. Sự phối hợp hoạt động của chồng giao thức cũng giống như hoạt động của các tầng trong mô hình OSI, mỗi giao thức trong chồng được thực hiện ở những cấp độ khác nhau. Cấp độ giao thức trong chồng tương ứng với tầng của mô hình OSI.

Trong những mạng máy tính lớn có nhiều mạng cục bộ nối với nhau, dữ liệu truyền từ mạng cục bộ này đến mạng cục bộ khác có thể đi qua nhiều đường khác nhau, ta gọi là các đường đã định tuyến. Giao thức cho phép truyền thông *đa tuyến* từ mạng cục bộ này đến mạng cục bộ khác được gọi là giao thức *có thể phân định đường truyền (routable)*. Ngược lại, giao thức nào chỉ cho phép đi theo một tuyến cố định gọi là giao thức không có khả năng phân định đường truyền (*nonroutable*). Các giao thức routable hiện nay đã trở thành phổ biến.

2. GIAO THỨC TRONG KIẾN TRÚC PHÂN TẦNG

Trong một mạng mà các hoạt động của nó được thực hiện bởi một dãy các giao thức phối hợp với nhau thì các giao thức phải được hoạch định để sự phối hợp không xảy ra xung đột hoặc xảy ra những hoạt động không hoàn chỉnh. Phương pháp hoạch định tốt nhất là *phân tầng (layering)* các giao thức, giao thức được xếp *chồng*. Tại mỗi tầng định rõ một giao thức chuyên đảm trách một chức năng của quá trình giao tiếp.

Tầng Ứng dụng	Khởi xướng hoặc chấp nhận một yêu cầu.
Tầng Trình diễn	Thêm thông tin định dạng, hiển thị và mã hóa.
Tầng Phiên	Thêm thông tin luồng lưu lượng nhằm xác định thời điểm gửi dữ liệu.
Tầng Giao vận	Thêm thông tin xử lý lỗi.
Tầng Mạng	Thêm thông tin thứ tự và địa chỉ vào gói.
Tầng Liên kết dữ liệu	Thêm thông tin kiểm tra lỗi và chuẩn bị dữ liệu cho kết nối vật lý.
Tầng Vật lý	Gói dữ liệu được gửi dạng luồng bit.

Hình 4.2. Chức năng của giao thức ở mỗi tầng

Kiến trúc của chồng giao thức là tương đương với mô hình OSI, các tầng thấp trong chồng giao thức định rõ cách các thiết bị của một hãng này kết nối được với các thiết bị của hãng khác. Tầng cao xác định rõ nguyên tắc thực hiện phiên giao dịch và giao tiếp với chương trình ứng dụng.

Quy trình liên kết (binding process) cho phép thiết lập mạng với mức độ linh hoạt rất cao. Trong quy trình này, hai chồng giao thức khác nhau có thể cùng liên kết với một NIC, nếu máy tính của chúng ta có nhiều hơn một NIC thì một chồng có thể liên kết với nhiều NIC. Chẳng hạn chúng ta cài đặt cả hai giao thức IPX/SPX và TCP/IP thì cả hai chồng này có thể dùng chung một NIC.

Quy trình liên kết còn quy định cả thứ tự liên kết, hệ điều hành sẽ căn cứ vào thứ tự liên kết để chạy giao thức trong trường hợp nhiều chồng giao thức được cài đặt. Chẳng hạn nếu máy tính của ta cài đặt các chồng giao thức theo thứ tự là NetBEUI – TCP/IP – IPX/SPX thì khi liên kết máy sẽ thử dùng giao thức đầu tiên là NetBEUI, nếu kết nối với giao thức này thất bại thì các giao thức kế tiếp sẽ được dùng.

Liên kết không bị giới hạn bởi chồng giao thức đang liên kết với NIC, giao thức tại một tầng của chồng này có khả năng liên kết, phối hợp với giao thức của các chồng giao thức khác tại các tầng trên hoặc dưới nó.

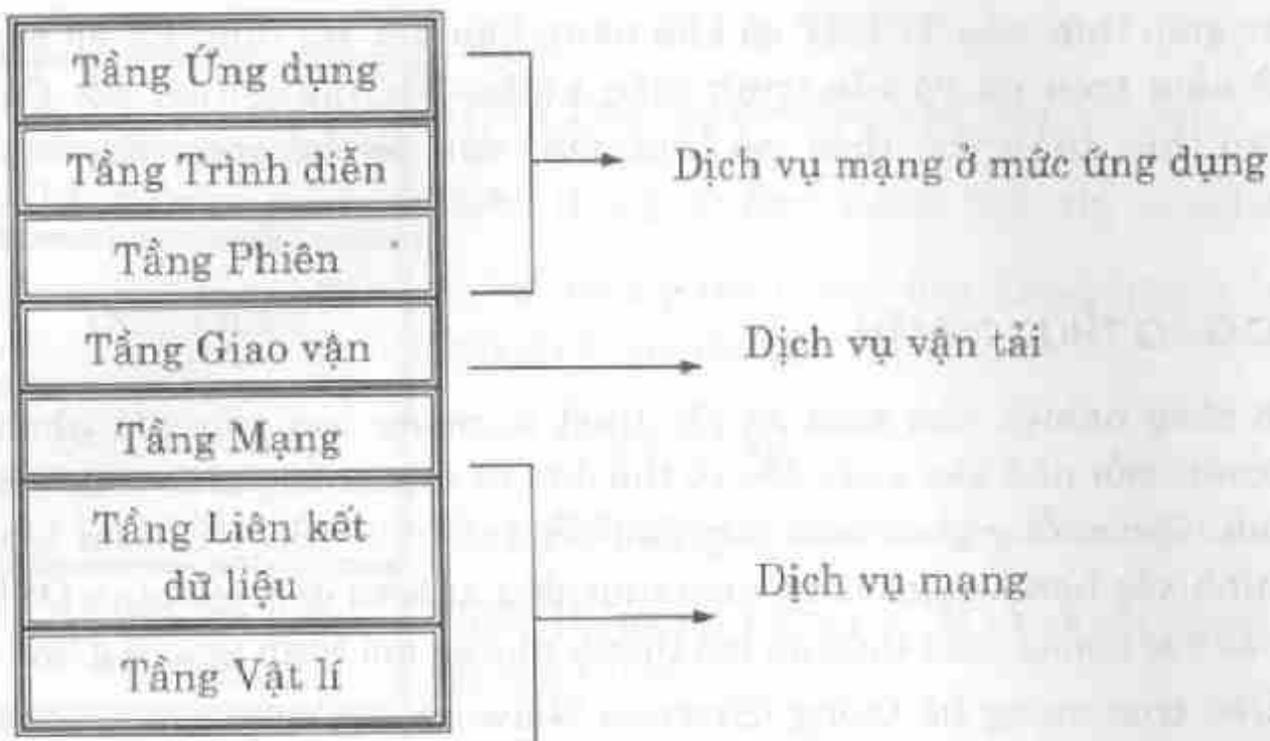
Ví dụ, các giao thức của TCP/IP có khả năng liên kết với tầng Phiên của NetBIOS nằm trên nó và các trình điều khiển NIC nằm dưới nó. Các chồng giao thức tuân thủ theo mô hình OSI đều có thể giao tiếp được với nhau.

3. CÁC GIAO THỨC CHUẨN

Nền công nghiệp sản xuất ra các thiết bị mạng bao gồm rất nhiều nhà sản xuất, mỗi nhà sản xuất đều có thể đưa ra một chồng giao thức của riêng mình. Các chồng giao thức này đều lấy mô hình ISO/OSI làm tiêu chuẩn, chính xác hơn là các chồng giao thức đều ánh xạ đến mô hình OSI. Hiện nay có các chồng giao thức đã trở thành những mô hình chuẩn gồm:

- Kiến trúc mạng hệ thống (Systems Network Architecture – SNA) của IBM.
- Digital DECnet™.
- Novell NetWare
- Apple AppleTalk®
- Dây giao thức Internet, TCP/IP

Trong các chồng giao thức này, những tác vụ truyền thông cần thi hành qua mạng được thực hiện bởi một trong ba loại giao thức tương ứng với các lớp trong mô hình OSI là: Ứng dụng (Application), Giao vận (Transport), Mạng (Network).



Hình 4.3. Chồng giao thức trong mô hình OSI

• Giao thức Ứng dụng (Application protocol)

Các giao thức ứng dụng hoạt động trong các tầng cao của mô hình OSI, cung cấp các khả năng tương tác giữa các chương trình ứng dụng và trao đổi dữ liệu, bao gồm:

- APC (Advanced Program-to-Program Communication) trong chồng giao thức SNA của IBM. Chồng giao thức này chủ yếu dùng trong hệ thống máy AS/400@s.
- FLAM (File Access and Management), giao thức truy nhập tệp của mô hình OSI.
- X.400, giao thức CCITT dùng cho việc truyền e-mail.
- X.500, giao thức CCITT dùng cho dịch vụ tệp và thư mục ngang qua nhiều hệ thống.
- SMTP (Simple Mail Transfer Protocol), giao thức Internet cho việc truyền e-mail.
- FTP (File Transfer Protocol), giao thức truyền tệp trên Internet.
- SNMP (Simple Network Management Protocol), giao thức Internet dùng cho việc theo dõi mạng và các thành phần trên mạng.
- Telnet, giao thức Internet dùng cho việc đăng nhập máy chủ ở xa và xử lý dữ liệu trên máy cục bộ.

- Microsoft SMB (Server Message Blocks) bộ đối hướng trên máy khách.
- NCP (Novell NetWare Core Protocol) bộ đối hướng trên máy khách của Novell.
- Apple Talk và Apple Share[®], dây giao thức mạng của Apple.
- AFP (Apple Talk Filing Protocol), giao thức dùng cho việc truy nhập tệp từ xa của Apple.
- DAP (Data Access Protocol), giao thức truy nhập tệp của DECnet.

• Giao thức Giao vận (Transport Protocol)

Giao thức hoạt động ở lớp giao vận, đảm bảo dữ liệu được truyền đi một cách tin cậy giữa các máy tính, bao gồm:

- TCP (Transmission Control Protocol), giao thức TCP/IP bảo đảm giao nhận dữ liệu tuần tự.
- SPX, một phần của chồng giao thức IPX/SPX (Internetwork Packet Exchange/Sequential Packet Exchange) của Novell.
- NWLink là một phần của chồng giao thức IPX/SPX của Microsoft.
- NetBEUI (NetBIOS Extended User Interface), giao thức thiết lập phiên truyền thông giữa các máy tính (NetBIOS) và cung cấp dịch vụ vận tải dữ liệu.
- ATP (Apple Talk Transaction Protocol), NBP (Name Binding Protocol), giao thức phiên truyền thông và giao thức vận tải dữ liệu của Apple.

• Giao thức Mạng (Network Protocol)

Giao thức loại này cung cấp các dịch vụ liên kết (link services), xử lý thông tin địa chỉ, thông tin đường đi, yêu cầu kiểm tra lỗi và yêu cầu truyền lại. Giao thức Mạng cũng định nghĩa những nguyên tắc trong môi trường mạng cụ thể, như Ethernet hay Token Ring. Lớp giao thức mạng bao gồm:

- IP (Internet Protocol), giao thức của chồng TCP/IP.
- IPX (Internetwork Packet Exchange), giao thức của NetWare dùng để định tuyến và gửi tiếp gói dữ liệu.
- NWLink, một phần trong giao thức IPX/SPX của Microsoft.

- NetBEUI, giao thức thiết lập phiên truyền thông và dịch vụ vận tải.
- DDP (Datagram Delivery Protocol), giao thức vận tải dữ liệu của AppleTalk.

• Một số giao thức phổ biến

- TCP/IP: TCP/IP (Transmission Control Protocol/Internet Protocol) là một chồng giao thức truyền thông trong môi trường đa chủng loại. Giao thức này hoạt động trong cả môi trường mạng LAN, Intranet và Internet.

TCP/IP trở thành tiêu chuẩn dùng cho liên kết hoạt động (interoperability) trong nhiều loại máy tính khác nhau. Hầu như tất cả các hệ điều hành mạng hiện nay đều chấp nhận TCP/IP là một trong những giao thức chủ yếu của nó. TCP/IP hỗ trợ việc định tuyến và thường được dùng làm giao thức liên mạng (internetworking protocol).

Chồng giao thức TCP/IP bao gồm cả những giao thức sau đây:

- SMTP, giao thức chuyển e-mail đơn giản.
- FTP, giao thức truyền tập tin giữa các máy chạy TCP/IP.
- SNMP (Simple Network Management Protocol), giao thức quản lý mạng.

TCP/IP là giao thức tương đối lớn, điều này gây bất lợi cho các máy trạm chạy hệ điều hành DOS, song trên các trạm sử dụng Windows thì tốc độ của nó tương đương với giao thức IPX.

- NetBEUI: NetBEUI là một giao thức mở rộng của NetBIOS, thừa ban đầu NetBIOS và NetBEUI gắn bó chặt chẽ và được coi là một giao thức. Tuy nhiên hiện nay một số hãng đã tách phần NetBIOS, vốn dĩ là giao thức tầng Phiên, ra để có thể dùng nó với một vài giao thức vận tải có định tuyến.

NetBEUI là giao thức nhỏ và rất hiệu quả của tầng Giao vận, bất lợi chính là nó không hỗ trợ định tuyến và nó chỉ được dùng trên các máy tính dùng hệ điều hành của Microsoft.

- XNS: XNS (Xerox Network System) là chồng giao thức do hãng Xerox thiết kế cho mạng cục bộ Ethernet. Hiện nay giao thức này không còn được sử dụng nhiều nữa.

- IPX/SPX và NWLink: IPX/SPX là chồng giao thức của hãng Novell. Chồng giao thức này hỗ trợ định tuyến.

NWLink là phiên bản IPX/SPX của hãng Microsoft.

- APPC: APPC (Advance Program-to-Program Communication) là

giao thức vận tải của hãng IBM trong chồng giao thức SNA. APPC được thiết kế cho phép các chương trình ứng dụng chạy trên các máy tính khác nhau có thể giao tiếp và trao đổi dữ liệu trực tiếp cho nhau.

– AppleTalk: AppleTalk là chồng giao thức của hãng Apple, hãng chuyên sản xuất các máy tính Macintosh. Giao thức này cho phép các máy tính dùng chung tệp tin và máy in.

– DECnet: DECnet là chồng giao thức của hãng Digital Equipment Corporation (DEC). Đây là giao thức sử dụng trong LAN, MAN, WAN và có sử dụng đường truyền công cộng hay thuê bao. DECnet có thể giao tiếp với TCP/IP và là giao thức hỗ trợ định tuyến.

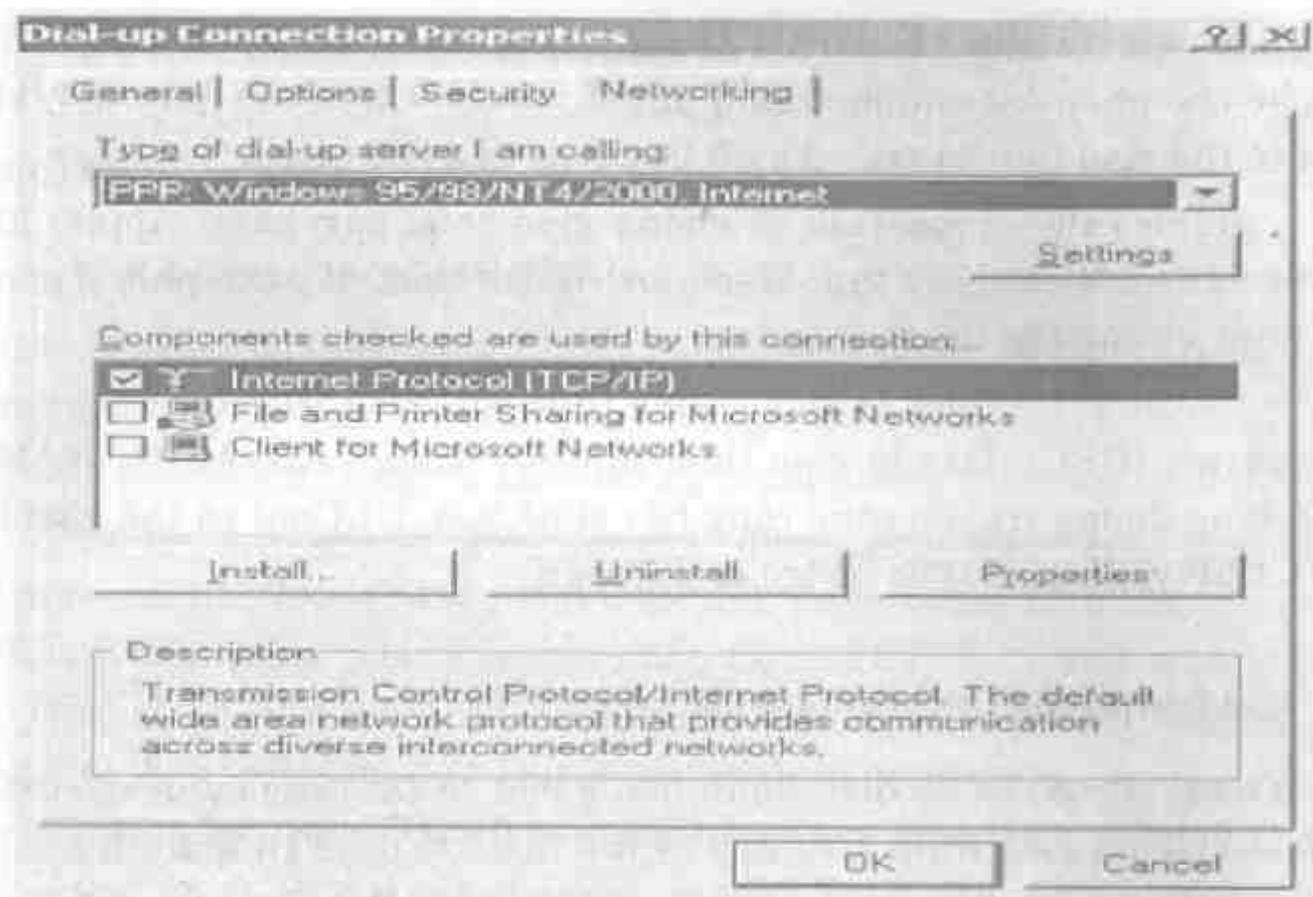
4. CÀI ĐẶT VÀ GỠ BỎ GIAO THỨC

Trong tất cả các hệ điều hành mạng đều có các công cụ để cài đặt và gỡ bỏ các chồng giao thức. Sau đây ta tìm hiểu về công cụ quản lí các liên kết mạng trong hệ điều hành Windows (bao gồm Windows 9x, 2000, XP, NT, 2000 server).

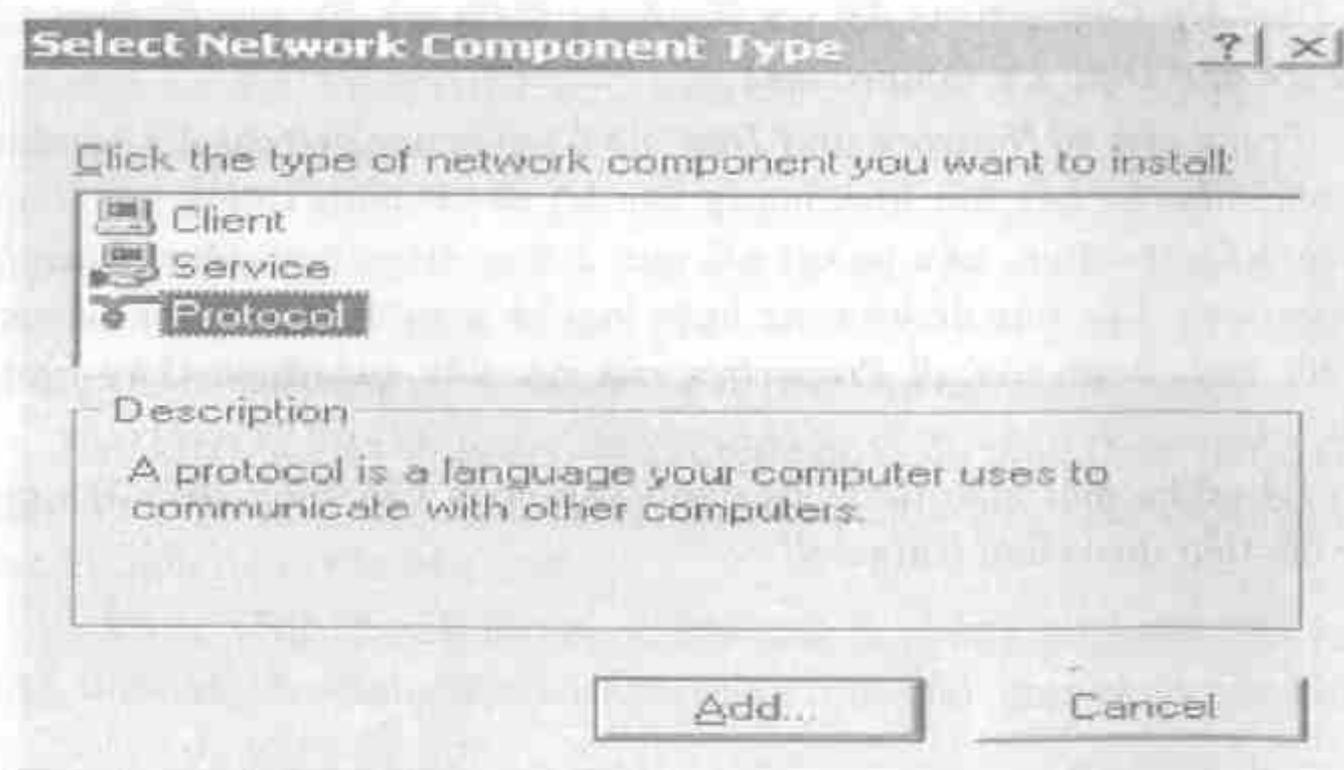
Đầu tiên ta chọn *Start/Control Panel* (hoặc là chọn thẳng *NetWork and Dial-Up Connections* đối với Windows 2000 trở đi), sau đó chọn tiếp *Network and Dial-Up Connections*.

Trong cửa sổ *Network and Dial-up Connections* có cài đặt các kiểu kết nối, nếu ta kết nối qua mạng cục bộ sẽ có biểu tượng của *Local Network Connection*, nếu ta kết nối qua đường điện thoại sẽ có *Dial-Up Connections*. Lúc này để bổ sung hoặc loại bỏ giao thức ta chọn kiểu kết nối rồi kích hoạt cửa sổ *Properties* của nó, kết quả được thấy như ở hình 4.4.

Để gỡ bỏ một giao thức: Ta đánh dấu chọn vào dòng chứa tên giao thức đó, tiếp theo chọn *Uninstall*.



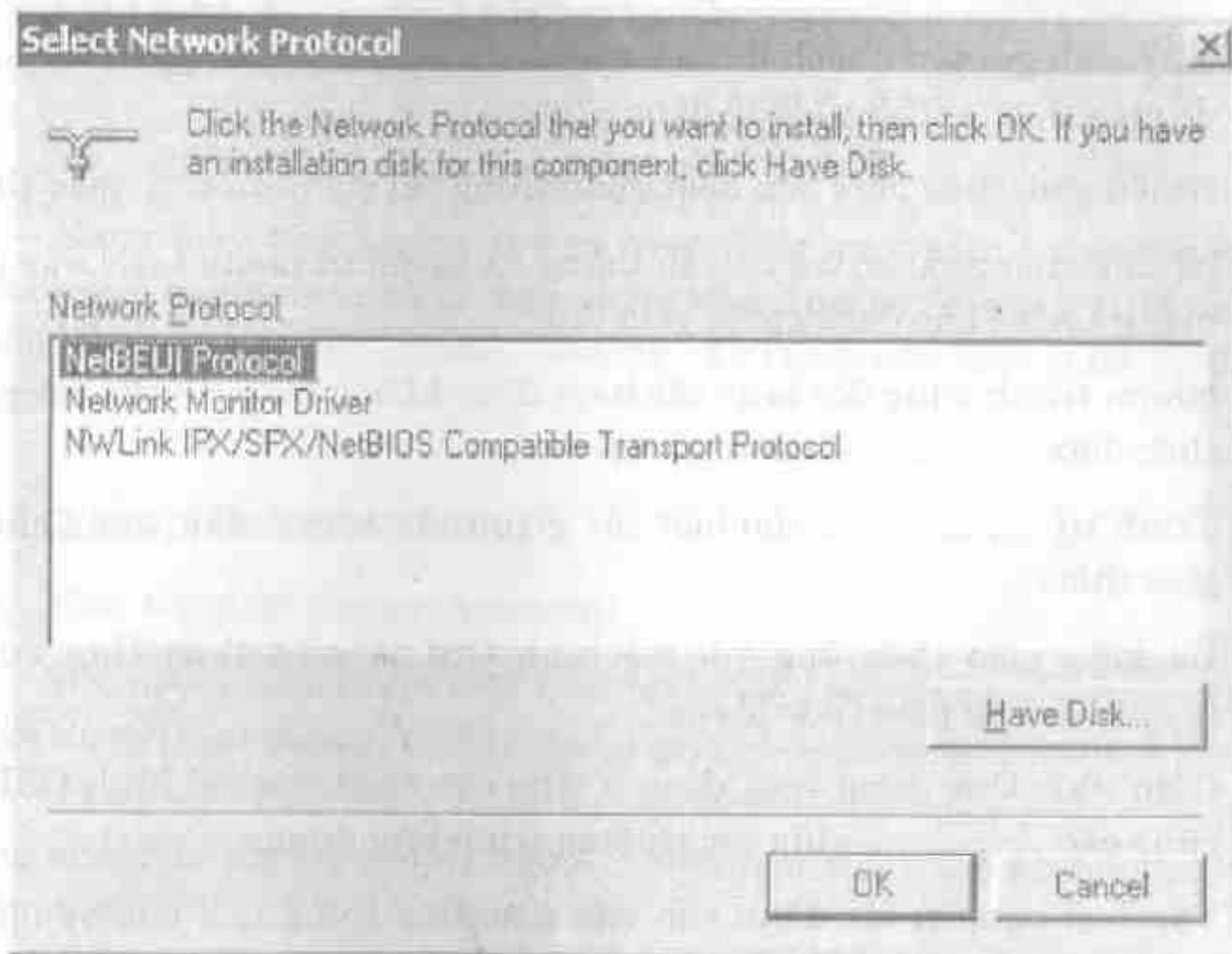
Hình 4.4. Cửa sổ Properties của kiểu kết nối Dial-up



Hình 4.5. Cửa sổ chọn bổ sung thêm thành phần mạng

Để bổ sung thêm giao thức: Ta chọn *Install*. Kết quả được thấy như hình 4.5. Chọn tiếp *Protocol* rồi nhấn vào nút *Add*. Kết quả ta có một danh

sách các giao thức mà hệ điều hành này hỗ trợ (hình 4.6), chọn vào tên của giao thức cần bổ sung rồi nhấn nút OK.



Hình 4.6. Danh sách các giao thức mà hệ điều hành hỗ trợ

CÂU HỎI CUỐI CHƯƠNG

Điền từ (cụm từ) thích hợp vào chỗ trống

1. Máy tính gửi phân tách dữ liệu thành nhiều phần nhỏ, gọi là để giao thức có thể xử lý dễ dàng.
2. Nhiều giao thức phối hợp hoạt động trong cái gọi là giao thức.
3. Những giao thức hỗ trợ truyền thông đa tuyến từ mạng LAN này đến mạng LAN khác được gọi là giao thức
4. Nhằm tránh xung đột hoặc các hoạt động không hoàn chỉnh, các giao thức được theo trình tự.
5. Trình tự cho biết các giao thức nằm ở đâu trong chồng giao thức.
6. Ba kiểu giao thức ứng với mô hình OSI là giao thức Ứng dụng, và giao thức Mạng.
7. Giao thức Ứng dụng hoạt động ở tầng cao nhất của mô hình OSI và cung cấp giữa các chương trình ứng dụng.
8. Tập hợp nguyên tắc dành cho việc giao tiếp trong môi trường mạng cục bộ cụ thể, như Ethernet hay Token Ring, được gọi là các giao thức
9. TCP/IP hỗ trợ định tuyến và được sử dụng phổ biến như một giao thức
10. NetBIOS là giao diện mạng cục bộ ở tầng Phiên của IBM đóng vai trò như một giao diện cho mạng.
11. APPC là giao thức của IBM.
12. Nhằm giúp người quản trị mạng cài đặt thêm giao thức sau khi đã cài đặt hệ thống lần đầu, một được cung cấp kèm với hệ điều hành.