BỘ CÔNG THƯƠNG

TRƯỜNG CĐ THƯƠNG MẠI VÀ DU LỊCH

GIÁO TRÌNH

MÔN HỌC: MẠNG MÁY TÍNH

NGÀNH: THƯƠNG MẠI ĐIỆN TỬ + CÔNG NGHỆ THÔNG TIN (ỨNG DỤNG PHẦN MỀM)

TRÌNH ĐỘ: TRUNG CẤP

(Ban hành kèm theo Quyết định số: 405 /QĐ-CĐTM ngày 5 tháng 7 năm 2022 của Trường Cao đẳng Thương mại và Du lịch)

Thái Nguyên, năm 2022

(Lưu hành nội bộ)

TUYÊN BỐ BẢN QUYỀN

LỜI GIỚI THIỆU

Trong những năm qua, dạy nghề đã có những bước tiến vượt bậc cả về số lượng và chất lượng, nhằm thực hiện nhiệm vụ đào tạo nguồn nhân lực kỹ thuật trực tiếp đáp ứng nhu cầu xã hội. Cùng với sự phát triển của khoa học công nghệ trên thế giới, lĩnh vực Công nghệ thông tin nói chung và ngành Thương mại điện tử ở Việt Nam nói riêng đã có những bước phát triển đáng kể.

Chương trình dạy nghề Thương mại điện tử đã được xây dựng trên cơ sở phân tích nghề, phần kỹ năng nghề được kết cấu theo các môđun. Để tạo điều kiện thuận lợi cho các cơ sở dạy nghề trong quá trình thực hiện, việc biên soạn giáo trình theo các môđun đào tạo nghề là cấp thiết hiện nay.

Mạng máy tính là mô đun đào tạo chuyên môn nghề được biên soạn theo hình thức tích hợp lý thuyết và thực hành. Trong quá trình thực hiện, nhóm biên soạn đã tham khảo nhiều tài liệu mạng máy tính trong và ngoài nước, kết hợp với kinh nghiệm trong thực tế.

Giáo trình này phục vụ cho học sinh chuyên ngành Thương mại điện tửvà Công nghệ thông tin - Ứng dụng phần mềm của trường Cao đẳng Thương mại và Du lịch.

Giáo trình gồm các nội dung chính sau:

Chương 1: Giới thiệu tổng quan về mạng máy tính. Phân loại các loại mạng máy tính và mục tiêu ứng dụng của nó.

Chương 2: Nghiên cứu các mô hình truyền thông. Giới thiệu mô hình OSI, được xem như là một mô hình chuẩn, một chiến lược phát triển các hệ thống mở.

Chương 3: Giới thiệu một số thiết bị mạng phổ biến. Đặc biệt trong chương này tìm hiểu sâu hơn về kỹ thuật bấm dây cáp mạng.

Chương 4: Chương này giới thiệu,cách nhận biết và phân biệt địa chỉ IPv4 và IPv6

Chương 5: Giới thiệu về An toàn mạng, một số phương thức tấn công và các biện pháp bảo vệ an toàn mạng.

Giáo trình không chỉ đề cập đến những vấn đề cơ sở lý luận mà còn trình bày một số kỹ năng, kỹ thuật cần thiết để thiết kế và cài đặt các mạng máy tính. Hy vọng sẽ có ích cho các bạn học sinh muốn tìm hiểu và xây dựng các hệ thống tin học ứng dụng phục vụ cho sản xuất, quản lý trong các doanh nghiệp. Mặc dầu có rất nhiều cố gắng, nhưng không tránh khỏi những khiếm khuyết, rất mong nhận được sự đóng góp ý kiến của độc giả để giáo trình được hoàn thiện hơn.

Xin chân thành cảm!

MỤC LỤC

LỜI GIỚI THIỆU 3
CHƯƠNG 1 – TỔNG QUAN VỀ MẠNG MÁY TÍNH 14
1.1. Định nghĩa mạng máy tính 16
1.2. Phân loại mạng máy tính 17
1.2.1. Dựa theo vị trí địa lý 17
1.2.2. Dựa theo cấu trúc mạng 17
1.2.3. Dựa theo phương pháp chuyển mạch 18
1.3. So sánh giữa mạng cục bộ và mạng diện rộng 19
1.3.1. Địa phương hoạt động 19
1.3.2. Tốc độ đường truyền và tỷ lệ lỗi trên đường truyền 19
1.3.3. Chủ quản và điều hành của mạng 20
1.3.4. Đường đi của thông tin trên mạng 20
1.3.5. Dạng chuyển giao thông tin 20
1.4. Các thành phần của mạng máy tính 20
1.4.1. Một số bộ giao thức kết nối mạng 20
1.4.2. Hệ điều hành mạng - NOS (Network Operating System) 21
1.5. Các lợi ích của mạng máy tính 22
1.6. Các dịch vụ phổ biến trên mạng máy tính 23
❖ Tóm tắt Chương 1 23
❖ Câu hỏi: 24
CHƯƠNG 2 – MÔ HÌNH TRUYỀN THÔNG 25
2.1. Sự cần thiết phải có mô hình truyền thông 27
2.2. Các nhu cầu về chuẩn hóa đối với mạng 28
2.3. Mô hình OSI (Open Systems Interconnection) 29
2.3.1. Nguyên tắc sử dụng khi định nghĩa các tầng hệ thống mở 29
2.3.2. Các giao thức trong mô hình OSI 30
2.3.3. Các chức năng chủ yếu của các tầng của mô hình OSI. 31
2.4. Quá trình chuyển vận gói tin 36
2.4.1. Quá trình đóng gói dữ liệu (tại máy gửi) 36
2.4.2. Quá trình truyền dữ liệu từ máy gửi đến máy nhận. 38
2.4.3. Chi tiết quá trình xử lý tại máy nhận 38
2.5. Mô hình TCP/IP 39
2.5.1. Tổng quan về bộ giao thức TCP/IP 39
2.5.2. So sánh TCP/IP với OSI 41
❖ Tóm tắt Chương 2 41

❖ Câu hỏi: 42
CHƯƠNG 3 – THIẾT BỊ MẠNG 43
3.1. Môi trường truyền dẫn 45
3.1.1. Khái niệm 45
3.1.2. Tần số truyền thông 45
3.1.3. Các đặc tính của phương tiện truyền dẫn 45
3.1.4. Các kiểu truyền dẫn. 46
3.2. Đường cáp truyền mạng 46
3.2.1. Cáp xoắn cặp 46
3.2.2. Cáp đồng trục 47
3.2.3. Cáp sợi quang (Fiber - Optic Cable) 48
3.2.4. Các yêu cầu cho một hệ thống cáp 49
3.3. Đường truyền vô tuyến 49
3.3.1. Sóng vô tuyến (radio) 50
3.3.2. Sóng viba 50
3.3.3. Hồng ngoại 50
3.4. Các kỹ thuật bấm cáp mạng 50
3.4.1. Kỹ thuật bấm dây cáp mạng thẳng 50
3.4.2. Kỹ thuật bấm dây cáp mạng chéo 51
3.5. Các thiết bị liên kết mạng 52
3.5.1. Repeater (Bộ tiếp sức) 52
3.5.2. Bridge (Cầu nối) 53
3.5.3. Router (Bộ tìm đường) 56
3.5.4. Gateway (cổng nối) 58
3.5.5. Hub (Bộ tập trung) 59
3.5.6. Bộ chuyển mạch (switch) 60
❖ Tóm tắt Chương 3 60
❖ Câu hỏi: 60
CHƯƠNG 4 – ĐỊA CHỈ IP 62
4.1. Địa chỉ IP 64
4.1.1. Khái niệm 64
4.1.2. Cấu trúc của các địa chỉ IP 64
4.1.3. Phân loại IP 67
4.1.4. Cách tìm địa chỉ IP 70
4.1.5. Ưu và nhược điểm của địa chỉ IP 71
4.2. Một số khái niệm và thuật ngữ liên quan 72

4.3. Địa chỉ IPv4 73
4.3.1. Thành phần và hình dạng của địa chỉ Ipv4 73
4.3.2. Các lớp địa chỉ IPv4 73
4.4. Địa chỉ IPv6 75
4.4.1. Giao thức liên mạng thế hệ mới (IPv6) 75
4.4.2. Một số đặc điểm mới của IPv6: 75
4.4.3. Kiến trúc địa chỉ trong IPv6: 76
❖ Tóm tắt Chương 1 77
❖ Câu hỏi: 77
CHƯƠNG 5: AN TOÀN MẠNG 79
5.1. Tổng quan về an toàn mạng 81
5.1.1. An toàn mạng là gì? 81
5.1.2. Các đặc trưng kỹ thuật của an toàn mạng 81
5.1.3. Các lỗ hổng và điểm yếu của mạng 83
5.1.4. Các biện pháp phát hiện hệ thống bị tấn công 83
5.2. Một số phương thức tấn công mạng phổ biến 84
5.2.1. Scanner 84
5.2.2. Bẻ khoá (Password Cracker) 84
5.2.3. Trojans 85
5.2.4. Sniffer 85
5.3. Biện pháp đảm bảo an ninh mạng 86
5.3.1. Tổng quan về bảo vệ thông tin bằng mật mã (Cryptography) 86
5.3.2. Firewall 87
5.3.3. Các loại Firewall 87
5.3.4. Kỹ thuật Fire wall 88
5.3.5. Kỹ thuật Proxy 88
❖ Tóm tắt Chương 1 89
❖ Câu hỏi: 89
TÀI LIỆU THAM KHẢO 90

GIÁO TRÌNH MÔN HỌC

1. Tên môn học: Mạng máy tính

2. Mã môn học:MH20

3. Vị trí, tính chất, ý nghĩa và vai trò của môn học của môn học:

3.1. Vị trí: Môn học Mạng máy tính là môn học cơ sở thuộc khối các môn học chuyên môn nghề Thương mại điện tử và nghề Công nghệ thông tin - Ứng dụng phần mềm được bố trí giảng dạy sau các môn học chung trong chương trình đào tạo trình độ Trung cấp.

3.2. Tính chất: Chương trình môn học Mạng máy tính bao gồm một số nội dung cơ bản về mạng máy tính như: khái niệm mạng máy tính; mô hình truyền thông; thiết bị mạng và cách thức đảm bảo an toàn mạng máy tính.

3.3. Ý nghĩa và vai trò của môn học: Mạng máy tính là môn học thực hành dành cho đối tượng là người học thuộc chuyên ngành Thương mại điện tử và Công nghệ thông tin - Ứng dụng phần mềm. Nội dung chủ yếu của môn học này nhằm cung cấp các kiến thức và kỹ năng cơ bản về mạng máy tínhvà có kỹ năng vận dụng được những kiến thức đã học vào quá trình xây dựng, sử dụng, quản trị một mạng máy tính của doanh nghiệp.

4. Mục tiêu môn học:

4.1. Về kiến thức:

A1. Nhận biết được những khái niệm cơ bản về mạng máy tính

A2. Hiểu được sự cần thiết của mô hình truyền thông và các mô hình truyền thông đang được sử dụng hiện nay

A3. Nhận biết được các thiết bị mạng.

A4. Trình bày được khái niệm về địa chỉ IP

A5. Trình bày được các kiến thức tổng quan về An toàn mạng

4.2. Về kỹ năng

B1. Phân loại và so sánh được các loại mạng máy tính

B2. Phân biệt và so sánh được giữa hai mô hình OSI và TCP/IP

B3. Phân biệt được các thiết bị mạng. Thực hiện được kỹ thuật bấm dây cáp mạng xoắn đôi

B4. Phân loại và so sánh được về địa chỉ IPv4 và địa chỉ Ipv6

B5. Phân biệt được một số phương thức tấn công mạng phổ biến và cài đặt được mộ số biện pháp đảm bảo an toàn mạng cơ bản

4.3. Về năng lực tự chủ và trách nhiệm:

C1. Ý thức được tầm quan trọng và ý nghĩa thực tiễn của mạng máy tính trong hoạt động của cơ quan, doanh nghiệp.

C2. Làm việc độc lập, làm việc theo nhóm.

C3. Tuân thủ nội quy, quy định nơi làm việc.

5. Nội dung của môn học

5.1. Chương trình khung

5.1.1. Chương trình khung ngành Thương mại điện tử

Mã MH	Tên môn học	Số tín chỉ	Thời gian học tập (giờ)			
			Tổng số	Trong đó		
				Lý thuyết	Thực hành/ thực tập/ bài tập/thảo luận	Kiểm tra
I	**Các môn học chung**	**12**	**255**	**94**	**148**	**13**
MH01	Chính trị	2	30	15	13	2
MH02	Pháp luật	1	15	9	5	1
MH03	Giáo dục thể chất	1	30	4	24	2
MH04	Giáo dục quốc phòng và an ninh	2	45	21	21	3
MH05	Tin học	2	45	15	29	1
MH06	Ngoại ngữ	4	90	30	56	4
II	**Các môn học chuyên môn**	**64**	**1590**	**511**	**1035**	**44**
II.1	***Môn học cơ sở***	***15***	***225***	***184***	***31***	***10***
MH07	Kinh tế vi mô	3	45	43	-	2
MH08	Thương mại điện tử căn bản	3	45	43	-	2
MH09	Pháp luật thương mại điện tử	2	30	28	-	2
MH10	Mạng máy tính	2	30	15	14	1
MH11	Marketing điện tử	2	30	28	-	2
MH12	Quản trị cơ sở dữ liệu	3	45	27	17	1
II.2	***Các môn học chuyên môn***	***47***	***1335***	***298***	***1004***	***33***
MH13	Tiếng Anh thương mại	4	60	57	-	3
MH14	Nghiệp vụ kinh doanh TM dịch vụ	4	60	57	-	3
MH15	Quản trị tác nghiệp TMĐT	4	60	57	-	3
MH16	Nghiệp vụ vận tải, giao nhận và bảo hiểm trong TMĐT	3	45	43	-	2
MH17	Khai báo hải quan điện tử	2	30	28	-	2
MH18	Thanh toán điện tử	2	30	28	-	2
MH19	An toàn hệ thống thông tin	2	30	28	-	2
MH20	Thực hành mạng và quản trị mạng	3	90	-	86	4
MH21	TH tác nghiệp TMĐT	3	90	-	86	4
MH22	TH vận tải, giao nhận và bảo hiểm trong TMĐT	2	60	-	56	4
MH23	TH khai báo hải quan ĐT	2	60	-	56	4

MH24	Thực tập tốt nghiệp	16	720		720	
II.3	***Các môn học, mô đun tự chọn***	***2***	***30***	***28***	**-**	***2***
MH25	Kỹ năng bán hàng trực tuyến	2	30	28	-	2
MH26	Khởi sự kinh doanh	2	30	28	-	2
	Tổng cộng	**76**	**1845**	**605**	**1183**	**57**

5.1.2. Chương trình khung ngành Công nghệ thông tin (Ứng dụng phần mềm)

Mã MH	**Tên môn học**	**Số tín chỉ**	**Thời gian học tập** *(giờ)*			
			Tổng số	**Trong đó**		
				Lý thuyết	**Thực hành/ thựctập/ bài tập/ thảo luận**	**Thi/ Kiểm tra**
I	**Các môn học chung**	**12**	**255**	**94**	**148**	**13**
MH01	Chính trị	2	30	15	13	2
MH02	Pháp luật	1	15	9	5	1
MH03	Giáo dục thể chất	1	30	4	24	2
MH04	Giáo dục quốc phòng và an ninh	2	45	21	21	3
MH05	Tin học	2	45	15	29	1
MH06	Ngoại ngữ	4	90	30	56	4
II	**Các môn học chuyên môn**	**64**	**1560**	**504**	**1013**	**43**
II.1	***Môn học cơ sở***	***16***	***240***	***179***	***48***	***13***
MH07	Tin học văn phòng	2	30	12	17	1
MH08	Bảng tính Excel	2	30	12	17	1
MH09	Cấu trúc máy tính	2	30	28	-	2
MH10	Mạng máy tính	2	30	15	14	1
MH11	Lập trình cơ bản	2	30	28	-	2
MH12	Cấu trúc dữ liệu và giải thuật	2	30	28	-	2
MH13	Cơ sở dữ liệu	2	30	28	-	2
MH14	Lắp ráp và bảo trì máy tính	2	30	28	-	2
II.2	***Môn học chuyên môn***	***46***	***1290***	***297***	***965***	***28***
MH15	Ngoại ngữ ch.ngành CNTT	4	60	57	-	3
MH16	Hệ điều hành Windows Server	2	30	28	-	2
MH17	Quản trị CSDL với Access 1	3	45	43	-	2
MH18	Quản trị CSDL với SQL Server	3	45	27	17	1
MH19	Lập trình Windows 1	3	45	43	-	2
MH20	Thiết kế và quản trị website	3	45	43	-	2
MH21	Đồ họa ứng dụng	2	30	28	-	2
MH22	An toàn và bảo mật thông tin	2	30	28	-	2
MH23	TH xây dựng phần mềm quản lý	4	120	-	114	6
MH24	TH thiết kế và quản trị website	4	120	-	114	6
MH25	Thực tập tốt nghiệp	16	720	-	720	

II.3	***Môn học tự chọn****(chọn 1 trong 2)*	***2***	***30***	***28***	***-***	***2***
MH26	Kỹ năng giao tiếp, phục vụ khách hàng	2	30	28	-	2
MH27	Lập trình mạng	2	30	28	-	2
	Tổng cộng	**76**	**1815**	**598**	**1161**	**56**

5.2. Chương trình chi tiết môn học

SốTT	Tên chương, mục	Thời gian (giờ)			
		Tổng số	Lýthuyết	Thực hành, thí nghiệm, thảo luận, bài tập	Kiểm tra
1	**Chương 1: Những khái niệm cơ bản về mạng máy tính** 1.1. Định nghĩa mạng máy tính 1.2. Phân loại mạng máy tính 1.3 So sánh giữa mạng cục bộ và mạng diện rộng 1.4. Các thành phần của mạng máy tính 1.5. Các lợi ích của mạng máy tính 1.6. Các dịch vụ phổ biến trên mạng máy tính	2	2	0	0
2	**Chương 2: Mô hình truyền thông** 2.1. Sự cần thiết phải có mô hình truyền thông 2.2. Các nhu cầu chuẩn hóa đối với mạng 2.3. Mô hình OSI 2.4. Quá trình chuyển vận gói tin 2.5. Mô hình TCP/IP	10	6	4	0
3	**Chương 3: Thiết bị mạng** 3.1. Mô trường truyền dẫn 3.2. Đường cáp truyền mạng 3.3. Đường truyền vô tuyến 3.4. Các kỹ thuật bấm cáp mạng 3.5. Các thiết bị liên kết mạng	10	2	8	0

4	**Chương 4: Địa chỉ IP** 4.1. Địa chỉ IP 4.2. Một số khái niệm và thuật ngữ liên quan 4.3. Địa chỉ IPv4 4.4. Địa chỉ IPv6	4	2	2	0
5	**Chương 5: An toàn mạng** 5.1. Tổng quan về an toàn mạng 5.2. Một số phương thức tấn công mạng phổ biến 5.3. Biện pháp đảm bảo an ninh mạng	3	3	0	0
6	**Kiểm tra**	1			1
	Cộng	**30**	**15**	**14**	**1**

6. Điều kiện thực hiện môn học:

6.1. Phòng học chuyên môn / nhà xưởng:

- Phòng học lý thuyết, thực hành được trang bị hệ thống đèn đủ ánh sáng.
- Bàn ghế cho sinh viên.
- Bàn ghế giáo viên, bảng, phấn.

6.2. Trang thiết bị máy móc:

- Máy tính, máy chiếu

6.3. Học liệu, dụng cụ, nguyên vật liệu:

- Giáo án, bài giảng.
- Dây mạng, kìm bấm mạng, các đầu nối RJ45, Hub, Switch, Router.
- Giáo trình nội bộ và các tài liệu giảng dạy khác hỗ trợ bài giảng.

6.4. Các điều kiện khác: Không

7. Nội dung và phương pháp đánh giá:

7.1. Nội dung:

- Kiến thức: Đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức
- Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kỹ năng.
- Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:

+ Nghiên cứu bài trước khi đến lớp.

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

7.2. Phương pháp:

Người học được đánh giá tích lũy môn học như sau:

7.2.1. Cách đánh giá

- Áp dụng quy chế đào tạo Cao đẳng hệ chính quy ban hành kèm theo Thông tư số 04/2022/TT-BLĐTBXH ngày 30 tháng 3 năm 2022 của Bộ trưởng Bộ Lao động – Thương binh và Xã hội.

- Quy chế Tổ chức đào tạo trình độ trung cấp, trình độ cao đẳng theo phương thức tích lũy mô-đun hoặc tín chỉ của Nhà trường ban hành kèm theo Quyết định số 246/QĐ-CĐTMDL ngày 1 tháng 6 năm 2022 của Hiệu trưởng Trường cao đẳng Thương mại và Du lịch và hướng dẫn cụ thể theo từng môn học/mô-đun trong chương trình đào tạo

Điểm đánh giá	**Trọng số**
+ Điểm kiểm tra thường xuyên (Hệ số 1)	40%
+ Điểm kiểm tra định kỳ (Hệ số 2)	
+ Điểm thi kết thúc môn học	60%

7.2.2. Phương pháp đánh giá

Phương pháp đánh giá	**Phương pháp tổ chức**	**Hình thức kiểm tra**	**Chuẩn đầu ra đánh giá**	**Số bài**	**Thời điểm kiểm tra**
Thường xuyên	Trắc nghiệm + Tự luận	Trắc nghiệm + Tự luận	A1, A2, B1, B2, C1, C2	1	Sau 12 giờ.
Định kỳ	Trắc nghiệm + Tự luận	Trắc nghiệm + Tự luận	A3, A4, A5, B3,B4, B5, C1, C2	1	Sau 20 giờ
Kết thúc môn học	Trắc nghiệm + Tự luận	Trắc nghiệm + Tự luận	A1, A2, A3, A4, A5, B1, B2, B3, B4, B5, C1, C2, C3,	1	Sau 30 giờ

7.2.3. Cách tính điểm

- Điểm đánh giá thành phần và điểm thi kết thúc môn học được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến một chữ số thập phân.

- Điểm môn học là tổng điểm của tất cả điểm đánh giá thành phần của môn học nhân với trọng số tương ứng. Điểm môn học theo thang điểm 10 làm tròn đến một chữ số thập phân, sau đó được quy đổi sang điểm chữ và điểm số theo thang điểm 4 theo quy định của Bộ Lao động Thương binh và Xã hội về đào tạo theo tín chỉ..

8. Hướng dẫn thực hiện môn học

8.1. Phạm vi, đối tượng áp dụng: Môn học được sử dụng để giảng dạy cho nghề Thương mại điện tử và nghề Công nghệ thông tin - Ứng dụng phần mềm. Tổng thời gian thực hiện môn học là: 30 giờ, giáo viên giảng các giờ lý thuyết, kết hợp với các giờ thực hành đan xen.

8.2. Phương pháp giảng dạy, học tập môn học

8.2.1. Đối với người dạy:

*** Lý thuyết:** Áp dụng phương pháp dạy học tích cực bao gồm: thuyết trình ngắn, nêu vấn đề, hướng dẫn đọc tài liệu, bài tập tình huống, câu hỏi thảo luận….

* **Bài tập:** Phân chia nhóm nhỏ thực hiện bài tập theo nội dung đề ra.

*** Thực hành:** Phân chia thực hành theo nội dung đề ra.

*** Hướng dẫn tự học theo nhóm:** Nhóm trưởng phân công các thành viên trong nhóm tìm hiểu, nghiên cứu theo yêu cầu nội dung trong bài học, cả nhóm thảo luận, trình bày nội dung, ghi chép và viết báo cáo nhóm.

8.2.2. Đối với người học:

- Nghiên cứu kỹ bài học tại nhà trước khi đến lớp. Các tài liệu tham khảo sẽ được cung cấp nguồn trước khi người học vào học môn học này (trang web, thư viện, tài liệu...)

- Tham dự tối thiểu 80% các buổi giảng lý thuyết. Nếu người học vắng >20% số tiết lý thuyết phải học lại môn học mới được tham dự kì thi lần sau.

- Tự học và thảo luận nhóm: là một phương pháp học tập kết hợp giữa làm việc theo nhóm và làm việc cá nhân. Một nhóm gồm 8-10 người học sẽ được cung cấp chủ đề thảo luận trước khi học lý thuyết, thực hành. Mỗi người học sẽ chịu trách nhiệm về 1 hoặc một số nội dung trong chủ đề mà nhóm đã phân công để phát triển và hoàn thiện tốt nhất toàn bộ chủ đề thảo luận của nhóm.

- Tham dự đủ các bài kiểm tra thường xuyên, định kỳ.

- Tham dự thi kết thúc môn học.

- Chủ động tổ chức thực hiện giờ tự học.

9. Tài liệu tham khảo:

(1) Ts. Phạm Thế Quế, Sách hướng dẫn học tập Mạng máy tính, 2006

(2) Hồ Đắc Phương, Nhập môn Mạng máy tính, Nhà xuất bản Giáo dục Việt Nam

(3) Khoa Công nghệ Thông tin, Giáo trình nhập môn Mạng máy tính, Trường Trung cấp Kinh tế Kỹ thuật Quang Trung.

CHƯƠNG 1 – TỔNG QUAN VỀ MẠNG MÁY TÍNH

❖ GIỚI THIỆU CHƯƠNG 1

Chương 1 là phần lý thuyết các kiến thức cơ bản về mạng máy tính.

❖ MỤC TIÊU CHƯƠNG 1

Sau khi học xong phần này, người học có khả năng:

➢ ***Về kiến thức:***

- Trình bày được một số khái niệm cơ bản về mạng máy tính.
- Hiểu được các loại mạng máy tính và mục tiêu ứng dụng của mạng máy tính.

➢ ***Về kỹ năng:***

- Nhận biết và phân loại các loại mạng máy tính.

➢ ***Về năng lực tự chủ và trách nhiệm:***

- Ý thức được tầm quan trọng và ý nghĩa thực tiễn của mạng máy tính trong thế giới công nghệ ngày nay.
- Tích cực, chủ động và hợp tác trong học tập. Thể hiện sự nhiệt tình, trách nhiệm, tác phong nhanh nhẹn trong công việc.

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP CHƯƠNG 1

- Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp); yêu cầu người học thực hiện trả lời câu hỏi và bài tập Chương 1 (cá nhân hoặc nhóm).
- Đối với người học: chủ động đọc trước giáo trình (Chương 1) trước buổi học; hoàn thành đầy đủ bài tập Chương 1 theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.

❖ ĐIỀU KIỆN THỰC HIỆN CHƯƠNG 1

➢ ***Phòng học chuyên môn hóa/nhà xưởng:***

- Phòng học lý thuyết, thực hành được trang bị hệ thống đèn đủ ánh sáng.
- Bàn ghế cho sinh viên.
- Bàn ghế giáo viên, bảng, phấn.

➢ ***Trang thiết bị máy móc:***

- Máy tính, máy chiếu

➢ ***Học liệu, dụng cụ, nguyên vật liệu:***

- Giáo án, bài giảng.
- Giáo trình nội bộ và các tài liệu giảng dạy khác hỗ trợ bài giảng

➢ ***Các điều kiện khác:*** Không có

❖ KIỂM TRA VÀ ĐÁNH GIÁ CHƯƠNG 1

- **Nội dung:**

✓ Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức

✓ Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.

✓ Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ Điểm kiểm tra thường xuyên: Không có

✓ Kiểm tra định kỳ: Không có

NỘI DUNG CHƯƠNG 1

Mạng máy tính ngày nay đã phát triển một cách nhanh chóng và đa dạng. Hệ điều hành cùng các ứng dụng của mạng ngày càng phong phú, các lợi ích của mạng ngày càng được khẳng định. Mạng máy tính bao gồm rất nhiều loại, nhiều mô hình triển khai. Trong một mạng máy tính lại có nhiều thành phần cấu thành. Trước khi đi chi tiết về mạng máy tính, chúng ta sẽ tìm hiểu các khái niệm cơ bản của mạng máy tính.

1.1. Định nghĩa mạng máy tính

Mạng máy tính là một tập hợp các máy tính được nối với nhau bởi đường truyền theo một cấu trúc nào đó và thông qua đó các máy tính trao đổi thông tin qua lại với nhau.

Đường truyền là hệ thống các thiết bị truyền dẫn có dây hay không dây dùng để chuyển các tín hiệu điện tử từ máy tính này đến máy tính khác. Các tín hiệu điện tử đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on - off). Tất cả các tín hiệu được truyền giữa các máy tính đều thuộc một dạng sóng điện từ. Tùy theo tần số của sóng điện từ có thể dùng các đường truyền vật lý khác nhau để truyền các tín hiệu. Ở đây đường truyền được kết nối có thể là dây cáp đồng trục, cáp xoắn, cáp quang, dây điện thoại, sóng vô tuyến ... Các đường truyền dữ liệu tạo nên cấu trúc của mạng.

Hình 1-1: Mạng máy tính

Với sự trao đổi qua lại giữa máy tính này với máy tính khác đã phân biệt mạng máy tính với các hệ thống thu phát một chiều như truyền hình, phát thông tin từ vệ tinh xuống các trạm thu thụ động... vì tại đây chỉ có thông tin một chiều từ nơi phát đến nơi thu mà không quan tâm đến có bao nhiêu nơi thu, có thu tốt hay không.

Đặc trưng cơ bản của đường truyền vật lý là giải thông. Giải thông của một đường chuyền chính là độ đo phạm vi tần số mà nó có thể đáp ứng được. Tốc độ truyền dữ liệu trên đường truyền còn được gọi là thông lượng của đường truyền - thường được tính bằng số lượng bit được truyền đi trong một giây (Bps). Thông lượng còn được đo bằng đơn vị khác là Baud (lấy từ tên nhà bác học - Emile Baudot). Baud biểu thị số lượng thay đổi tín hiệu trong một giây.

Ở đây Baud và Bps không phải bao giờ cũng đồng nhất. Ví dụ: nếu trên đường dây có 8 mức tín hiệu khác nhau thì mỗi mức tín hiệu tương ứng với 3 bit hay là 1 Baud tương ứng với 3 bit. Chỉ khi có 2 mức tín hiệu trong đó mỗi mức tín hiệu tương ứng với 1 bit thì 1 Baud mới tương ứng với 1 bit.

1.2. Phân loại mạng máy tính

Có nhiều cách để phân biệt mạng máy tính nhưng người ta thường phân biệt mạng máy tính theo vị trí địa lý, cấu trúc mạng, phương pháp chuyển mạch.

1.2.1.Dựa theo vị trí địa lý

Dựa vào phạm vi phân bổ của mạng người ta có thể phân ra các loại mạng như sau:

- **GAN (Global Area Network)** - Kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.

- **WAN (Wide Area Network)** - Mạng diện rộng, kết nối máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong cùng một châu lục. Thông thường kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.

- **MAN (Metropolitan Area Network)** - Kết nối các máy tính trong phạm vi một thành phố hay giữa các thành phố với nhau.

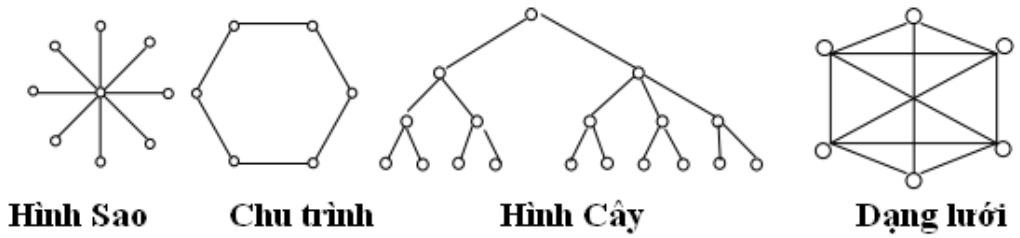
- **LAN (Local Area Network)** - Mạng cục bộ, kết nối các máy tính trong một khu vực bán kính hẹp thông thường khoảng vài trăm mét. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao ví dụ cáp đồng trục thay cáp quang. LAN thường được sử dụng trong nội bộ một cơ quan/tổ chức... Các LAN có thể được kết nối với nhau thành WAN.

Trong các khái niệm nói trên, thường được sử dụng nhất hiện này là khái niệm Mạng diện rộng WAN và mạng cục bộ LAN.

1.2.2. Dựa theo cấu trúc mạng

Kiểu điểm - điểm (point - to - point)

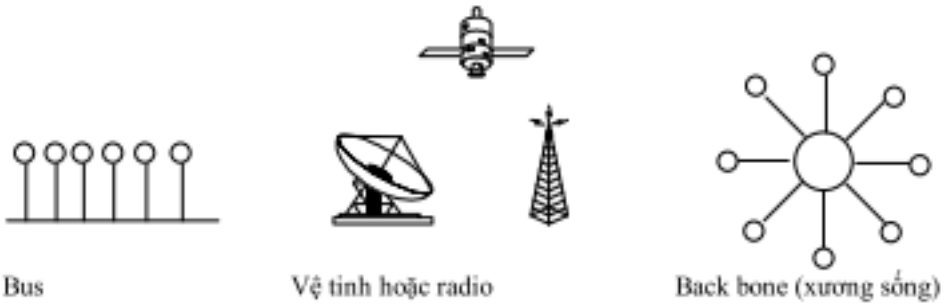
Đường truyền nối từng cặp nút mạng với nhau. Thông tin đi từ nút nguồn qua nút trung gian rồi gởi tiếp nếu đường truyền không bị bận. Do đó, còn có tên là mạng lưu trữ và chuyển tiếp (store and forward).



Hình 1-2: Cấu trúc điểm – điểm

Kiểu khuyếch tán

Bản tin được gởi đi từ một nút sẽ được tiếp nhận bởi các nút còn lại (còn gọi là broadcasting hay point to multipoint). Trong bản tin phải có vùng địa chỉ cho phép mỗi nút kiểm xem có phải tin của mình không và xử lý nếu đúng bản tin được gởi đến.

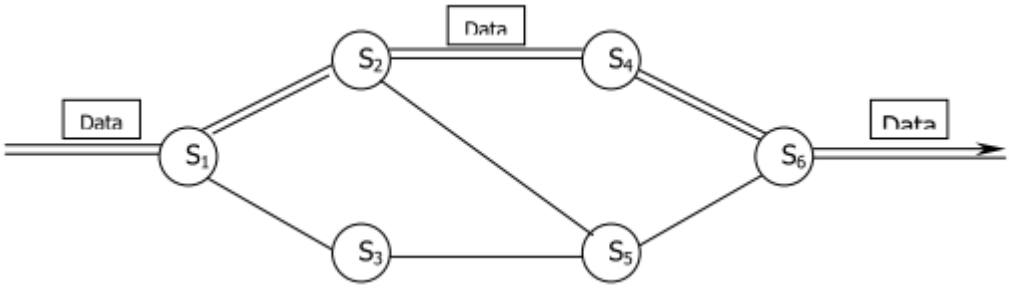


Hình 1-3: Cấu trúc kiểu khuyếch tán

1.2.3. Dựa theo phương pháp chuyển mạch

Mạng chuyển mạch kênh (Line switching network)

Chuyển mạch kênh dùng trong mạng điện thoại. Một kênh cố định được thiết lập giữa cặp thực thể cần liên lạc với nhau. Mạng này có hiệu suất không cao vì có lúc kênh bỏ không.

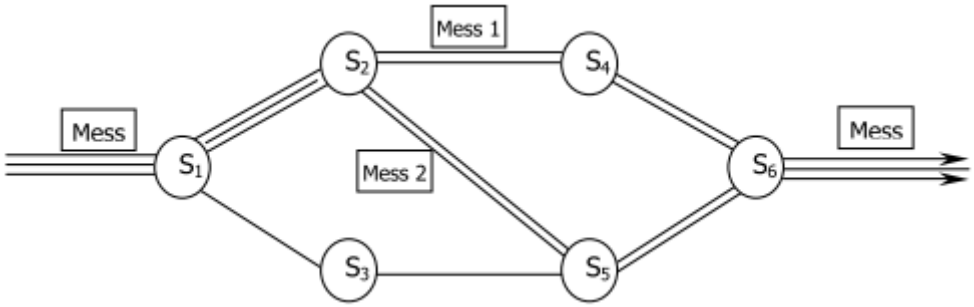


Hình 1-4: Mạng chuyển mạch kênh

Mạng chuyển mạch thông điệp (Message switching network)

Các nút của mạng căn cứ vào địa chỉ đích của "thông điệp" để chọn nút kế tiếp. Như vậy các nút cần lưu trữ và đọc tin nhận được, quản lý việc truyền tin. Trong trường hợp bản tin quá dài và nếu sai phải truyền lại. Phương pháp này giống như cách gởi thư thông thường.

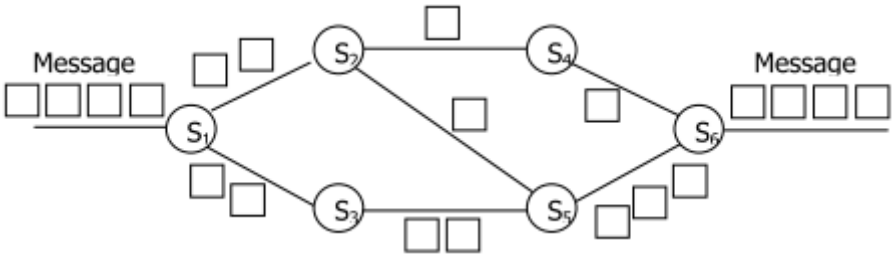
Mạng chuyển mạch thông báo thích hợp với các dịch vụ thông tin kiểu thư điện tử (Email) hơn là đối với các ứng dụng có tính thời gian thực vì tồn tại độ trễ nhất định do lưu trữ và xử lý thông tin điều khiển tại mỗi nút.



Hình 1-5: Mạng chuyển mạch thông điệp

Mạng chuyển mạch gói (Packet switching network)

Bản tin được chia thành nhiều gói tin (packet) có độ dài 512 bytes, phần đầu của gói tin thường là địa chỉ đích, mã để tập hợp các gói. Các gói tin của các thông điệp khác nhau có thể được truyền độc lập trên cùng một đường truyền. Vấn đề phức tạp ở đây là tạo lại bản tin ban đầu, đặc biệt là khi truyền trên các con đường khác nhau. Chuyển mạch gói mềm dẻo, hiệu suất cao. Sử dụng hai kĩ thuật chuyển mạch kênh và chuyển mạch gói trong cùng một mạng thống nhất gọi là mạng ISDN (Integrated Services Digital Network – Mạng thông tin số đa dịch vụ)



Hình 1-6: Mạng chuyển mạch gói

1.3. So sánh giữa mạng cục bộ và mạng diện rộng

Mạng cục bộ và mạng diện rộng có thể được phân biệt bởi: địa phương hoạt động, tốc độ đường truyền và tỷ lệ lỗi trên đường truyền, chủ quản của mạng, đường đi của thông tin trên mạng, dạng chuyển giao thông tin.

1.3.1. Địa phương hoạt động

Liên quan đến khu vực địa lý thì mạng cục bộ sẽ là mạng liên kết các máy tính nằm ở trong một khu vực nhỏ. Khu vực có thể bao gồm một tòa nhà hay là một khu nhà... Điều đó hạn chế bởi khoảng cách đường dây cáp được dùng để liên kết các máy tính của mạng cục bộ (Hạn chế đó còn là hạn chế của khả năng kỹ thuật của đường truyền dữ liệu). Ngược lại mạng diện rộng là mạng có khả năng liên kết các máy tính trong một vùng rộng lớn như là một thành phố, một miền, một đất nước, mạng diện rộng được xây dựng để nối hai hoặc nhiều khu vực địa lý riêng biệt.

1.3.2. Tốc độ đường truyền và tỷ lệ lỗi trên đường truyền

Do các đường cáp của mạng cục bộ đươc xây dựng trong một khu vực nhỏ cho nên nó ít bị ảnh hưởng bởi tác động của thiên nhiên (như là sấm chớp, ánh sáng...). Điều đó cho phép mạng cục bộ có thể truyền dữ liệu với tốc độ cao mà chỉ chịu một tỷ lệ lỗi nhỏ. Ngược lại với mạng diện rộng do phải truyền ở những khoảng cách khá xa với những đường truyền dẫn dài có khi lên tới hàng ngàn km. Do vậy mạng diện rộng không thể truyền với tốc độ quá cao vì khi đó tỉ lệ lỗi sẽ trở nên khó chấp nhận được.

Mạng cục bộ thường có tốc độ truyền dữ liệu từ 4 đến 16 Mbps và đạt tới 100 Mbps nếu dùng cáp quang. Còn phần lớn các mạng diện rộng cung cấp đường truyền có tốc độ thấp hơn nhiều như T1 với 1.544 Mbps hay E1 với 2.048 Mbps.

Đơn vị bps (Bit Per Second) là một đơn vị trong truyền thông tương đương với 1 bit được truyền trong một giây, ví dụ như tốc độ đường truyền là 1 Mbps tức là có thể truyền tối đa 1 Megabit trong 1 giây trên đường truyền đó.

Thông thường trong mạng cục bộ tỷ lệ lỗi trong truyền dữ liệu vào khoảng 1/107-108 còn trong mạng diện rộng thì tỷ lệ đó vào khoảng 1/106 - 107

1.3.3. Chủ quản và điều hành của mạng

Do sự phức tạp trong việc xây dựng, quản lý, duy trì các đường truyền dẫn nên khi xây dựng mạng diện rộng người ta thường sử dụng các đường truyền được thuê từ các công ty viễn thông hay các nhà cung cấp dịch vụ truyền số liệu. Tùy theo cấu trúc của mạng những đường truyền đó thuộc cơ quan quản lý khác nhau như các nhà cung cấp đường truyền nội hạt, liên tỉnh, liên quốc gia. Các đường truyền đó phải tuân thủ các quy định của chính phủ các khu vực có đường dây đi qua như: tốc độ, việc mã hóa.

Còn đối với mạng cục bộ thì công việc đơn giản hơn nhiều, khi một cơ quan cài đặt mạng cục bộ thì toàn bộ mạng sẽ thuộc quyền quản lý của cơ quan đó.

1.3.4. Đường đi của thông tin trên mạng

Trong mạng cục bộ thông tin được đi theo con đường xác định bởi cấu trúc của mạng. Khi người ta xác định cấu trúc của mạng thì thông tin sẽ luôn luôn đi theo cấu trúc đã xác định đó. Còn với mạng diện rộng dữ liệu cấu trúc có thể phức tạp hơn nhiều do việc sử dụng các dịch vụ truyền dữ liệu. Trong quá trình hoạt động các điểm nút có thể thay đổi đường đi của các thông tin khi phát hiện ra có trục trặc trên đường truyền hay khi phát hiện có quá nhiều thông tin cần truyền giữa hai điểm nút nào đó. Trên mạng diện rộng thông tin có thể có các con đường đi khác nhau, điều đó cho phép có thể sử dụng tối đa các năng lực của đường truyền hay nâng cao điều kiện an toàn trong truyền dữ liệu.

1.3.5. Dạng chuyển giao thông tin

Phần lớn các mạng diện rộng hiện nay được phát triển cho việc truyền đồng thời trên đường truyền nhiều dạng thông tin khác nhau như: video, tiếng nói, dữ liệu... Trong khi đó các mạng cục bộ chủ yếu phát triển trong việc truyền dữ liệu thông thường. Điều này có thể giải thích do việc truyền các dạng thông tin như video, tiếng nói trong một khu vực nhỏ ít được quan tâm hơn như khi truyền qua những khoảng cách lớn.

Các hệ thống mạng hiện nay ngày càng phức tạp về chất lượng, đa dạng về chủng loại và phát triển rất nhanh về chất. Trong sự phát triển đó số lượng những nhà sản xuất từ phần mềm, phần cứng máy tính, các sản phẩm viễn thông cũng tăng nhanh với nhiều sản phẩm đa dạng. Chính vì vậy vai trò chuẩn hóa cũng mang những ý nghĩa quan trọng. Tại các nước các cơ quan chuẩn quốc gia đã đưa ra các những chuẩn về phần cứng và các quy định về giao tiếp nhằm giúp cho các nhà sản xuất có thể làm ra các sản phẩm có thể kết nối với các sản phẩm do hãng khác sản xuất.

1.4. Các thành phần của mạng máy tính

Mạng máy tính bao gồm các thiết bị phần cứng, các giao thức và các phần mềm mạng. Khi nghiên cứu về mạng máy tính, các vấn đề quan trọng cần được xem xét là giao thức mạng, cấu hình kết nối của mạng và các dịch vụ mạng.

1.4.1. Một số bộ giao thức kết nối mạng

TCP/IP

- Ưu thế chính của bộ giao thức này là khả năng liên kết hoạt động của nhiều loại máy tính khác nhau.

- TCP/IP đã trở thành tiêu chuẩn thực tế cho kết nối liên mạng cũng như kết nối Internet toàn cầu.

NetBEUI

- Bộ giao thức nhỏ, nhanh và hiệu quả được cung cấp theo các sản phẩm của hãng IBM, cũng như sự hỗ trợ của Microsoft.

- Bất lợi chính của bộ giao thức này là không hỗ trợ định tuyến và sử dụng giới hạn ở mạng dựa vào Microsoft.

IPX/SPX

- Đây là bộ giao thức sử dụng trong mạng Novell.

- Ưu thế: nhỏ, nhanh và hiệu quả trên các mạng cục bộ đồng thời hỗ trợ khả năng định tuyến.

DECnet

- Đây là bộ giao thức độc quyền của hãng Digital Equipment Corporation.

- DECnet định nghĩa mô hình truyền thông qua mạng LAN, mạng MAN và WAN. Hỗ trợ khả năng định tuyến

1.4.2. Hệ điều hành mạng - NOS (Network Operating System)

Cùng với sự nghiên cứu và phát triển mạng máy tính, hệ điều hành mạng đã được nhiều công ty đầu tư nghiên cứu và đã công bố nhiều phần mềm quản lý và điều hành mạng có hiệu quả như: NetWare của công ty NOVELL, LAN Manager của Microsoft dùng cho các máy server chạy hệ điều hành OS/2, LAN server của IBM (gần như đồng nhất với LAN Manager), Vines của Banyan Systems là hệ điều hành mạng dùng cho server chạy hệ điều hành UNIX, Promise LAN của Mises Computer chạy trên card điều hợp mạng độc quyền, Windows for Workgroups của Microsoft, LANtastic của Artisoft, NetWare Lite của Novell,....

Một trong những sự lựa chọn cơ bản mà ta phải quyết định trước là hệ điều hành mạng nào sẽ làm nền tảng cho mạng của ta, việc lựa chọn tuỳ thuộc vào kích cỡ của mạng hiện tại và sự phát triển trong tương lai, còn tuỳ thuộc vào những ưu điểm và nhược điểm của từng hệ điều hành.

Một số hệ điều hành mạng phổ biến hiện nay:

Hệ điều hành mạng UNIX: Đây là hệ điều hành do các nhà khoa học xây dựng và được dùng rất phổ biến trong giới khoa học, giáo dục. Hệ điều hành mạng UNIX là hệ điều hành đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt. Nhược điểm của nó là hiện nay có nhiều Version khác nhau, không thống nhất gây khó khăn cho người sử dụng. Ngoài ra hệ điều hành này khá phức tạp lại đòi hỏi cấu hình máy mạnh (trước đây chạy trên máy mini, gần đây có SCO UNIX chạy trên máy vi tính với cấu hình mạnh).

Hệ điều hành mạng Windows NT: Đây là hệ điều hành của hãng Microsoft, cũng là hệ điều hành đa nhiệm, đa người sử dụng. Đặc điểm của nó là tương đối dễ sử dụng, hỗ trợ mạnh cho phần mềm WINDOWS. Do hãng Microsoft là hãng phần mềm lớn nhất thế giới hiện nay, hệ điều hành này có khả năng sẽ được ngày càng phổ biến rộng rãi. Ngoài ra, Windows NT có thể liên kết tốt với máy chủ Novell Netware. Tuy nhiên, để chạy có hiệu quả, Windows NT cũng đòi hỏi cấu hình máy tương đối mạnh.

Hệ điều hành mạng Windows for Workgroup: Đây là hệ điều hành mạng ngang hàng nhỏ, cho phép một nhóm người làm việc (khoảng 3-4 người) dùng chung ổ đĩa trên máy của nhau, dùng chung máy in nhưng không cho phép chạy chung một ứng dụng. Hệ dễ dàng cài đặt và cũng khá phổ biến.

Hệ điều hành mạng NetWare của Novell: Đây là hệ điều hành phổ biến nhất hiện nay ở nước ta và trên thế giới trong thời gian cuối, nó có thể dùng cho các mạng nhỏ (khoảng từ 5-25 máy tính) và cũng có thể dùng cho các mạng lớn gồm hàng trăm máy tính. Trong những năm qua, Novell đã cho ra nhiều phiên bản của Netware: Netware 2.2, 3.11. 4.0 và hiện có 4.1. Netware là một hệ điều hành mạng cục bộ dùng cho các máy vi tính theo chuẩn của IBM hay các máy tính Apple Macintosh, chạy hệ điều hành MS-DOS hoặc OS/2.

Hệ điều hành này tương đối gọn nhẹ, dễ cài đặt (máy chủ chỉ cần thậm chí AT386) do đó phù hợp với hoàn cảnh trang thiết bị hiện tại của nước ta. Ngoài ra, vì là một phần mềm phổ biến nên Novell Netware được các nhà sản xuất phần mềm khác hỗ trợ (theo nghĩa các phân mềm do các hãng phần mềm lớn trên thế giới làm đều có thể chạy tốt trên hệ điều hành mạng này).

1.5. Các lợi ích của mạng máy tính

Mạng tạo khả năng dùng chung tài nguyên cho các người dùng.

Vấn đề là làm cho các tài nguyên trên mạng như chương trình, dữ liệu và thiết bị, đặc biệt là các thiết bị đắt tiền, có thể sẵn dùng cho mọi người trên mạng mà không cần quan tâm đến vị trí thực của tài nguyên và người dùng.

Về mặt thiết bị, các thiết bị chất lượng cao thường đắt tiền, chúng thường được dùng chung cho nhiều người nhằm giảm chi phí và dễ bảo quản.

Về mặt chương trình và dữ liệu, khi được dùng chung, mỗi thay đổi sẽ sẵn dùng cho mọi thành viên trên mạng ngay lập tức. Điều này thể hiện rất rõ tại các nơi như ngân hàng, các đại lý bán vé máy bay...

Mạng cho phép nâng cao độ tin cậy.

Khi sử dụng mạng, có thể thực hiện một chương trình tại nhiều máy tính khác nhau, nhiều thiết bị có thể dùng chung. Điều này tăng độ tin cậy trong công việc vì khi có máy tính hoặc thiết bị bị hỏng, công việc vẫn có thể tiếp tục với các máy tính hoặc thiết bị khác trên mạng trong khi chờ sửa chữa.

Mạng giúp cho công việc đạt hiệu suất cao hơn.

Khi chương trình và dữ liệu đã dùng chung trên mạng, có thể bỏ qua một số khâu đối chiếu không cần thiết. Việc điều chỉnh chương trình (nếu có) cũng tiết kiệm thời gian hơn do chỉ cần cài đặt lại trên một máy.

Về mặt tổ chức, việc sao chép dữ liệu phòng hờ tiện lợi hơn do có thể giao cho chỉ một người thay vì mọi người phải tự sao chép phần của mình.

Tiết kiệm chi phí.

Việc dùng chung các thiết bị ngoại vi cho phép giảm chi phí trang bị tính trên số người dùng. Về phần mềm, nhiều nhà sản xuất phần mềm cung cấp cả những ấn bản cho nhiều người dùng, với chi phí thấp hơn tính trên mỗi người dùng.

Tăng cường tính bảo mật thông tin.

Dữ liệu được lưu trên các máy phục vụ tập tin (file server) sẽ được bảo vệ tốt hơn so với đặt tại các máy cá nhân nhờ cơ chế bảo mật của các hệ điều hành mạng.

Việc phát triển mạng máy tính đã tạo ra nhiều ứng dụng mới

Một số ứng dụng có ảnh hưởng quan trọng đến toàn xã hội: khả năng truy xuất các chương trình và dữ liệu từ xa, khả năng thông tin liên lạc dễ dàng và hiệu quả, tạo môi trường giao tiếp thuận lợi giữa những người dùng khác nhau, khả năng tìm kiếm thông tin nhanh chóng trên phạm vi toàn thế giới,...

1.6. Các dịch vụ phổ biến trên mạng máy tính

Dịch vụ tập tin (File services)

Cho phép chia sẻ tài nguyên thông tin chung, chuyển giao các tập tin dữ liệu từ máy này sang máy khác. Tìm kiếm thông tin và điều khiển truy nhập. Dịch vụ thư điện tử E_Mail (Electronic mail) cung cấp cho người sử dụng phương tiện trao đổi, tranh luận bằng thư điện tử. Dịch vụ thư điện tử giá thành hạ, chuyển phát nhanh, an toàn và nội dung có thể tích hợp các loại dữ liệu.

Dịch vụ in ấn

Có thể dùng chung các máy in đắt tiền trên mạng. Cung cấp khả năng đa truy nhập đến máy in, phục vụ đồng thời cho nhiều nhu cầu in khác nhau. Cung cấp các dịch vụ FAX và quản lý được các trang thiết bị in chuyên dụng.

Các dịch vụ ứng dụng hướng đối tượng

Sử dụng các dịch vụ thông điệp (Message) làm trung gian tác động đến các đối tượng truyền thông. Đối tượng chỉ bàn giao dữ liệu cho tác nhân (Agent) và tác nhân sẽ bàn giao dữ liệu cho đối tượng đích.

Các dịch vụ ứng dụng quản trị luồng công việc trong nhóm làm việc:

Định tuyến các tài liệu điện tử giữa những người trong nhóm. Khi chữ ký điện tử được xác nhận trong các phiên giao dịch thì có thể thay thế được nhiều tiến trình mới hiệu quả và nhanh chóng hơn.

Dịch vụ cơ sở dữ liệu

Là dịch vụ phổ biến về các dịch vụ ứng dụng, là các ứng dụng theo mô hình Client/Server. Dịch vụ xử lý phân tán lưu trữ dữ liệu phân tán trên mạng, người dùng trong suốt và dễ sử dụng, đáp ứng các nhu cầu truy nhập của người sử dụng.

❖ Tóm tắt Chương 1

Trong chương này, một số nội dung chính được giới thiệu:

- Định nghĩa, phân loại mạng máy tính
- So sánh giữa mạng cục bộ và mạng diện rộng
- Các thành phần của mạng máy tính
- Các lợi ích và dịch vụ phổ biến của mạng máy tính

❖ **Câu hỏi:**

- Trắc nghiệm:

Câu 1: Khi sử dụng mạng máy tính ta sẽ được các lợi ích

A. Chia sẻ tài nguyên (cơ sở dữ liệu, máy in, các phần mềm tiện ích, …)

B. Quản lý tập trung, bảo mật và backup tốt

C. Sử dụng các dịch vụ mạng

D. Tất cả đều đúng

Câu 2: Các thành phần tạo nên mạng máy tính là?

A. Máy vi tính

B. Các thiết bị kết nối mạng

C. Giao thức

D. Tất cả đều đúng

Câu 3: Phân loại mạng máy tính theo khoảng cách địa lý có mấy loại?

A. 3

B. 4

C. 5

D. 6

Câu 4: LAN là từ viết tắt của mạng nào?

A. Mạng diện rộng

B. Mạng đô thị

C. Mạng nội bộ

D. Mạng toàn cầu

- Tự luận:

1. Hãy trình bày mục tiêu và ứng dụng mạng máy tính.
2. Hãy phát biểu các lợi ích khi nối máy tính thành mạng.
3. Hãy trình bày tổng quát về xu hướng phát triển các dịch vụ mạng.
4. Hiểu thế nào là mạng máy tính. Hãy trình bày tóm tắt chức năng các thành phần chủ yếu của một mạng máy tính?.

CHƯƠNG 2 –MÔ HÌNH TRUYỀN THÔNG

❖ GIỚI THIỆU CHƯƠNG 2

Chương 2 là phần lý thuyết các kiến thức cơ bản về mô hình truyền thông.

❖ MỤC TIÊU CHƯƠNG 2

Sau khi học xong phần này, người học có khả năng:

➢ ***Về kiến thức:***

- Trình bày được một số kiến thức cơ bản về mô hình truyền thông.
- Hiểu được các mô hình truyền thông phổ biến.

➢ ***Về kỹ năng:***

- Nhận biết, phân loại và so sánhđược mô hình OSI và mô hình TCP/IP.

➢ ***Về năng lực tự chủ và trách nhiệm:***

- Ý thức được tầm quan trọng và ý nghĩa thực tiễn của mô hình truyền thông được sử dụng trong việc truyền và nhận dữ liệu giữa các hệ thống trong mạng máy tính.
- Tích cực, chủ động và hợp tác trong học tập. Thể hiện sự nhiệt tình, trách nhiệm, tác phong nhanh nhẹn trong công việc.

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP CHƯƠNG 2

- Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp); yêu cầu người học thực hiện trả lời câu hỏi và bài tập Chương 2 (cá nhân hoặc nhóm).
- Đối với người học: chủ động đọc trước giáo trình (Chương 2) trước buổi học; hoàn thành đầy đủ bài tập Chương 2 theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.

❖ ĐIỀU KIỆN THỰC HIỆN CHƯƠNG 2

➢ ***Phòng học chuyên môn hóa/nhà xưởng:***

- Phòng học lý thuyết, thực hành được trang bị hệ thống đèn đủ ánh sáng.
- Bàn ghế cho sinh viên.
- Bàn ghế giáo viên, bảng, phấn.

➢ ***Trang thiết bị máy móc:***

- Máy tính, máy chiếu

➢ ***Học liệu, dụng cụ, nguyên vật liệu:***

- Giáo án, bài giảng.
- Giáo trình nội bộ và các tài liệu giảng dạy khác hỗ trợ bài giảng

➢ ***Các điều kiện khác:*** Không có

❖ KIỂM TRA VÀ ĐÁNH GIÁ CHƯƠNG 2

- **Nội dung:**

✓ Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức

✓ Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.

✓ Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ Điểm kiểm tra thường xuyên: 01 bài kiểm tra (hình thức: viết)

✓ Kiểm tra định kỳ: Không có

NỘI DUNG CHƯƠNG 2

2.1. Sự cần thiết phải có mô hình truyền thông

Để một mạng máy tính trở một môi trường truyền dữ liệu thì nó cần phải có những yếu tố sau:

- Mỗi máy tính cần phải có một địa chỉ phân biệt trên mạng.

- Việc chuyển dữ liệu từ máy tính này đến máy tính khác do mạng thực hiện thông qua những quy định thống nhất gọi là giao thức của mạng.

Khi các máy tính trao đổi dữ liệu với nhau thì một quá trình truyền giao dữ liệu đã được thực hiện hoàn chỉnh. Ví dụ như để thực hiện việc truyền một file giữa một máy tính với một máy tính khác cùng được gắn trên một mạng các công việc sau đây phải được thực hiện:

- Máy tính cần truyền cần biết địa chỉ của máy nhận.

- Máy tính cần truyền phải xác định được máy tính nhận đã sẵn sàng nhận thông tin

- Chương trình gửi file trên máy truyền cần xác định được rằng chương trình nhận file trên máy nhận đã sẵn sàng tiếp nhận file.

- Nếu cấu trúc file trên hai máy không giống nhau thì một máy phải làm nhiệm vụ chuyển đổi file từ dạng này sang dạng kia.

- Khi truyền file máy tính truyền cần thông báo cho mạng biết địa chỉ của máy nhận để các thông tin được mạng đưa tới đích.

Điều trên đó cho thấy giữa hai máy tính đã có một sự phối hợp hoạt động ở mức độ cao. Bây giờ thay vì chúng ta xét cả quá trình trên như là một quá trình chung thì chúng ta sẽ chia quá trình trên ra thành một số công đoạn và mỗi công đoạn con hoạt động một cách độc lập với nhau. Ở đây chương trình truyền nhận file của mỗi máy tính được chia thành ba module là: Module truyền và nhận File, Module truyền thông và Module tiếp cận mạng. Hai module tương ứng sẽ thực hiện việc trao đổi với nhau trong đó:

- Module truyền và nhận file cần được thực hiện tất cả các nhiệm vụ trong các ứng dụng truyền nhận file. Ví dụ: truyền nhận thông số về file, truyền nhận các mẫu tin của file, thực hiện chuyển đổi file sang các dạng khác nhau nếu cần. Module truyền và nhận file không cần thiết phải trực tiếp quan tâm tới việc truyền dữ liệu trên mạng như thế nào mà nhiệm vụ đó được giao cho Module truyền thông.

- Module truyền thông quan tâm tới việc các máy tính đang hoạt động và sẵn sàng trao đổi thông tin với nhau. Nó còn kiểm soát các dữ liệu sao cho những dữ liệu này có thể trao đổi một cách chính xác và an toàn giữa hai máy tính. Điều đó có nghĩa là phải truyền file trên nguyên tắc đảm bảo an toàn cho dữ liệu, tuy nhiên ở đây có thể có một vài mức độ an toàn khác nhau được dành cho từng ứng dụng. Ở đây việc trao đổi dữ liệu giữa hai máy tính không phụ thuộc vào bản chất của mạng đang liên kết chúng. Những yêu cầu liên quan đến mạng đã được thực hiện ở module thứ ba là module tiếp cận mạng và nếu mạng thay đổi thì chỉ có module tiếp cận mạng bị ảnh hưởng.

- Module tiếp cận mạng được xây dựng liên quan đến các quy cách giao tiếp với mạng và phụ thuộc vào bản chất của mạng. Nó đảm bảo việc truyền dữ liệu từ máy tính này đến máy tính khác trong mạng.

Như vậy thay vì xét cả quá trình truyền file với nhiều yêu cầu khác nhau như một tiến trình phức tạp thì chúng ta có thể xét quá trình đó với nhiều tiến trình con phân biệt dựa trên việc trao đổi giữa các Module tương ứng trong chương trình truyền file. Cách này cho phép chúng ta phân tích kỹ quá trình file và dễ dàng trong việc viết chương trình.

Việc xét các module một cách độc lập với nhau như vậy cho phép giảm độ phức tạp cho việc thiết kế và cài đặt. Phương pháp này được sử dụng rộng rãi trong việc xây dựng mạng và các chương trình truyền thông và được gọi là phương pháp phân tầng (layer).

Nguyên tắc của phương pháp phân tầng là:

- Mỗi hệ thống thành phần trong mạng được xây dựng như một cấu trúc nhiều tầng và đều có cấu trúc giống nhau như: số lượng tầng và chức năng của mỗi tầng.

- Các tầng nằm chồng lên nhau, dữ liệu được chỉ trao đổi trực tiếp giữa hai tầng kề nhau từ tầng trên xuống tầng dưới và ngược lại.

- Cùng với việc xác định chức năng của mỗi tầng chúng ta phải xác định mối quan hệ giữa hai tầng kề nhau. Dữ liệu được truyền đi từ tầng cao nhất của hệ thống truyền lần lượt đến tầng thấp nhất sau đó truyền qua đường nối vật lý dưới dạng các bit tới tầng thấp nhất của hệ thống nhận, sau đó dữ liệu được truyền ngược lên lần lượt đến tầng cao nhất của hệ thống nhận.

- Chỉ có hai tầng thấp nhất có liên kết vật lý với nhau còn các tầng trên cùng thứ tư chỉ có các liên kết logic với nhau. Liên kết logic của một tầng được thực hiện thông qua các tầng dưới và phải tuân theo những quy định chặt chẽ, các quy định đó được gọi giao thức của tầng.

Hình 2-1: Mô hình phân tầng

2.2. Các nhu cầu về chuẩn hóa đối với mạng

Trong thực tế việc phân chia các tầng như trong mô hình trên thực sự chưa đủ. Trên thế giới hiện có một số cơ quan định chuẩn, họ đưa ra hàng loạt chuẩn về mạng tuy các chuẩn đó có tính chất khuyến nghị chứ không bắt buộc nhưng chúng rất được các cơ quan chuẩn quốc gia coi trọng.

Hai trong số các cơ quan chuẩn quốc tế là:

- **ISO (The International Standards Organization)** - Là tổ chức tiêu chuẩn quốc tế hoạt động dưới sự bảo trợ của Liên hợp Quốc với thành viên là các cơ quan chuẩn

quốc gia với số lượng khoảng hơn 100 thành viên với mục đích hỗ trợ sự phát triển các chuẩn trên phạm vi toàn thế giới. Một trong những thành tựu của ISO trong lãnh vực truyền thông là mô hình hệ thống mở (Open Systems Interconnection - gọi tắt là OSI).

- CCITT (Commité Consultatif International pour le Telegraphe et la Téléphone) - Tổ chức tư vấn quốc tế về điện tín và điện thoại làm việc dưới sự bảo trợ của Liên Hiệp Quốc có trụ sở chính tại Geneva - Thụy sỹ. Các thành viên chủ yếu là các cơ quan bưu chính viễn thông các quốc gia. Tổ chức này có vai trò phát triển các khuyến nghị trong các lãnh vực viễn thông.

2.3. Mô hình OSI (Open Systems Interconnection)

Mô hình OSI là một cơ sở dành cho việc chuẩn hoá các hệ thống truyền thông, nó được nghiên cứu và xây dựng bởi ISO. Việc nghiên cứu về mô hình OSI được bắt đầu tại ISO vào năm 1971 với mục tiêu nhằm tới việc nối kết các sản phẩm của các hãng sản xuất khác nhau và phối hợp các hoạt động chuẩn hoá trong các lĩnh vực viễn thông và hệ thống thông tin. Theo mô hình OSI chương trình truyền thông được chia ra thành 7 tầng với những chức năng phân biệt cho từng tầng. Hai tầng đồng mức khi liên kết với nhau phải sử dụng một giao thức chung.

Việc nghiên cứu về OSI được bắt đầu tại ISO vào năm 1971 với các mục tiêu nhằm nối kết các sản phẩm của các hãng sản xuất khác. Ưu điểm chính của OSI là ở chỗ nó hứa hẹn giải pháp cho vấn đề truyền thông giữa các máy tính không giống nhau. Hai hệ thống, dù có khác nhau đều có thể truyền thông với nhau một các hiệu quả nếu chúng đảm bảo những điều kiện chung sau đây:

- Chúng cài đặt cùng một tập các chức năng truyền thông.

- Các chức năng đó được tổ chức thành cùng một tập các tầng. các tầng đồng mức phải cung cấp các chức năng như nhau.

- Các tầng đồng mức khi trao đổi với nhau sử dụng chung một giao thức

Mô hình OSI tách các mặt khác nhau của một mạng máy tính thành bảy tầng theo mô hình phân tầng. Mô hình OSI là một khung mà các tiêu chuẩn lập mạng khác nhau có thể khớp vào. Mô hình OSI định rõ các mặt nào của hoạt động của mạng có thể nhằm đến bởi các tiêu chuẩn mạng khác nhau. Vì vậy, theo một nghĩa nào đó, mô hình OSI là một loại tiêu chuẩn của các chuẩn.

2.3.1.Nguyên tắc sử dụng khi định nghĩa các tầng hệ thống mở

Sau đây là các nguyên tắc mà ISO quy định dùng trong quá trình xây dựng mô hình OSI:

- Không định nghĩa quá nhiều tầng để việc xác định và ghép nối các tầng không quá phức tạp.

- Tạo các ranh giới các tầng sao cho việc giải thích các phục vụ và số các tương tác qua lại hai tầng là nhỏ nhất.

- Tạo các tầng riêng biệt cho các chức năng khác biệt nhau hoàn toàn về kỹ thuật sử dụng hoặc quá trình thực hiên.

- Các chức năng giống nhau được đặt trong cùng một tầng.

- Lựa chọn ranh giới các tầng tại các điểm mà những thử nghiệm trong quá khứ thành công.

- Các chức năng được xác định sao cho chúng có thể dễ dàng xác định lại, và các nghi thức của chúng có thể thay đổi trên mọi hướng.

- Tạo ranh giới các tầng mà ở đó cần có những mức độ trừu tượng khác nhau trong việc sử dụng số liệu.

- Cho phép thay đổi các chức năng hoặc giao thức trong tầng không ảnh hưởng đến các tầng khác.

- Tạo các ranh giới giữa mỗi tầng với tầng trên và dưới nó.

2.3.2.Các giao thức trong mô hình OSI

Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless).

- Giao thức có liên kết: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết náy, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.

- Giao thức không liên kết: trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

Như vậy với giao thức có liên kết, quá trình truyền thông phải gồm 3 giai đoạn phân biệt:

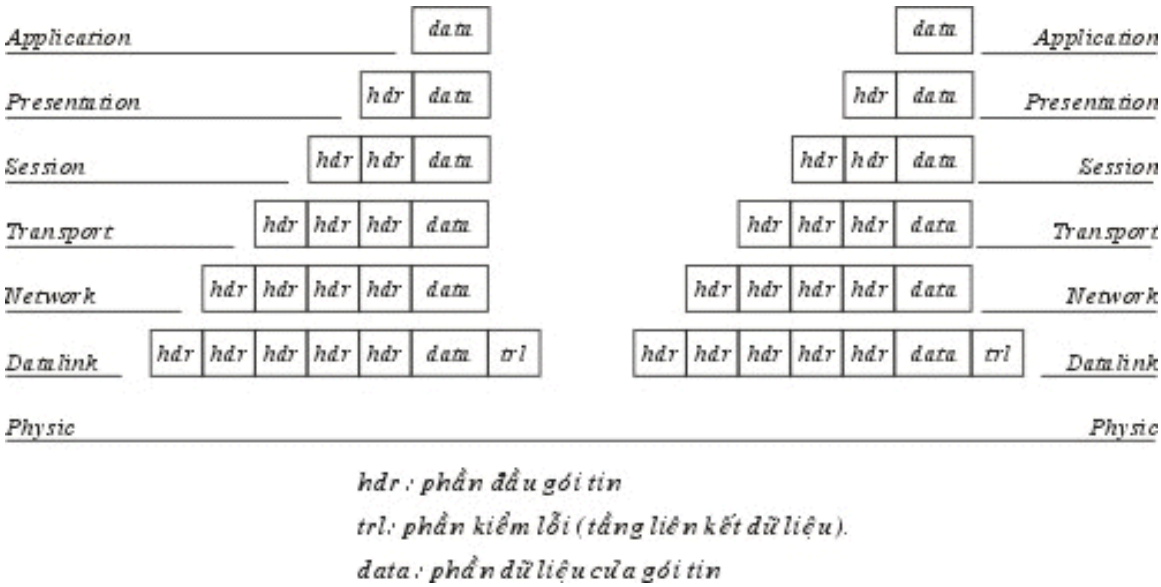
- Thiết lập liên kết (logic): hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).

- Truyền dữ liệu: dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (như kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu...) để tăng cường độ tin cậy và hiệu quả của việc truyền dữ liệu.

- Hủy bỏ liên kết (logic): giải phóng tài nguyên hệ thống đã được cấp phát cho liên kết để dùng cho liên kết khác.

Đối với giao thức không liên kết thì chỉ có duy nhất một giai đoạn truyền dữ liệu mà thôi.

Gói tin của giao thức: Gói tin (Packet) được hiểu như là một đơn vị thông tin dùng trong việc liên lạc, chuyển giao dữ liệu trong mạng máy tính. Những thông điệp (message) trao đổi giữa các máy tính trong mạng, được tạo dạng thành các gói tin ở máy nguồn. Và những gói tin này khi đích sẽ được kết hợp lại thành thông điệp ban đầu. Một gói tin có thể chứa đựng các yêu cầu phục vụ, các thông tin điều khiển và dữ liệu.



Hình 2-2: Phương thức xác lập các gói tin trong mô hình OSI

Trên quan điểm mô hình mạng phân tầng tầng mỗi tầng chỉ thực hiện một chức năng là nhận dữ liệu từ tầng bên trên để chuyển giao xuống cho tầng bên dưới và ngược lại. Chức năng này thực chất là gắn thêm và gỡ bỏ phần đầu (header) đối với các gói tin trước khi chuyển nó đi. Nói cách khác, từng gói tin bao gồm phần đầu (header) và phần dữ liệu. Khi đi đến một tầng mới gói tin sẽ được đóng thêm một phần đầu đề khác và được xem như là gói tin của tầng mới, công việc trên tiếp diễn cho tới khi gói tin được truyền lên đường dây mạng để đến bên nhận.

Tại bên nhận các gói tin được gỡ bỏ phần đầu trên từng tầng tướng ứng và đây cũng là nguyên lý của bất cứ mô hình phân tầng nào.

Chú ý: Trong mô hình OSI phần kiểm lỗi của gói tin tầng liên kết dữ liệu đặt ở cuối gói tin

2.3.3.Các chức năng chủ yếu của các tầng của mô hình OSI.

Tầng 1: Vật lý (Physical)

Tầng vật lý (Physical layer) là tầng dưới cùng của mô hình OSI là. Nó mô tả các đặc trưng vật lý của mạng: Các loại cáp được dùng để nối các thiết bị, các loại đầu nối được dùng , các dây cáp có thể dài bao nhiêu v.v... Mặt khác các tầng vật lý cung cấp các đặc trưng điện của các tín hiệu được dùng để khi chuyển dữ liệu trên cáp từ một máy này đến một máy khác của mạng, kỹ thuật nối mạch điện, tốc độ cáp truyền dẫn.

Tầng vật lý không qui định một ý nghĩa nào cho các tín hiệu đó ngoài các giá trị nhị phân 0 và 1. Ở các tầng cao hơn của mô hình OSI ý nghĩa của các bit được truyền ở tầng vật lý sẽ được xác định.

Ví dụ: Tiêu chuẩn Ethernet cho cáp xoắn đôi 10 baseT định rõ các đặc trưng điện của cáp xoắn đôi, kích thước và dạng của các đầu nối, độ dài tối đa của cáp.

Khác với các tầng khác, tầng vật lý là không có gói tin riêng và do vậy không có phần đầu (header) chứa thông tin điều khiển, dữ liệu được truyền đi theo dòng bit. Một giao thức tầng vật lý tồn tại giữa các tầng vật lý để quy định về phương thức truyền (đồng bộ, phi đồng bộ), tốc độ truyền.

Các giao thức được xây dựng cho tầng vật lý được phân chia thành phân chia thành hai loại giao thức sử dụng phương thức truyền thông dị bộ (asynchronous) và phương thức truyền thông đồng bộ (synchronous).

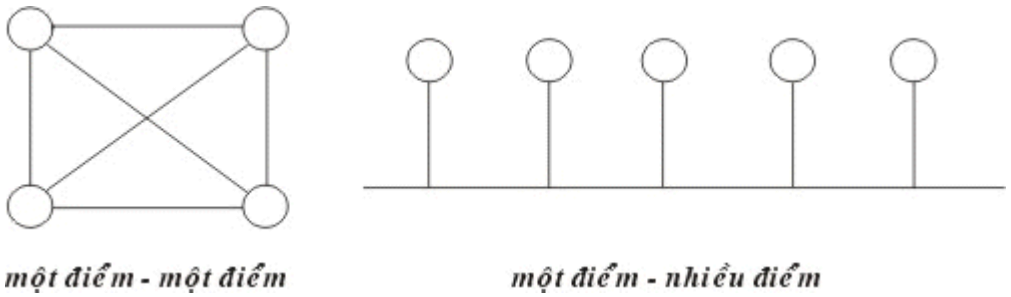
Phương thức truyền dị bộ: Không có một tín hiệu quy định cho sự đồng bộ giữa các bit giữa máy gửi và máy nhận, trong quá trình gửi tín hiệu máy gửi sử dụng các bit đặc biệt START và STOP được dùng để tách các xâu bit biểu diễn các ký tự trong dòng dữ liệu cần truyền đi. Nó cho phép một ký tự được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó.

Phương thức truyền đồng bộ: Sử dụng phương thức truyền cần có đồng bộ giữa máy gửi và máy nhận, nó chèn các ký tự đặc biệt như SYN (Synchronization), EOT (End Of Transmission) hay đơn giản hơn, một cái "cờ " (flag) giữa các dữ liệu của máy gửi để báo hiệu cho máy nhận biết được dữ liệu đang đến hoặc đã đến.

Tầng 2: Liên kết dữ liệu (Data link)

Tầng liên kết dữ liệu (data link layer) là tầng mà ở đó ý nghĩa được gán cho các bít được truyền trên mạng. Tầng liên kết dữ liệu phải quy định được các dạng thức, kích thước, địa chỉ máy gửi và nhận của mỗi gói tin được gửi đi. Nó phải xác định cơ chế truy nhập thông tin trên mạng và phương tiện gửi mỗi gói tin sao cho nó được đưa đến cho người nhận đã định.

Tầng liên kết dữ liệu có hai phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức "một điểm - một điểm" và phương thức "một điểm - nhiều điểm". Với phương thức "một điểm - một điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Phương thức "một điểm - nhiều điểm " tất cả các máy phân chia chung một đường truyền vật lý.



Hình 2-3: Các đường truyền kết nối kiểu "một điểm - một điểm" và "một điểm - nhiều điểm"

Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. Nếu một gói tin có lỗi không sửa được, tầng liên kết dữ liệu phải chỉ ra được cách thông báo cho nơi gửi biết gói tin đó có lỗi để nó gửi lại.

Các giao thức tầng liên kết dữ liệu chia làm 2 loại chính là các giao thức hướng ký tư và các giao thức hướng bit. Các giao thức hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hay EBCDIC), trong khi đó các giao thức hướng bit lại dùng các cấu trúc nhị phân (xâu bit) để xây dựng các phần tử của giao thức (đơn vị dữ liệu, các thủ tục.) và khi nhận, dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

Tầng 3: Mạng (Network)

Tầng mạng (network layer) nhắm đến việc kết nối các mạng với nhau bằng cách tìm đường (routing) cho các gói tin từ một mạng này đến một mạng khác. Nó xác định việc chuyển hướng, vạch đường các gói tin trong mạng, các gói này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng. Nó luôn tìm các tuyến truyền thông không tắc nghẽn để đưa các gói tin đến đích.

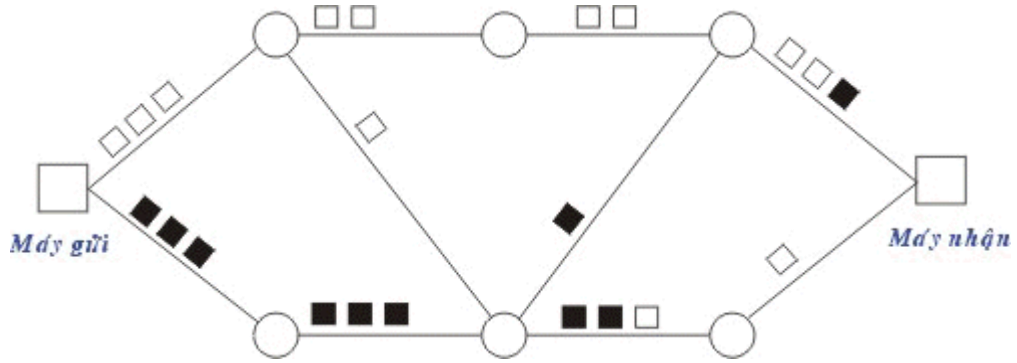
Tầng mạng cung các các phương tiện để truyền các gói tin qua mạng, thậm chí qua một mạng của mạng (network of network). Bởi vậy nó cần phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ cung cấp bởi các mạng khác nhau. hai chức năng chủ yếu của tầng mạng là chọn đường (routing) và chuyển tiếp (relaying). Tầng mạng là quan trọng nhất khi liên kết hai loại mạng khác nhau như mạng Ethernet với mạng Token Ring khi đó phải dùng một bộ tìm đường (quy định bởi tầng mạng) để chuyển các gói tin từ mạng này sang mạng khác và ngược lại.

Đối với một mạng chuyển mạch gói (packet - switched network) - gồm tập hợp các nút chuyển mạch gói nối với nhau bởi các liên kết dữ liệu. Các gói dữ liệu được truyền từ một hệ thống mở tới một hệ thống mở khác trên mạng phải được chuyển qua một chuỗi các nút. Mỗi nút nhận gói dữ liệu từ một đường vào (incoming link) rồi chuyển tiếp nó tới một đường ra (outgoing link) hướng đến đích của dữ liệu. Như vậy ở mỗi nút trung gian nó phải thực hiện các chức năng chọn đường và chuyển tiếp.

Việc chọn đường là sự lựa chọn một con đường để truyền một đơn vị dữ liệu (một gói tin chẳng hạn) từ trạm nguồn tới trạm đích của nó. Một kỹ thuật chọn đường phải thực hiện hai chức năng chính sau đây:

Quyết định chọn đường tối ưu dựa trên các thông tin đã có về mạng tại thời điểm đó thông qua những tiêu chuẩn tối ưu nhất định.

Cập nhật các thông tin về mạng, tức là thông tin dùng cho việc chọn đường, trên mạng luôn có sự thay đổi thường xuyên nên việc cập nhật là việc cần thiết.



Hình 2-4: Mô hình chuyển vận các gói tin trong mạng chuyển mạch gói

Người ta có hai phương thức đáp ứng cho việc chọn đường là phương thức xử lý tập trung và xử lý tại chỗ.

Phương thức chọn đường xử lý tập trung được đặc trưng bởi sự tồn tại của một (hoặc vài) trung tâm điều khiển mạng, chúng thực hiện việc lập ra các bảng đường đi tại từng thời điểm cho các nút và sau đó gửi các bảng chọn đường tới từng nút dọc theo con đường đã được chọn đó. Thông tin tổng thể của mạng cần dùng cho việc chọn đường chỉ cần cập nhập và được cất giữ tại trung tâm điều khiển mạng.

Phương thức chọn đường xử lý tại chỗ được đặc trưng bởi việc chọn đường được thực hiện tại mỗi nút của mạng. Trong từng thời điểm, mỗi nút phải duy trì các thông tin của mạng và tự xây dựng bảng chọn đường cho mình. Như vậy các thông tin tổng thể của mạng cần dùng cho việc chọn đường cần cập nhập và được cất giữ tại mỗi nút.

Thông thường các thông tin được đo lường và sử dụng cho việc chọn đường bao gồm:

- Trạng thái của đường truyền.

- Thời gian trễ khi truyền trên mỗi đường dẫn.

- Mức độ lưu thông trên mỗi đường.

- Các tài nguyên khả dụng của mạng.

Khi có sự thay đổi trên mạng (ví dụ thay đổi về cấu trúc của mạng do sự cố tại một vài nút, phục hồi của một nút mạng, nối thêm một nút mới... hoặc thay đổi về mức độ lưu thông) các thông tin trên cần được cập nhật vào các cơ sở dữ liệu về trạng thái của mạng.

Hiện nay khi nhu cầu truyền thông đa phương tiện (tích hợp dữ liệu văn bản, đồ hoạ, hình ảnh, âm thanh) ngày càng phát triển đòi hỏi các công nghệ truyền dẫn tốc độ cao nên việc phát triển các hệ thống chọn đường tốc độ cao đang rất được quan tâm.

Tầng 4: Vận chuyển (Transport)

Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên. nó là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở. Nó cùng các tầng dưới cung cấp cho người sử dụng các phục vụ vận chuyển.

Tầng vận chuyển (transport layer) là tầng cơ sở mà ở đó một máy tính của mạng chia sẻ thông tin với một máy khác. Tầng vận chuyển đồng nhất mỗi trạm bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm. Tầng vận chuyển cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi. Thông thường tầng vận chuyển đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự.

Tầng vận chuyển là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc rất nhiều vào bản chất của tầng mạng. Người ta chia giao thức tầng mạng thành các loại sau:

- Mạng loại A: Có tỷ suất lỗi và sự cố có báo hiệu chấp nhận được (tức là chất lượng chấp nhận được). Các gói tin được giả thiết là không bị mất. Tầng vận chuyển không cần cung cấp các dịch vụ phục hồi hoặc sắp xếp thứ tự lại.

- Mạng loại B: Có tỷ suất lỗi chấp nhận được nhưng tỷ suất sự cố có báo hiệu lại không chấp nhận được. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra sự cố.

- Mạng loại C: Có tỷ suất lỗi không chấp nhận được (không tin cậy) hay là giao thức không liên kết. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra lỗi và sắp xếp lại thứ tự các gói tin.

Trên cơ sở loại giao thức tầng mạng chúng ta có 5 lớp giao thức tầng vận chuyển đó là:

- Giao thức lớp 0 (Simple Class - lớp đơn giản): cung cấp các khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết trên mạng "có liên kết" loại A. Nó có khả năng phát hiện và báo hiệu các lỗi nhưng không có khả năng phục hồi.

- Giao thức lớp 1 (Basic Error Recovery Class - Lớp phục hồi lỗi cơ bản) dùng với các loại mạng B, ở đây các gói tin (TPDU) được đánh số. Ngoài ra giao thức còn có khả năng báo nhận cho nơi gửi và truyền dữ liệu khẩn. So với giao thức lớp 0 giao thức lớp 1 có thêm khả năng phục hồi lỗi.

- Giao thức lớp 2 (Multiplexing Class - lớp dồn kênh) là một cải tiến của lớp 0 cho phép dồn một số liên kết chuyển vận vào một liên kết mạng duy nhất, đồng thời có thể kiểm soát luồng dữ liệu để tránh tắc nghẽn. Giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi. Do vậy nó cần đặt trên một tầng mạng loại A.

- Giao thức lớp 3 (Error Recovery and Multiplexing Class - lớp phục hồi lỗi cơ bản và dồn kênh) là sự mở rộng giao thức lớp 2 với khả năng phát hiện và phục hồi lỗi, nó cần đặt trên một tầng mạng loại B.

- Giao thức lớp 4 (Error Detection and Recovery Class - Lớp phát hiện và phục hồi lỗi) là lớp có hầu hết các chức năng của các lớp trước và còn bổ sung thêm một số khả năng khác để kiểm soát việc truyền dữ liệu.

Tầng 5: Giao dịch (Session)

Tầng giao dịch (session layer) thiết lập "các giao dịch" giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi thành phần muốn đối thoại với nhau và lập ánh xa giữa các tên với địa chỉ của chúng. Một giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng, tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định.

Tầng giao dịch còn cung cấp cho người sử dụng các chức năng cần thiết để quản trị các giao dịnh ứng dụng của họ, cụ thể là:

- Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách lôgic) các phiên (hay còn gọi là các hội thoại - dialogues)

- Cung cấp các điểm đồng bộ để kiểm soát việc trao đổi dữ liệu.

- Áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.

- Cung cấp cơ chế "lấy lượt" (nắm quyền) trong quá trình trao đổi dữ liệu.

Trong trường hợp mạng là hai chiều luân phiên thì nẩy sinh vấn đề: hai người sử dụng luân phiên phải "lấy lượt" để truyền dữ liệu. Tầng giao dịch duy trì tương tác luân phiên bằng cách báo cho mỗi người sử dụng khi đến lượt họ được truyền dữ liệu. Vấn đề đồng bộ hóa trong tầng giao dịch cũng được thực hiện như cơ chế kiểm tra/phục hồi, dịch vụ này cho phép người sử dụng xác định các điểm đồng bộ hóa trong dòng dữ liệu đang chuyển vận và khi cần thiết có thể khôi phục việc hội thoại bắt đầu từ một trong các điểm đó

Ở một thời điểm chỉ có một người sử dụng đó quyền đặc biệt được gọi các dịch vụ nhất định của tầng giao dịch, việc phân bổ các quyền này thông qua trao đổi thẻ bài (token). Ví dụ: Ai có được token sẽ có quyền truyền dữ liệu, và khi người giữ token trao token cho người khác thi cũng có nghĩa trao quyền truyền dữ liệu cho người đó.

Tầng giao dịch có các hàm cơ bản sau:

- Give Token cho phép người sử dụng chuyển một token cho một người sử dụng khác của một liên kết giao dịch.

- Please Token cho phép một người sử dụng chưa có token có thể yêu cầu token đó.

- Give Control dùng để chuyển tất cả các token từ một người sử dụng sang một người sử dụng khác.

Tầng 6: Trình bày (Presentation)

Trong giao tiếp giữa các ứng dụng thông qua mạng với cùng một dữ liệu có thể có nhiều cách biểu diễn khác nhau. Thông thường dạng biểu diễn dùng bởi ứng dụng nguồn và dạng biểu diễn dùng bởi ứng dụng đích có thể khác nhau do các ứng dụng được chạy trên các hệ thống hoàn toàn khác nhau (như hệ máy Intel và hệ máy Motorola). Tầng trình bày (Presentation layer) phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn chung dùng để truyền thông và cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

Tầng trình bày cũng có thể được dùng kĩ thuật mã hóa để xáo trộn các dữ liệu trước khi được truyền đi và giải mã ở đầu đến để bảo mật. Ngoài ra tầng biểu diễn cũng có thể dùng các kĩ thuật nén sao cho chỉ cần một ít byte dữ liệu để thể hiện thông tin khi nó được truyền ở trên mạng, ở đầu nhận, tầng trình bày bung trở lại để được dữ liệu ban đầu.

Tầng 7: Ứng dụng (Application)

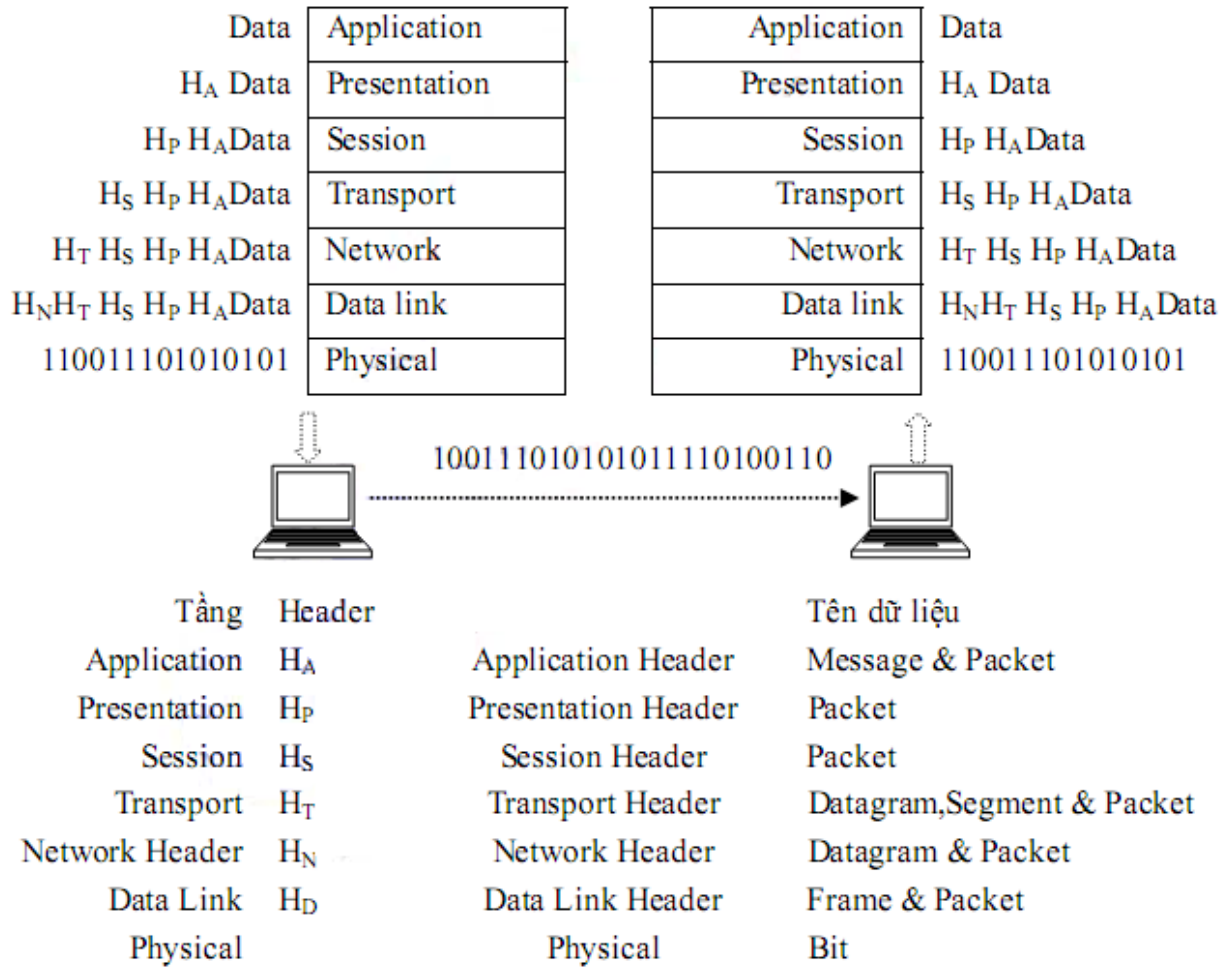
Tầng ứng dụng (Application layer) là tầng cao nhất của mô hình OSI, nó xác định giao diện giữa người sử dụng và môi trường OSI và giải quyết các kỹ thuật mà các chương trình ứng dụng dùng để giao tiếp với mạng.

Để cung cấp phương tiện truy nhập môi trường OSI cho các tiến trình ứng dụng, Người ta thiết lập các thực thể ứng dụng (AE), các thực thể ứng dụng sẽ gọi đến các phần tử dịch vụ ứng dụng (Application Service Element - viết tắt là ASE) của chúng. Mỗi thực thể ứng dụng có thể gồm một hoặc nhiều các phần tử dịch vụ ứng dụng. Các phần tử dịch vụ ứng dụng được phối hợp trong môi trường của thực thể ứng dụng thông qua các liên kết (association) gọi là đối tượng liên kết đơn (Single Association Object - viết tắt là SAO). SAO điều khiển việc truyền thông trong suốt vòng đời của liên kết đó cho phép tuần tự hóa các sự kiện đến từ các ASE thành tố của nó.

2.4. Quá trình chuyển vận gói tin

2.4.1. Quá trình đóng gói dữ liệu (tại máy gửi)

Đóng gói dữ liệu là quá trình đặt dữ liệu nhận được vào sau header (và trước trailer) trên mỗi lớp. Lớp Physical không đóng gói dữ liệu vì nó không dùng header và trailer. Việc đóng gói dữ liệu không nhất thiết phải xảy ra trong mỗi lần truyền dữ liệu của trình ứng dụng. Các lớp 5, 6, 7 sử dụng header trong quá trình khởi động, nhưng trong phần lớn các lần truyền thì không có header của lớp 5, 6, 7 lý do là không có thông tin mới để trao đổi.



Tầng	Header		Tên dữ liệu
Application	H_A	Application Header	Message & Packet
Presentation	H_P	Presentation Header	Packet
Session	H_S	Session Header	Packet
Transport	H_T	Transport Header	Datagram,Segment & Packet
Network Header	H_N	Network Header	Datagram & Packet
Data Link	H_D	Data Link Header	Frame & Packet
Physical		Physical	Bit

Hình 2-5: Bổ sung phần đầu thông điệp & tên dữ liệu sử dụng

Các dữ liệu tại máy gửi được xử lý theo trình tự như sau:

- Người dùng thông qua lớp Application để đưa các thông tin vào máy tính. Các thông tin này có nhiều dạng khác nhau như: hình ảnh, âm thanh, văn bản…

- Tiếp theo các thông tin đó được chuyển xuống lớp Presentation để chuyển thành dạng chung, rồi mã hoá và nén dữ liệu.

- Tiếp đó dữ liệu được chuyển xuống lớp Session để bổ sung các thông tin về phiên giao dịch này.

- Dữ liệu tiếp tục được chuyển xuống lớp Transport, tại lớp này dữ liệu được cắt ra thành nhiều Segment và bổ sung thêm các thông tin về phương thức vận chuyển dữ liệu để đảm bảo độ tin cậy khi truyền.

- Dữ liệu tiếp tục được chuyển xuống lớp Network, tại lớp này mỗi Segment được cắt ra thành nhiều Packet và bổ sung thêm các thông tin định tuyến.

- Tiếp đó dữ liệu được chuyển xuống lớp Data Link, tại lớp này mỗi Packet sẽ được cắt ra thành nhiều Frame và bổ sung thêm các thông tin kiểm tra gói tin (để kiểm tra ở nơi nhận).

- Cuối cùng, mỗi Frame sẽ được tầng Vật Lý chuyển thành một chuỗi các bit, và được đẩy lên các phương tiện truyền dẫn để truyền đến các thiết bị khác.

2.4.2. Quá trình truyền dữ liệu từ máy gửi đến máy nhận.

Bước 1: Trình ứng dụng (trên máy gửi) tạo ra dữ liệu và các chương trình phần cứng, phần mềm cài đặt mỗi lớp sẽ bổ sung vào header và trailer (quá trình đóng gói dữ liệu tại máy gửi).

Bước 2: Lớp Physical (trên máy gửi) phát sinh tín hiệu lên môi trường truyền tải để truyền dữ liệu.

Bước 3: Lớp Physical (trên máy nhận) nhận dữ liệu.

Bước 4: Các chương trình phần cứng, phần mềm (trên máy nhận) gỡ bỏ header và trailer và xử lý phần dữ liệu (quá trình xử lý dữ liệu tại máy nhận).

Giữa bước 1 và bước 2 là quá trình tìm đường đi của gói tin. Thông thường, máy gửi đã biết địa chỉ IP của máy nhận. Vì thế, sau khi xác định được địa chỉ IP của máy nhận thì lớp Network của máy gửi sẽ so sánh địa chỉ IP của máy nhận và địa chỉ IP của chính nó:

- Nếu cùng địa chỉ mạng thì máy gửi sẽ tìm trong bảng MAC Table của mình để có được địa chỉ MAC của máy nhận. Trong trường hợp không có được địa chỉ MAC tương ứng, nó sẽ thực hiện giao thức ARP để truy tìm địa chỉ MAC. Sau khi tìm được địa chỉ MAC, nó sẽ lưu địa chỉ MAC này vào trong bảng MAC Table để lớp Datalink sử dụng ở các lần gửi sau. Sau khi có địa chỉ MAC thì máy gửi sẽ gởi gói tin đi.

- Nếu khác địa chỉ mạng thì máy gửi sẽ kiểm tra xem máy có được khai báo Default Gateway hay không.

+ Nếu có khai báo Default Gateway thì máy gửi sẽ gởi gói tin thông qua Default Gateway.

+ Nếu không có khai báo Default Gateway thì máy gởi sẽ loại bỏ gói tin và thông báo "Destination host Unreachable"

2.4.3. Chi tiết quá trình xử lý tại máy nhận

Bước 1: Lớp Physical kiểm tra quá trình đồng bộ bit và đặt chuỗi bit nhận được vào vùng đệm. Sau đó thông báo cho lớp Data Link dữ liệu đã được nhận.

Bước 2: Lớp Data Link kiểm lỗi frame bằng cách kiểm tra FCS trong trailer. Nếu có lỗi thì frame bị bỏ.

Sau đó kiểm tra địa chỉ lớp Data Link (địa chỉ MAC) xem có trùng với địa chỉ máy nhận hay không. Nếu đúng thì phần dữ liệu sau khi loại header và trailer sẽ được chuyển lên cho lớp Network.

Bước 3: Địa chỉ lớp Network được kiểm tra xem có phải là địa chỉ máy nhận hay không (địa chỉ IP) ? Nếu đúng thì dữ liệu được chuyển lên cho lớp Transport xử lý.

Bước 4: Nếu giao thức lớp Transport có hỗ trợ việc phục hồi lỗi thì số định danh phân đoạn được xử lý. Các thông tin ACK, NAK (gói tin ACK, NAK dùng để phản hồi về việc các gói tin đã được gởi đến máy nhận chưa) cũng được xử lý ở lớp này. Sau quá trình phục hồi lỗi và sắp thứ tự các phân đoạn, dữ liệu được đưa lên lớp Session.

Bước 5: Lớp Session đảm bảo một chuỗi các thông điệp đã trọn vẹn. Sau khi các luồng đã hoàn tất, lớp Session chuyển dữ liệu sau header lớp 5 lên cho lớp Presentation xử lý.

Bước 6: Dữ liệu sẽ được lớp Presentation xử lý bằng cách chuyển đổi dạng thức dữ liệu. Sau đó kết quả chuyển lên cho lớp Application.

Bước 7: Lớp Application xử lý header cuối cùng. Header này chứa các tham số thoả thuận giữa hai trình ứng dụng. Do vậy tham số này thường chỉ được trao đổi lúc khởi động quá trình truyền thông giữa hai trình ứng dụng.

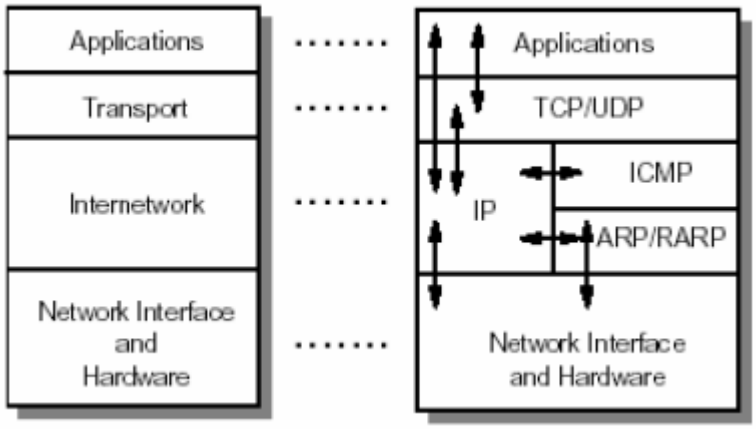
2.5. Mô hình TCP/IP

2.5.1. Tổng quan về bộ giao thức TCP/IP

TCP/IP là bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau. Ngày nay, TCP/IP được sử dụng rộng rãi trong các mạng cục bộ cũng như trên mạng Internet toàn cầu.

TCP/IP được xem là giản lược của mô hình tham chiếu OSI với bốn tầng như sau:

- Tầng liên kết mạng (Network Access Layer)
- Tầng Internet (Internet Layer)
- Tầng giao vận (Host-to-Host Transport Layer)
- Tầng ứng dụng (Application Layer)



Hình 2-6: Kiến trúc TCP/IP

Tầng liên kết:

Tầng liên kết (còn được gọi là tầng liên kết dữ liệu hay là tầng giao tiếp mạng) là tầng thấp nhất trong mô hình TCP/IP, bao gồm các thiết bị giao tiếp mạng và chương trình cung cấp các thông tin cần thiết để có thể hoạt động, truy nhập đường truyền vật lý qua thiết bị giao tiếp mạng đó.

Tầng Internet:

Tầng Internet (còn gọi là tầng mạng) xử lý qua trình truyền gói tin trên mạng. Các giao thức của tầng này bao gồm: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Messages Protocol).

Tầng giao vận:

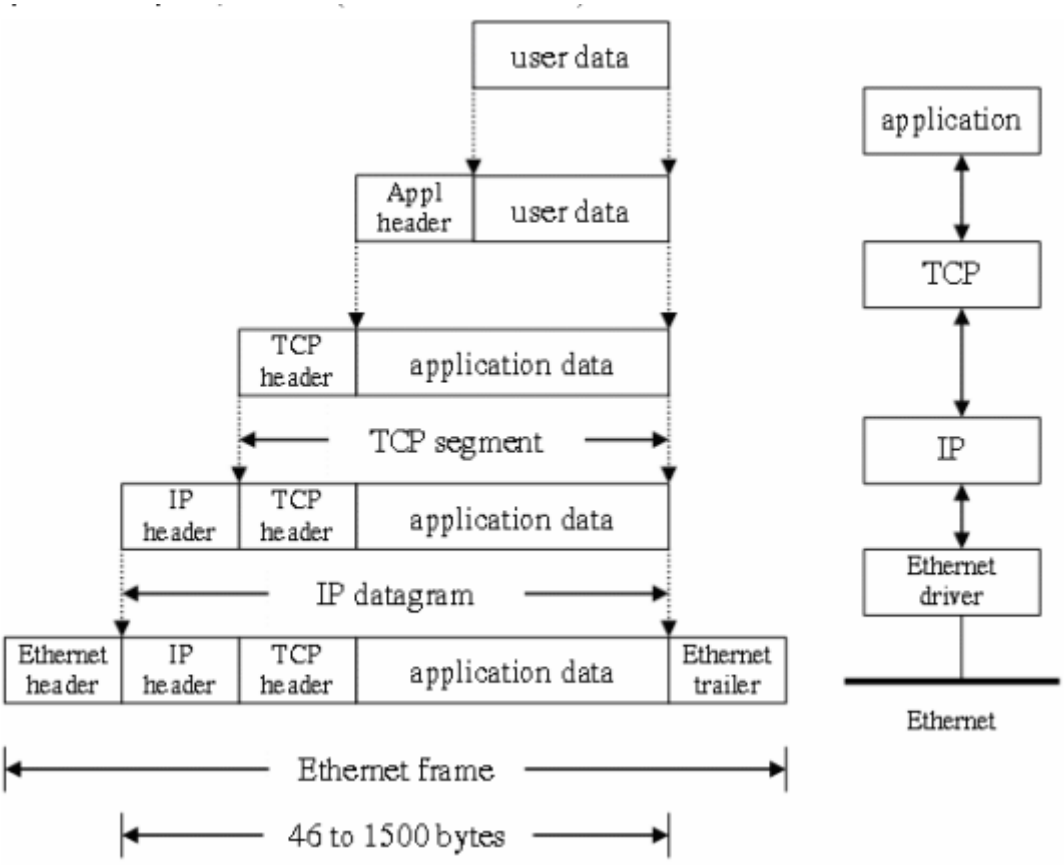
Tầng giao vận phụ trách luồng dữ liệu giữa hai trạm thực hiện các ứng dụng của tầng trên. Tầng này có hai giao thức chính: TCP (Transmission Control Protocol) và UDP (User Datagram Protocol)

TCP cung cấp một luồng dữ liệu tin cậy giữa hai trạm, nó sử dụng các cơ chế như chia nhỏ các gói tin của tầng trên thành các gói tin có kích thước thích hợp cho tầng mạng bên dưới, báo nhận gói tin,đặt hạn chế thời gian time-out để đảm bảo bên nhận biết được các gói tin đã gửi đi. Do tầng này đảm bảo tính tin cậy, tầng trên sẽ không cần quan tâm đến nữa.

UDP cung cấp một dịch vụ đơn giản hơn cho tầng ứng dụng. Nó chỉ gửi các gói dữ liệu từ trạm này tới trạm kia mà không đảm bảo các gói tin đến được tới đích. Các cơ chế đảm bảo độ tin cậy cần được thực hiện bởi tầng trên.

Tầng ứng dụng:

Tầng ứng dụng là tầng trên cùng của mô hình TCP/IP bao gồm các tiến trình và các ứng dụng cung cấp cho người sử dụng để truy cập mạng. Có rất nhiều ứng dụng được cung cấp trong tầng này, mà phổ biến là: Telnet: sử dụng trong việc truy cập mạng từ xa, FTP (File Transfer Protocol): dịch vụ truyền tệp, Email: dịch vụ thư tín điện tử, WWW (World Wide Web).



Hình 2-7: Quá trình đóng/mở gói dữ liệu trong TCP/IP

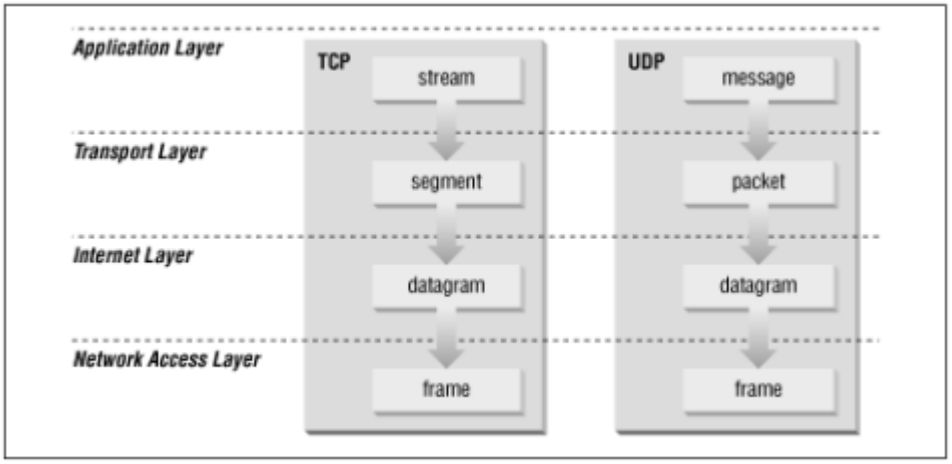
Cũng tương tự như trong mô hình OSI, khi truyền dữ liệu, quá trình tiến hành từ tầng trên xuống tầng dưới, qua mỗi tầng dữ liệu được thêm vào một thông tin điều khiển được gọi là phần header. Khi nhận dữ liệu thì quá trình xảy ra ngược lại, dữ liệu được truyền từ tầng dưới lên và qua mỗi tầng thì phần header tương ứng được lấy đi và khi đến tầng trên cùng thì dữ liệu không còn phần header nữa. Hình vẽ sau cho ta thấy lược đồ dữ liệu qua các tầng. Trong hình vẽ này ta thấy tại các tầng khác nhau dữ liệu được mang những thuật ngữ khác nhau:

- Trong tầng ứng dụng dữ liệu là các luồng được gọi là stream.

- Trong tầng giao vận, đơn vị dữ liệu mà TCP gửi xuống tầng dưới gọi là TCP segment.

- Trong tầng mạng, dữ liệu mà IP gửi tới tầng dưới được gọi là IP datagram.

- Trong tầng liên kết, dữ liệu được truyền đi gọi là frame.



Hình 2-8: Cấu trúc dữ liệu trong TCP/IP

2.5.2. So sánh TCP/IP với OSI

Mỗi tầng trong TCP/IP có thể là một hay nhiều tầng của OSI.

Bảng sau chỉ rõ mối tương quan giữa các tầng trong mô hình TCP/IP với OSI

OSI	TCP/IP
Physical Layer và Data link Layer	Data link Layer
Network Layer	Internet Layer
Transport Layer	Transport Layer
Session Layer, Presentation Layer, Application Layer	Application Layer

Sự khác nhau giữa TCP/IP và OSI chỉ là:

- Tầng ứng dụng trong mô hình TCP/IP bao gồm luôn cả 3 tầng trên của mô hình OSI

- Tầng giao vận trong mô hình TCP/IP không phải luôn đảm bảo độ tin cậy của việc truyền tin như ở trong tầng giao vận của mô hình OSI mà cho phép thêm một lựa chọn khác là UDP

❖ Tóm tắt Chương 2

Trong chương này, một số nội dung chính được giới thiệu:

- Sự cần thiết phải có mô hình truyền thông

- Các nhu cầu chuẩn hóa đối với mạng

- Mô hình OSI và mô hình TCP/IP
- Quá trình chuyển vận gói tin

❖ **Câu hỏi:**

- Trắc nghiệm:

Câu 1: Tầng nào trong mô hình OSI làm việc với các tín hiệu điện

A. Tầng mạng **B.** Tầng liên kết dữ liệu

C. Tầng vận chuyển **D.** Tầng Vật lý

Câu 2: Thứ tự các tầng của mô hình OSI theo thứ tự dưới lên trên là:

A.Physical-Data Link-Network-Transport-Session-Presentation-Application

B. Physical-Data Link-Network-Transport-Session-Application- Presentation

C. Physical-Network-Data Link-Transport-Session-Application- Presentation

D. Physical-Data Link-Network-Session-Transport-Presentation-Application

Câu 3: Mô hình OSI có bao nhiêu tầng?

A. 4 **B.** 5 **C.** 6 **D.** 7

Câu 4: Tầng mạng (Network Layer) là tầng thứ mấy trong mô hình OSI

A. 3 **B.** 4 **C.** 5 **D.** 6

Câu 5: Nhiệm vụ nào dưới đây không phải là của tầng mạng (Network Layer):

A. Định địa chỉ logic **B.** Định tuyến

C. Định địa chỉ vật lý **D.** Định địa chỉ logic và Định tuyến

- Tự luận:

1. Trình bày các nguyên tắc truyền thông đồng tầng
2. Giao diện tầng, quan hệ các tầng kề nhau và dịch vụ
3. Trình bày khái niệm dịch vụ và dịch vụ liên kết, dịch vụ không liên kết
4. Vai trò và chức năng chủ yếu các tầng phiên (Session Layer)
5. Vai trò & chức năng tầng vận chuyển (Transport Layer)
6. Vai trò & chức năng tầng mạng (Network Layer)
7. Vai trò & chức năng tầng liên kết dữ liệu (Data link Layer)
8. Hiểu thế nào là thực thể tầng vật lý và dịch vụ tầng vât lý.
9. Giao thức tầng vật lý khác với giao thức các tầng khác như thế nào ?

CHƯƠNG 3 – THIẾT BỊ MẠNG

❖ GIỚI THIỆU CHƯƠNG 3

Chương 3 là phần lý thuyết và thực hành các kiến thức cơ bản về môi trường truyền dẫn và các thiết bị mạng phổ biến.

❖ MỤC TIÊU CHƯƠNG 3

Sau khi học xong phần này, người học có khả năng:

➢ ***Về kiến thức:***

- Trình bày được một số loại cáp mạng, thiết bị mạng phổ biến.
- Hiểu được các chuẩn bấm dây cáp mạng và kỹ thuật bấm dây cáp mạng xoắn đôi.

➢ ***Về kỹ năng:***

- Nhận biết được một số loại cáp mạng, thiết bị mạng phổ biến.
- Thực hiện được kỹ thuật bấm dây cáp mạng, lắp đặt hệ thống mạng nội bộ.

➢ ***Về năng lực tự chủ và trách nhiệm:***

- Ý thức được tầm quan trọng và ý nghĩa thực tiễn của môi trường truyền dẫn và các thiết bị mạng phổ biến trong lắp đặt và cài đặt hệ thống mạng máy tính.
- Tích cực, chủ động và hợp tác trong học tập. Thể hiện sự nhiệt tình, trách nhiệm, tác phong nhanh nhẹn trong công việc.

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP CHƯƠNG 3

- Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp); yêu cầu người học thực hiện trả lời câu hỏi và bài tập Chương 3 (cá nhân hoặc nhóm).
- Đối với người học: chủ động đọc trước giáo trình (Chương 3) trước buổi học; hoàn thành đầy đủ bài tập Chương 3 theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.

❖ ĐIỀU KIỆN THỰC HIỆN CHƯƠNG 3

➢ ***Phòng học chuyên môn hóa/nhà xưởng:***

- Phòng học lý thuyết, thực hành được trang bị hệ thống đèn đủ ánh sáng.
- Bàn ghế cho sinh viên.
- Bàn ghế giáo viên, bảng, phấn.

➢ ***Trang thiết bị máy móc:***

- Máy tính, máy chiếu

➢ ***Học liệu, dụng cụ, nguyên vật liệu:***

- Giáo án, bài giảng.
- Dây mạng, kìm bấm mạng, các đầu nối RJ45, Hub, Switch, Router
- Giáo trình nội bộ và các tài liệu giảng dạy khác hỗ trợ bài giảng

➢ ***Các điều kiện khác:*** Không có

❖ KIỂM TRA VÀ ĐÁNH GIÁ CHƯƠNG 3

- **Nội dung:**

✓ Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức

✓ Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.

✓ Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ Điểm kiểm tra thường xuyên: Không có

✓ Kiểm tra định kỳ: Không có

NỘI DUNG CHƯƠNG 3

3.1. Môi trường truyền dẫn

3.1.1. Khái niệm

Trên một mạng máy tính, các dữ liệu được truyền trên một môi trường truyền dẫn (transmission media), nó là phương tiện vật lý cho phép truyền tải tín hiệu giữa các thiết bị. Có hai loại phương tiện truyền dẫn chủ yếu:

- Hữu tuyến (bounded media)

- Vô tuyến (boundless media)

Thông thường hệ thống mạng sử dụng hai loại tín hiệu là: digital và analog.

3.1.2. Tần số truyền thông

Phương tiện truyền dẫn giúp truyền các tín hiệu điện tử từ máy tính này sang máy tính khác. Các tín hiệu điện tử này biểu diễn các giá trị dữ liệu theo dạng các xung nhị phân (bật/tắt). Các tín hiệu truyền thông giữa các máy tính và các thiết bị là các dạng sóng điện từ trải dài từ tần số radio đến tần số hồng ngoại.

Các sóng tần số radio thường được dùng để phát tín hiệu LAN. Các tần số này có thể được dùng với cáp xoắn đôi, cáp đồng trục hoặc thông qua việc truyền phủ sóng radio.

Sóng viba (microware) thường dùng truyền thông tập trung giữa hai điểm hoặc giữa các trạm mặt đất và các vệ tinh, ví dụ như mạng điện thoại cellular.

Tia hồng ngoại thường dùng cho các kiểu truyền thông qua mạng trên các khoảng cách tương đối ngắn và có thể phát được sóng giữa hai điểm hoặc từ một điểm phủ sóng cho nhiều trạm thu. Chúng ta có thể truyền tia hồng ngoại và các tần số ánh sáng cao hơn thông qua cáp quang.

3.1.3. Các đặc tính của phương tiện truyền dẫn

Mỗi phương tiện truyền dẫn đều có những tính năng đặc biệt thích hợp với mỗi kiểu dịch vụ cụ thể, nhưng thông thường chúng ta quan tâm đến những yếu tố sau:

- Chi phí

- Yêu cầu cài đặt

- Độ bảo mật

- Băng thông (bandwidth): được xác định bằng tổng lượng thông tin có thể truyền dẫn trên đường truyền tại một thời điểm. Băng thông là một số xác định, bị giới hạn bởi phương tiện truyền dẫn, kỹ thuật truyền dẫn và thiết bị mạng được sử dụng. Băng thông là một trong những thông số dùng để phân tích độ hiệu quả của đường mạng. Đơn vị của băng thông:

+ Bps (Bits per second-số bit trong một giây): đây là đơn vị cơ bản của băng thông.

+ KBps (Kilobits per second): 1 KBps=103 bps=1000 Bps

+ MBps (Megabits per second): 1 MBps = 103 KBps

+ GBps (Gigabits per second): 1 GBps = 103 MBps

+ TBps (Terabits per second): 1 TBps = 103 GBPS.

- Thông lượng (Throughput): lượng thông tin thực sự được truyền dẫn trên thiết bị tại một thời điểm.

- Băng tầng cơ sở (baseband): dành toàn bộ băng thông cho một kênh truyền, băng tầng mở rộng (broadband):cho phép nhiều kênh truyền chia sẻ một phương tiện truyền dẫn (chia sẻ băng thông).

- Độ suy giảm (attenuation): độ đo sự suy yếu đi của tín hiệu khi di chuyển trên một phương tiện truyền dẫn. Các nhà thiết kế cáp phải chỉ định các giới hạn về chiều dài dây cáp vì khi cáp dài sẽ dẫn đến tình trạng tín hiệu yếu đi mà không thể phục hồi được.

- Nhiễu điện từ (Electromagnetic interference - EMI): bao gồm các nhiễu điện từ bên ngoài làm biến dạng tín hiệu trong một phương tiện truyền dẫn.

- Nhiễu xuyên kênh (crosstalk): hai dây dẫn đặt kề nhau làm nhiễu lẫn nhau.

3.1.4. Các kiểu truyền dẫn.

Có các kiểu truyền dẫn như sau:

- Đơn công (Simplex): Trong kiểu truyền dẫn này, thiết bị phát tín hiệu và thiết bị nhận tín hiệu được phân biệt rõ ràng, thiết bị phát chỉ đảm nhiệm vai trò phát tín hiệu, còn thiết bị thu chỉ đảm nhiệm vai trò nhận tín hiệu. Truyền hình là một ví dụ của kiểu truyền dẫn này.

- Bán song công (Half-Duplex): trong kiểu truyền dẫn này, thiết bị có thể là thiết bị phát, vừa là thiết bị thu. Nhưng tại một thời điểm thì chỉ có thể ở một trạng thái (phát hoặc thu). Bộ đàm là thiết bị hoạt động ở kiểu truyền dẫn này.

- Song công (Full-Duplex): trong kiểu truyền dẫn này, tại một thời điểm, thiết bị có thể vừa phát vừa thu. Điện thoại là một minh họa cho kiểu truyền dẫn này.

3.2.Đường cáp truyền mạng

Đường cáp truyền mạng là cơ sở hạ tầng của một hệ thống mạng, nên nó rất quan trọng và ảnh hưởng rất nhiều đến khả năng hoạt động của mạng. Hiện nay người ta thường dùng 3 loại dây cáp là cáp xoắn cặp, cáp đồng trục và cáp quang.

3.2.1. Cáp xoắn cặp

Đây là loại cáp gồm hai đường dây dẫn đồng được xoắn vào nhau nhằm làm giảm nhiễu điện từ gây ra bởi môi trường xung quanh và giữa chúng với nhau.

Hiện nay có hai loại cáp xoắn là cáp có bọc kim loại (STP - Shield Twisted Pair) và cáp không bọc kim loại (UTP -Unshield Twisted Pair).

- Cáp có bọc kim loại (STP): Lớp bọc bên ngoài có tác dụng chống nhiễu điện từ, có loại có một đôi giây xoắn vào nhau và có loại có nhiều đôi giây xoắn với nhau.

- Cáp không bọc kim loại (UTP): Tính tương tự như STP nhưng kém hơn về khả năng chống nhiễu và suy hao vì không có vỏ bọc.

STP và UTP có các loại (Category - Cat) thường dùng:

- Loại 1 & 2 (Cat 1 & Cat 2): Thường dùng cho truyền thoại và những đường truyền tốc độ thấp (nhỏ hơn 4Mb/s).

- Loại 3 (Cat 3): tốc độ truyền dữ liệu khoảng 16 Mb/s , nó là chuẩn cho hầu hết các mạng điện thoại.

- Loại 4 (Cat 4): Thích hợp cho đường truyền 20Mb/s.

- Loại 5 (Cat 5): Thích hợp cho đường truyền 100Mb/s.

- Loại 6 (Cat 6): Thích hợp cho đường truyền 300Mb/s.

Đây là loại cáp rẻ, dễ cài đặt tuy nhiên nó dễ bị ảnh hưởng của môi trường.

3.2.2. Cáp đồng trục

Cáp đồng trục có hai đường dây dẫn và chúng có cùng một trục chung, một dây dẫn trung tâm (thường là dây đồng cứng) đường dây còn lại tạo thành đường ống bao xung quanh dây dẫn trung tâm (dây dẫn này có thể là dây bện kim loại và vì nó có chức năng chống nhiễu nên còn gọi là lớp bọc kim). Giữa hai dây dẫn trên có một lớp cách ly, và bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp.

Các loại cáp	**Dây xoắn cặp**	**Cáp đồng trục mỏng**	**Cáp đồng trục dày**	**Cáp quang**
Chi tiết	Bằng đồng, có 4 và 25 cặp dây (loại 3, 4, 5)	Bằng đồng, 2 dây, đường kính 5mm	Bằng đồng, 2 dây, đường kính 10mm	Thủy tinh, 2 sợi
Loại kết nối	RJ-25 hoặc 50-pin telco	BNC	N-series	ST
Chiều dài đoạn tối đa	100m	185m	500m	1000m
Số đầu nối tối đa trên 1 đoạn	2	30	100	2
Chạy 10 Mbit/s	Được	Được	Được	Được
Chạy 100 Mbit/s	Được	Không	Không	Được
Chống nhiễu	Tốt	Tốt	Rất tốt	Hoàn toàn
Bảo mật	Trung bình	Trung bình	Trung bình	Hoàn toàn

Độ tin cậy	Tốt	Trung bình	Tốt	Tốt
Lắp đặt	Dễ dàng	Trung bình	Khó	Khó
Khắc phục lỗi	Tốt	Dở	Dở	Tốt
Quản lý	Dễ dàng	Khó	Khó	Trung bình
Chi phí cho 1 trạm	Rất thấp	Thấp	Trung bình	Cao
Ứng dụng tốt nhất	Hệ thống Workgroup	Đường backbone	Đường backbone trong tủ mạng	Đường backbone dài trong tủ mạng hoặc các tòa nhà

Bảng 3-1 Tính năng kỹ thuật của một số loại cáp mạng

Cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác (ví dụ như cáp xoắn đôi) do ít bị ảnh hưởng của môi trường. Các mạng cục bộ sử dụng cáp đồng trục có thể có kích thước trong phạm vi vài ngàn mét, cáp đồng trục được sử dụng nhiều trong các mạng dạng đường thẳng. Hai loại cáp thường được sử dụng là cáp đồng trục mỏng và cáp đồng trục dày trong đường kính cáp đồng trục mỏng là 0,25 inch, cáp đồng trục dày là 0,5 inch. Cả hai loại cáp đều làm việc ở cùng tốc độ nhưng cáp đồng trục mỏng có độ hao suy tín hiệu lớn hơn

Hiện nay có cáp đồng trục sau:

- RG -58,50 ohm: dùng cho mạng Thin Ethernet

- RG -59,75 ohm: dùng cho truyền hình cáp

- RG -62,93 ohm: dùng cho mạng ARCnet

Các mạng cục bộ thường sử dụng cáp đồng trục có dải thông từ 2,5 - 10 Mb/s, cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác vì nó có lớp vỏ bọc bên ngoài, độ dài thông thường của một đoạn cáp nối trong mạng là 200m, thường sử dụng cho dạng Bus.

3.2.3. Cáp sợi quang (Fiber - Optic Cable)

Cáp sợi quang bao gồm một dây dẫn trung tâm (là một hoặc một bó sợi thủy tinh có thể truyền dẫn tín hiệu quang) được bọc một lớp vỏ bọc có tác dụng phản xạ các tín hiệu trở lại để giảm sự mất mát tín hiệu. Bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp. Như vậy cáp sợi quang không truyền dẫn các tín hiệu điện mà chỉ truyền các tín hiệu quang (các tín hiệu dữ liệu phải được chuyển đổi thành các tín hiệu quang và khi nhận chúng sẽ lại được chuyển đổi trở lại thành tín hiệu điện).

Cáp quang có đường kính từ 8.3 - 100 micron, Do đường kính lõi sợi thuỷ tinh có kích thước rất nhỏ nên rất khó khăn cho việc đấu nối, nó cần công nghệ đặc biệt với kỹ thuật cao đòi hỏi chi phí cao.

Dải thông của cáp quang có thể lên tới hàng Gbps và cho phép khoảng cách đi cáp khá xa do độ suy hao tín hiệu trên cáp rất thấp. Ngoài ra, vì cáp sợi quang không dùng tín hiệu điện từ để truyền dữ liệu nên nó hoàn toàn không bị ảnh hưởng của nhiễu điện từ và tín hiệu truyền không thể bị phát hiện và thu trộm bởi các thiết bị điện tử của người khác.

Chỉ trừ nhược điểm khó lắp đặt và giá thành còn cao , nhìn chung cáp quang thích hợp cho mọi mạng hiện nay và sau này.

3.2.4. Các yêu cầu cho một hệ thống cáp

An toàn, thẩm mỹ: Tất cả các dây mạng phải được bao bọc cẩn thận, cách xa các nguồn điện, các máy có khả năng phát sóng để tránh trường hợp bị nhiễu. Các đầu nối phải đảm bảo chất lượng, tránh tình trạng hệ thống mạng bị chập chờn.

Đúng chuẩn: Hệ thống cáp phải thực hiện đúng chuẩn, đảm bảo cho khả năng nâng cấp sau này cũng như dễ dàng cho việc kết nối các thiết bị khác nhau của các nhà sản xuất khác nhau. Tiêu chuẩn quốc tế dùng cho các hệ thống mạng hiện nay là EIA/TIA 568B.

Tiết kiệm và "linh hoạt" (flexible): Hệ thống cáp phải được thiết kế sao cho kinh tế nhất, dễ dàng trong việc di chuyển các trạm làm việc và có khả năng mở rộng sau này.

3.3. Đường truyền vô tuyến

Khi dùng các loại cáp ta gặp một số khó khăn như cơ sở cài đặt cố định, khoảng cách không xa, vì vậy để khắc phục những khuyết điểm trên người ta dùng đường truyền vô tuyến. Đường truyền vô tuyến mang lại những lợi ích sau:

- Cung cấp nối kết tạm thời với mạng cáp có sẵn.

- Những người liên tục di chuyển vẫn nối kết vào mạng dùng cáp.

- Lắp đặt đường truyền vô tuyến ở những nơi địa hình phức tạp không thể đi dây được.

- Phù hợp cho những nơi phục vụ nhiều kết nối cùng một lúc cho nhiều khách hàng. Ví dụ như: Dùng đường vô tuyến cho phép khách hàng ở sân bay kết vào mạng để duyệt Internet.

- Dùng cho những mạng có giới hạn rộng lớn vượt quá khả năng cho phép của cáp đồng và cáp quang.

- Dùng làm kết nối dự phòng cho các kết nối hệ thống cáp.

Tuy nhiên, đường truyền vô tuyến cũng có một số hạn chế:

- Tín hiệu không an toàn.

- Dễ bị nghe lén.

- Khi có vật cản thì tín hiệu suy yếu rất nhanh.

- Băng thông không cao.

3.3.1. Sóng vô tuyến (radio)

Sóng radio nằm trong phạm vi từ 10 KHz đến 1 GHz, trong miền này ta có rất nhiều dải tần ví dụ như: sóng ngắn, VHF (dùng cho tivi và radio FM), UHF (dùng cho tivi). Tại mỗi quốc gia, nhà nước sẽ quản lý cấp phép sử dụng các băng tần để tránh tình trạng các sóng bị nhiễu. Nhưng có một số băng tần được chỉ định là vùng tự do có nghĩa là chúng ta dùng nhưng không cần đăng ký (vùng này thường có dải tần 2,4 Ghz). Tận dụng lợi điểm này các thiết bị Wireless của các hãng như Cisco, Compex đều dùng ở dải tần này. Tuy nhiên, chúng ta sử dụng tần số không cấp phép sẽ có nguy cơ nhiễu nhiều hơn.

3.3.2. Sóng viba

Truyền thông viba thường có hai dạng: truyền thông trên mặt đất và các nối kết với vệ tinh. Miền tần số của viba mặt đất khoảng 21-23 GHz, các kết nối vệ tinh khoảng 11-14 Mhz. Băng thông từ 1-10 MBps.

Sự suy yếu tín hiệu tùy thuộc vào điều kiện thời tiết, công suất và tần số phát. Chúng dễ bị nghe trộm nên thường được mã hóa.

3.3.3. Hồng ngoại

Tất cả mạng vô tuyến hồng ngoại đều hoạt động bằng cách dùng tia hồng ngoại để truyền tải dữ liệu giữa các thiết bị. Phương pháp này có thể truyền tín hiệu ở tốc độ cao do dải thông cao của tia hồng ngoại. Thông thường mạng hồng ngoại có thể truyền với tốc độ từ 1-10 Mbps. Miền tần số từ 100 Ghz đến 1000 GHz. Có bốn loại mạng hồng ngoại:

- Mạng đường ngắm: mạng này chỉ truyền khi máy phát và máy thu có một đường ngắm rõ rệt giữa chúng.

- Mạng hồng ngoại tán xạ: kỹ thuật này phát tia truyền dội tường và sàn nhà rồi mới đến máy thu. Diện tích hiệu dụng bị giới hạn ở khoảng 100 feet (35m) và có tín hiệu chậm do hiện tượng dội tín hiệu.

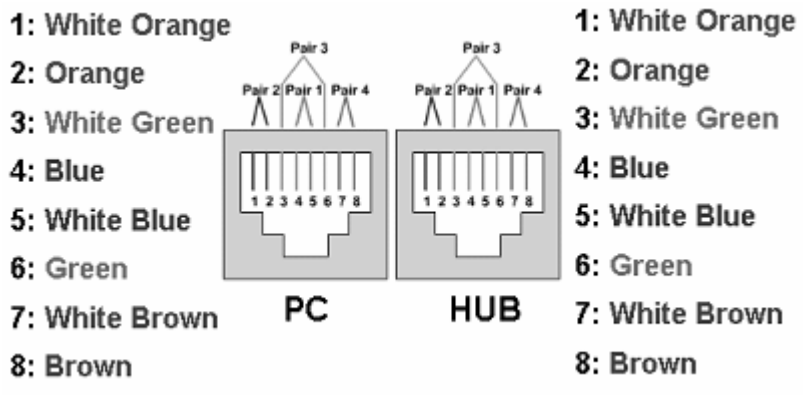
- Mạng phản xạ: ở loại mạng hồng ngoại này, máy thu-phát quang đặt gần máy tính sẽ truyền tới một vị trí chung, tại đây tia truyền được đổi hướng đến máy tính thích hợp.

- Broadband optical telepoint: loại mạng cục bộ vô tuyến hồng ngoại cung cấp các dịch vụ dải rộng. Mạng vô tuyến này có khả năng xử lý các yêu cầu đa phương tiện chất lượng cao, vốn có thể trùng khớp với các yêu cầu đa phương tiện của mạng cáp.

3.4. Các kỹ thuật bấm cáp mạng

3.4.1. Kỹ thuật bấm dây cáp mạng thẳng

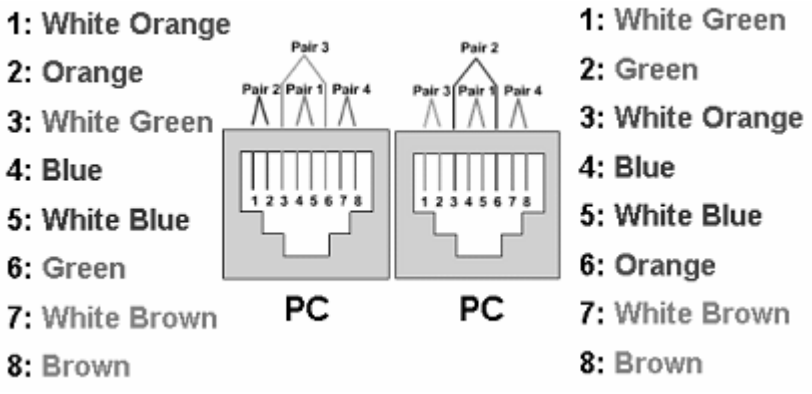
Cáp thẳng (Straight-through cable): là cáp dùng để nối PC và các thiết bị mạng như Hub, Switch, Router… Cáp thẳng theo chuẩn 10/100 Base-T dùng hai cặp dây xoắn nhau và dùng chân 1, 2, 3, 6 trên đầu RJ45. Cặp dây xoắn thứ nhất nối vào chân 1, 2, cặp xoắn thứ hai nối vào chân 3, 6. Đầu kia của cáp dựa vào màu nối vào chân của đầu RJ45 và nối tương tự.



Hình 3-1: Cách đấu dây thẳng.

3.4.2. Kỹ thuật bấm dây cáp mạng chéo

Cáp chéo (Crossover cable): là cáp dùng nối trực tiếp giữa hai thiết bị giống nhau như PC – PC, Hub – Hub, Switch – Switch. Cáp chéo trật tự dây cũng giống như cáp thẳng nhưng đầu dây còn lại phải chéo cặp dây xoắn sử dụng (vị trí thứ nhất đổi với vị trí thứ 3, vị trí thứ hai đổi với vị trí thứ sáu) .

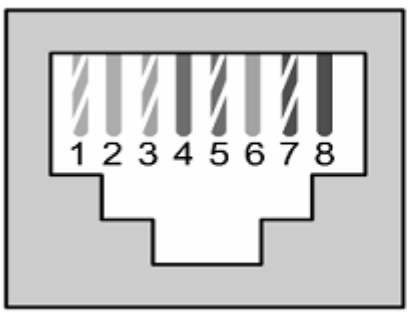


Hình 3-2: Cách đấu dây chéo.

Cáp Console: Dùng để nối PC vào các thiết bị mạng chủ yếu dùng để cấu hình các thiết bị. Thông thường khoảng cách dây Console ngắn nên chúng ta không cần chọn cặp dây xoắn, mà chọn theo màu từ 1-8 sao cho dễ nhớ và đầu bên kia ngược lại từ 8-1.

ANSI (Viện tiêu chuẩn quốc gia Hoa kỳ), TIA (hiệp hội công nghiệp viễn thông), EIA (hiệp hội công nghiệp điện tử) đã đưa ra 2 cách xếp đặt vị trí dây như sau:

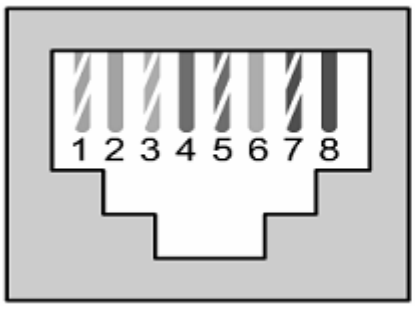
- Chuẩn T568-A (còn gọi là Chuẩn A):



1. Trắng Xanh lá cây (White Green)
2. Xanh lá cây (Green)
3. Trắng Cam (White Orange)
4. Xanh đậm (Blue)
5. Trắng Xanh đậm (White Blue)
6. Cam (Orange)
7. Trắng Nâu (White Brown)
8. Nâu (Brown)

Hình 3-3: Chuẩn T568-A

- Chuẩn T568-B (còn gọi là Chuẩn B):



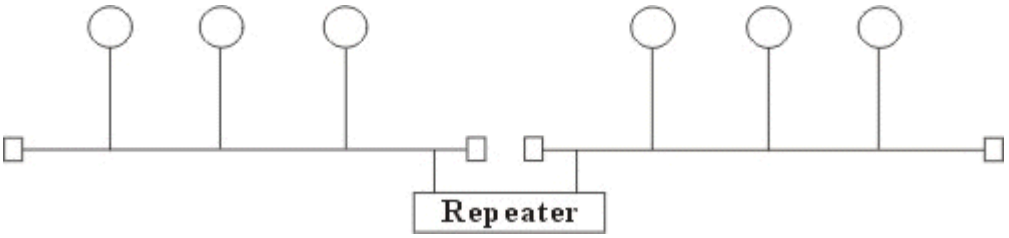
1. Trắng Cam (White Orange)
2. Cam (Orange)
3. Trắng Xanh lá cây (White Green)
4. Xanh đậm (Blue)
5. Trắng Xanh đậm (White Blue)
6. Xanh lá cây (Green)
7. Trắng Nâu (White Brown)
8. Nâu (Brown)

Hình 3-4: Chuẩn T568-B

3.5. Các thiết bị liên kết mạng

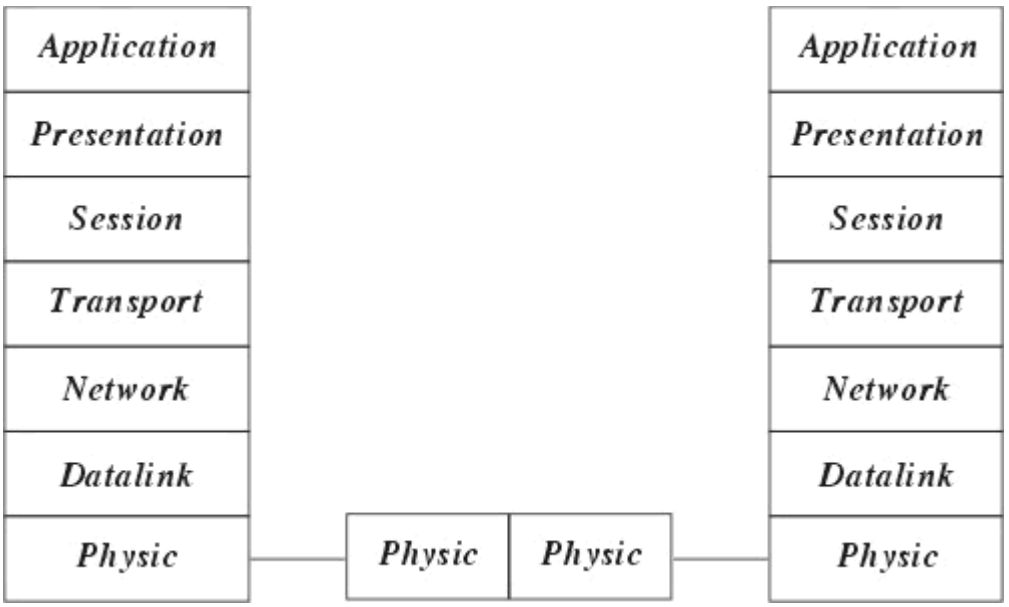
3.5.1. Repeater (Bộ tiếp sức)

Repeater là loại thiết bị phần cứng đơn giản nhất trong các thiết bị liên kết mạng, nó được hoạt động trong tầng vật lý của mô hình hệ thống mở OSI. Repeater dùng để nối 2 mạng giống nhau hoặc các phần một mạng cùng có một nghi thức và một cấu hình. Khi Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.



Hình 3-5: Mô hình liên kết mạng của Repeater.

Repeater không có xử lý tín hiệu mà nó chỉ loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao (vì đã được phát với khoảng cách xa) và khôi phục lại tín hiệu ban đầu. Việc sử dụng Repeater đã làm tăng thêm chiều dài của mạng.



Hình 3-6: Hoạt động của bộ tiếp sức trong mô hình OSI

Hiện nay có hai loại Repeater đang được sử dụng là Repeater điện và Repeater điện quang.

Repeater điện nối với đường dây điện ở cả hai phía của nó, nó nhận tín hiệu điện từ một phía và phát lại về phía kia. Khi một mạng sử dụng Repeater điện để nối các phần của mạng lại thì có thể làm tăng khoảng cách của mạng, nhưng khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu. Ví dụ với mạng sử dụng cáp đồng trục 50 thì khoảng cách tối đa là 2.8 km, khoảng cách đó không thể kéo thêm cho dù sử dụng thêm Repeater.

Repeater điện quang liên kết với một đầu cáp quang và một đầu là cáp điện, nó chuyển một tín hiệu điện từ cáp điện ra tín hiệu quang để phát trên cáp quang và ngược lại. Việc sử dụng Repeater điện quang cũng làm tăng thêm chiều dài của mạng.

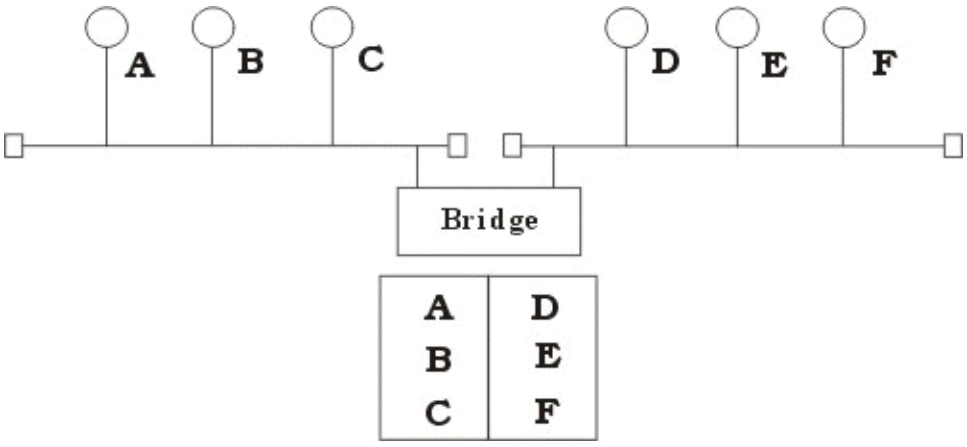
Việc sử dụng Repeater không thay đổi nội dung các tín hiện đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa Repeater không làm thay đổi khối lượng chuyển vận trên mạng nên việc sử dụng không tính toán nó trên mạng lớn sẽ hạn chế hiệu năng của mạng. Khi lựa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ chuyển vận phù hợp với tốc độ của mạng.

3.5.2. Bridge (Cầu nối)

Bridge là một thiết bị có xử lý dùng để nối hai mạng giống nhau hoặc khác nhau, nó có thể được dùng với các mạng có các giao thức khác nhau. Cầu nối hoạt động trên tầng liên kết dữ liệu nên không như bộ tiếp sức phải phát lại tất cả những gì nó nhận được thì cầu nối đọc được các gói tin của tầng liên kết dữ liệu trong mô hình OSI và xử lý chúng trước khi quyết định có chuyển đi hay không.

Khi nhận được các gói tin Bridge chọn lọc và chỉ chuyển những gói tin mà nó thấy cần thiết. Điều này làm cho Bridge trở nên có ích khi nối một vài mạng với nhau và cho phép nó hoạt động một cách mềm dẻo.

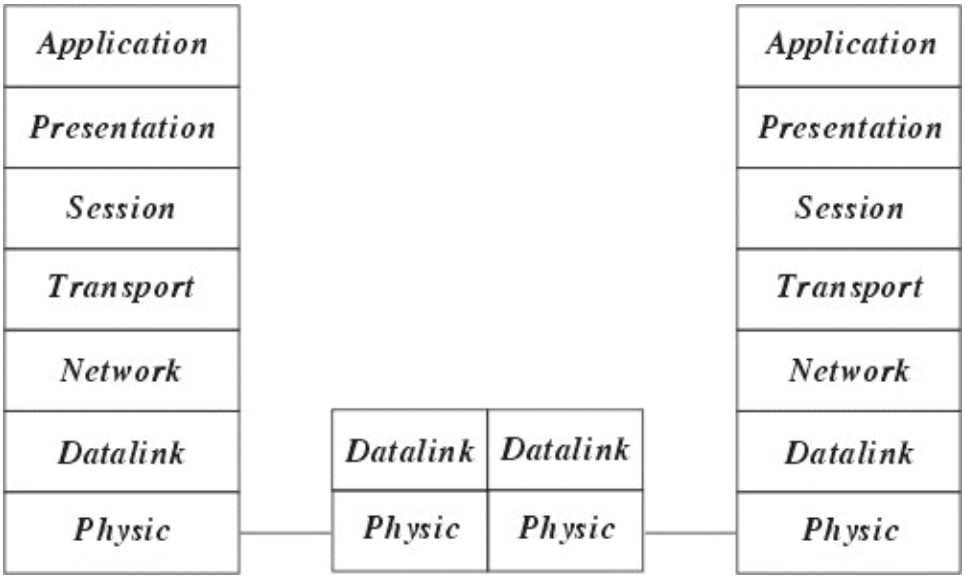
Để thực hiện được điều này trong Bridge ở mỗi đầu kết nối có một bảng các địa chỉ các trạm được kết nối vào phía đó, khi hoạt động cầu nối xem xét mỗi gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và bổ xung bảng địa chỉ.



Hình 3-7: Hoạt động của Bridge

Khi đọc địa chỉ nơi gửi Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu không có thì Bridge tự động bổ xung bảng địa chỉ (cơ chế đó được gọi là tự học của cầu nối).

Khi đọc địa chỉ nơi nhận Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu có thì Bridge sẽ cho rằng đó là gói tin nội bộ thuộc phần mạng mà gói tin đến nên không chuyển gói tin đó đi, nếu ngược lại thì Bridge mới chuyển sang phía bên kia. Ở đây chúng ta thấy một trạm không cần thiết chuyển thông tin trên toàn mạng mà chỉ trên phần mạng có trạm nhận mà thôi.



Hình 3-8: Hoạt động của Bridge trong mô hình OSI

Để đánh giá một Bridge người ta đưa ra hai khái niệm : Lọc và chuyển vận. Quá trình xử lý mỗi gói tin được gọi là quá trình lọc trong đó tốc độ lọc thể hiện trực tiếp khả năng hoạt động của Bridge. Tốc độ chuyển vận được thể hiện số gói tin/giây trong đó thể hiện khả năng của Bridge chuyển các gói tin từ mạng này sang mạng khác.

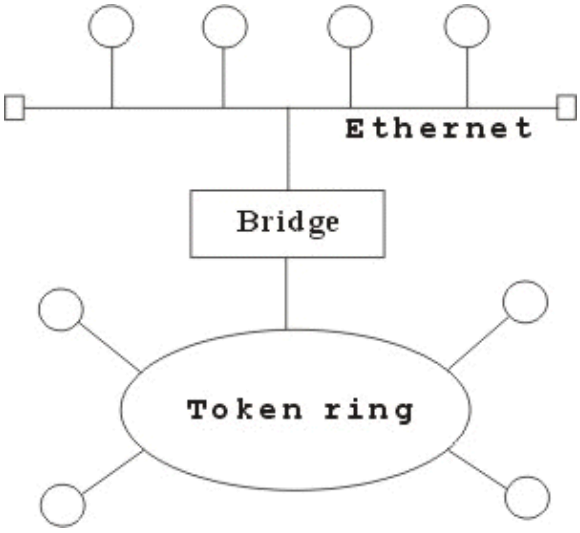
Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch. Bridge vận chuyển dùng để nối hai mạng cục bộ cùng sử dụng một giao thức truyền thông của tầng liên kết dữ liệu, tuy nhiên mỗi mạng có thể sử dụng loại dây nối khác nhau. Bridge vận chuyển không có khả năng thay đổi cấu trúc các gói tin mà nó nhận được mà chỉ quan tâm tới việc xem xét và chuyển vận gói tin đó đi.

Bridge biên dịch dùng để nối hai mạng cục bộ có giao thức khác nhau nó có khả năng chuyển một gói tin thuộc mạng này sang gói tin thuộc mạng kia trước khi chuyển qua

Ví dụ : Bridge biên dịch nối một mạng Ethernet và một mạng Token ring. Khi đó Cầu nối thực hiện như một nút token ring trên mạng Token ring và một nút Enthernet trên mạng Ethernet. Cầu nối có thể chuyển một gói tin theo chuẩn đang sử dụng trên mạng Enthernet sang chuẩn đang sử dụng trên mạng Token ring.

Tuy nhiên chú ý ở đây cầu nối không thể chia một gói tin ra làm nhiều gói tin cho nên phải hạn chế kích thước tối đa các gói tin phù hợp với cả hai mạng. Ví dụ như kích thước tối đa của gói tin trên mạng Ethernet là 1500 bytes và trên mạng Token ring là

6000 bytes do vậy nếu một trạm trên mạng token ring gửi một gói tin cho trạm trên mạng Ethernet với kích thước lớn hơn 1500 bytes thì khi qua cầu nối số lượng byte dư sẽ bị chặt bỏ.



Hình 3-9: Ví dụ về Bridge biên dịch

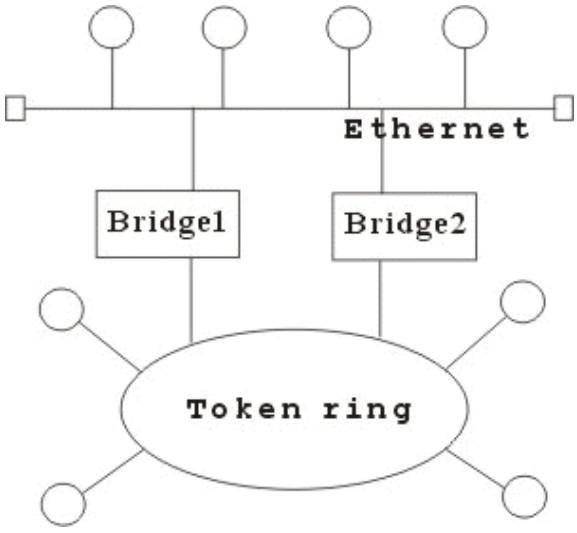
Người ta sử dụng Bridge trong các trường hợp sau :

- Mở rộng mạng hiện tại khi đã đạt tới khoảng cách tối đa do Bridge sau khi sử lý gói tin đã phát lại gói tin trên phần mạng còn lại nên tín hiệu tốt hơn bộ tiếp sức.

- Giảm bớt tắc nghẽn mạng khi có quá nhiều trạm bằng cách sử dụng Bridge, khi đó chúng ta chia mạng ra thành nhiều phần bằng các Bridge, các gói tin trong nội bộ tùng phần mạng sẽ không được phép qua phần mạng khác.

- Để nối các mạng có giao thức khác nhau.

Một vài Bridge còn có khả năng lựa chọn đối tượng vận chuyển. Nó có thể chỉ chuyển vận những gói tin của những địa chỉ xác định. Ví dụ : cho phép gói tin của máy A, B qua Bridge 1, gói tin của máy C, D qua Bridge 2.



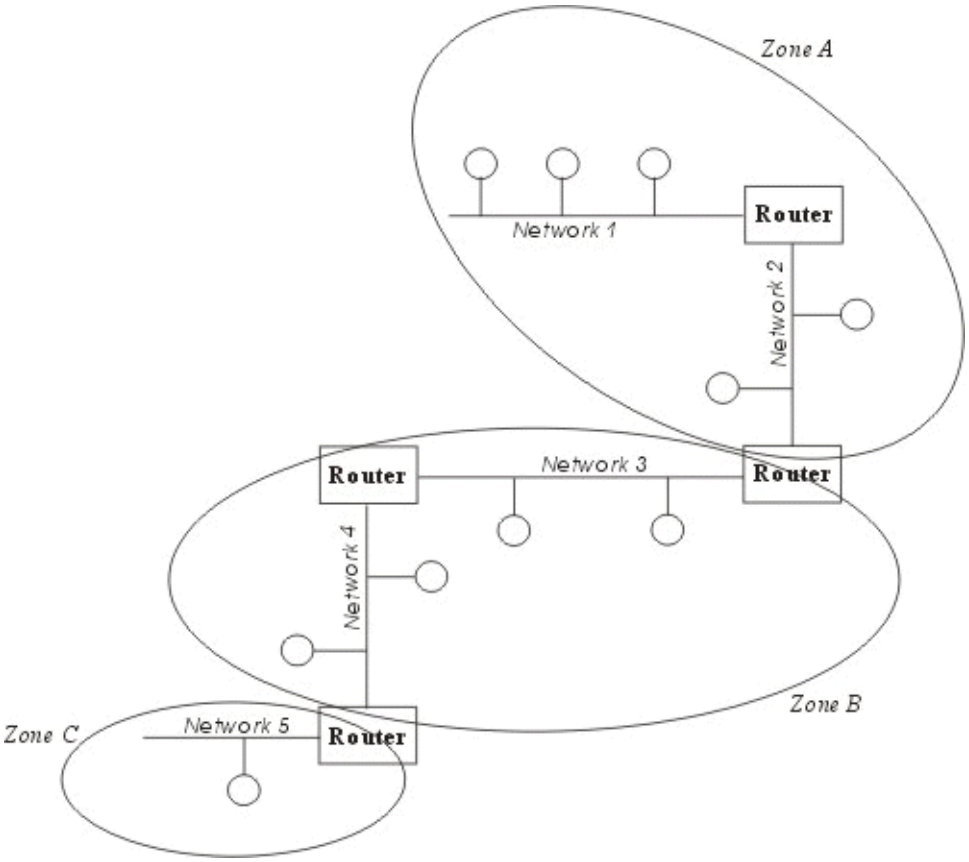
Hình 3-10: Liên kết mạng với 2 Bridge

Một số Bridge được chế tạo thành một bộ riêng biệt, chỉ cần nối dây và bật. Các Bridge khác chế tạo như card chuyên dùng cắïm vào máy tính, khi đó trên máy tính sẽ sử

dụng phần mềm Bridge. Việc kết hợp phần mềm với phần cứng cho phép uyển chuyển hơn trong hoạt động của Bridge.

3.5.3. Router (Bộ tìm đường)

Router là một thiết bị hoạt động trên tầng mạng, nó có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng cuối. Router có thể được sử dụng trong việc nối nhiều mạng với nhau và cho phép các gói tin có thể đi theo nhiều đường khác nhau để tới đích.



Hình 3-11: Hoạt động của Router.

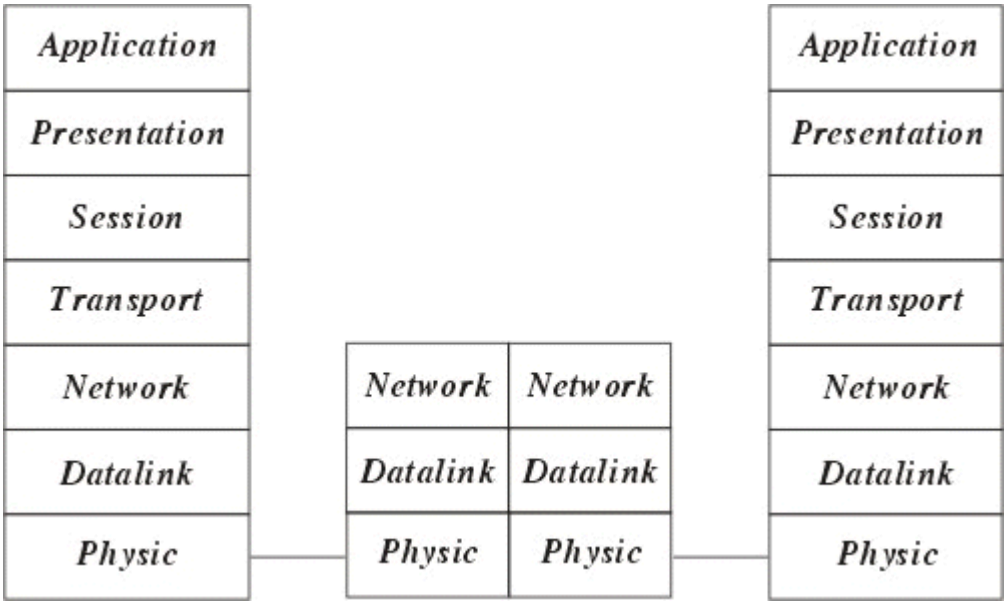
Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong gói tin đó phải chứa các thông tin khác về đích đến) và khi gói tin đến Router thì Router mới xử lý và gửi tiếp.

Khi xử lý một gói tin Router phải tìm được đường đi của gói tin qua mạng. Để làm được điều đó Router phải tìm được đường đi tốt nhất trong mạng dựa trên các thông tin nó có về mạng, thông thường trên mỗi Router có một bảng chỉ đường (Router table). Dựa trên dữ liệu về Router gần đó và các mạng trong liên mạng, Router tính được bảng chỉ đường (Router table) tối ưu dựa trên một thuật toán xác định trước.

Người ta phân chia Router thành hai loại là Router có phụ thuộc giao thức (The protocol dependent routers) và Router không phụ thuộc vào giao thức (The protocol independent router) dựa vào phương thức xử lý các gói tin khi qua Router.

Router có phụ thuộc giao thức: Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác chứ không chuyển đổi phương cách đóng gói của gói tin cho nên cả hai mạng phải dùng chung một giao thức truyền thông.

Router không phụ thuộc vào giao thức: có thể liên kết các mạng dùng giao thức truyền thông khác nhau và có thể chuyển đôi gói tin của giao thức này sang gói tin của giao thức kia, Router cũng chấp nhận kích thước các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).



Hình 3-3: Hoạt động của Router trong mô hình OSI

Để ngăn chặn việc mất mát số liệu Router còn nhận biết được đường nào có thể chuyển vận và ngừng chuyển vận khi đường bị tắc.

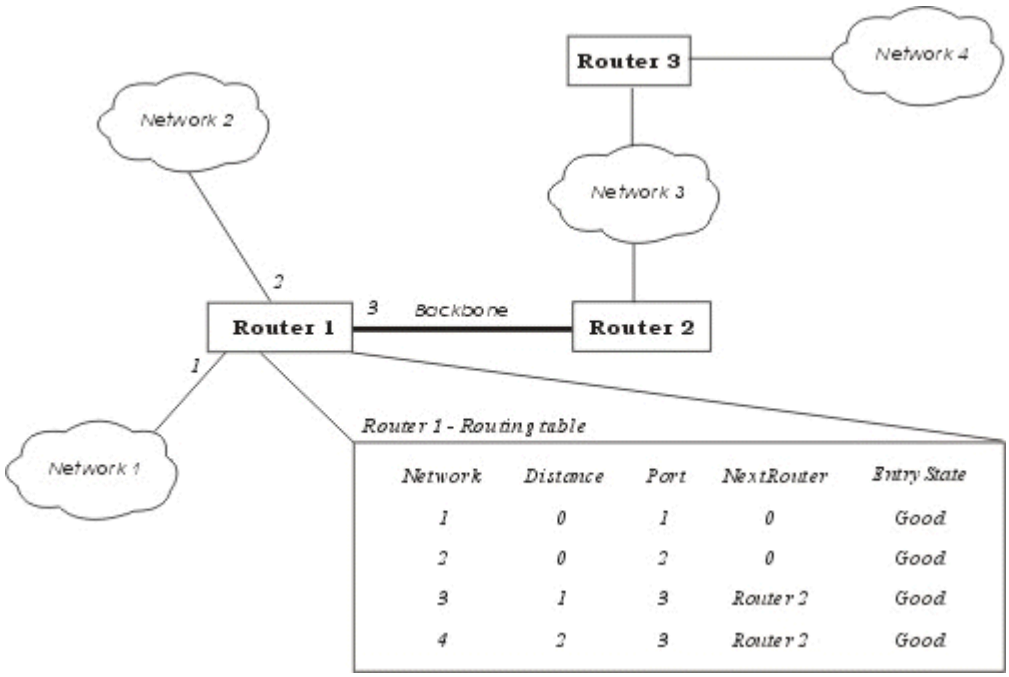
Các lý do sử dụng Router :

- Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin muốn đi qua Router cần phải gửi trực tiếp đến nó nên giảm được số lượng gói tin qua nó. Router thường được sử dụng trong khi nối các mạng thông qua các đường dây thuê bao đắt tiền do nó không truyền dư lên đường truyền.

- Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.

- Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.

- Trong một mạng phức hợp khi các gói tin luân chuyển các đường có thể gây nên tình trạng tắc nghẽn của mạng thì các Router có thể được cài đặt các phương thức nhằm tránh được tắc nghẽn.



Hình 3-4: Ví dụ về bảng chỉ đường (Routing table) của Router.

Các phương thức hoạt động của Router

- Đó là phương thức mà một Router có thể nối với các Router khác để qua đó chia sẻ thông tin về mạng hiện co. Các chương trình chạy trên Router luôn xây dựng bảng chỉ đường qua việc trao đổi các thông tin với các Router khác.

- Phương thức véc tơ khoảng cách : mỗi Router luôn luôn truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.

- Phương thức trạng thái tĩnh : Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng và chỉ khi đó các Router khác cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

Một số giao thức hoạt động chính của Router

- RIP (Routing Information Protocol) được phát triển bởi Xerox Network system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.

- NLSP (Netware Link Service Protocol) được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương thức véctơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng chỉ đường giảm đi..

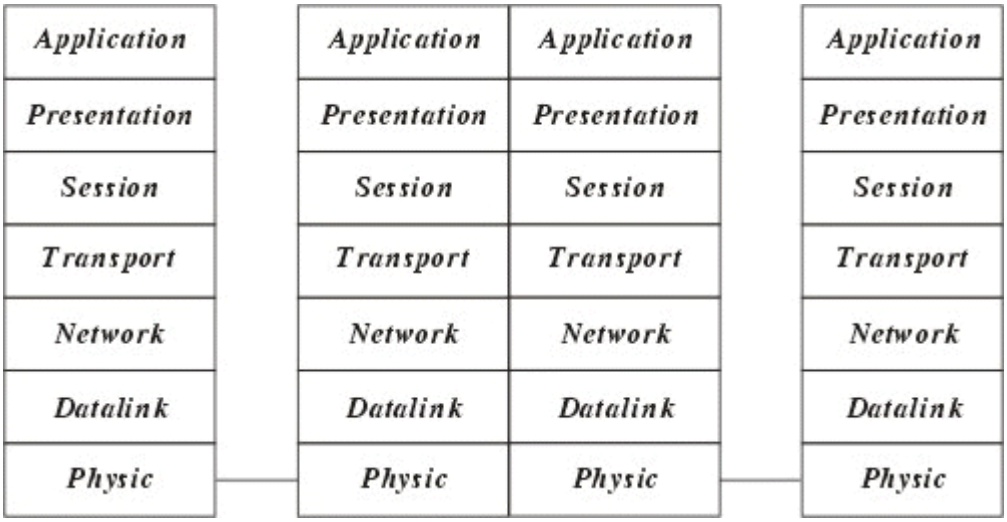
- OSPF (Open Shortest Path First) là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

- OSPF-IS (Open System Interconnection Intermediate System to Intermediate System) là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

3.5.4. Gateway (cổng nối)

Gateway dùng để kết nối các mạng không thuần nhất chẳng hạn như các mạng cục bộ và các mạng máy tính lớn (Mainframe), do các mạng hoàn toàn không thuần nhất nên việc chuyển đổi thực hiện trên cả 7 tầng của hệ thống mở OSI. Thường được sử dụng nối

các mạng LAN vào máy tính lớn. Gateway có các giao thức xác định trước thường là nhiều giao thức, một Gateway đa giao thức thường được chế tạo như các Card có chứa các bộ xử lý riêng và cài đặt trên các máy tính hoặc thiết bị chuyên biệt.



Hình 3-5: Hoạt động của Gateway trong mô hình OSI

Hoạt động của Gateway thông thường phức tạp hơn là Router nên thông suất của nó thường chậm hơn và thường không dùng nối mạng LAN -LAN.

3.5.5. Hub (Bộ tập trung)

Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng hình sao.

Người ta phân biệt các Hub thành 3 loại như sau sau:

- Hub bị động (Passive Hub): Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.

- Hub chủ động (Active Hub): Hub chủ động có các linh kiện điện tử có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Quá trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động.

- Hub thông minh (Intelligent Hub): cũng là Hub chủ động nhưng có thêm các chức năng mới so với loại trước, nó có thể có bộ vi xử lý của mình và bộ nhớ mà qua đó nó không chỉ cho phép điều khiển hoạt động thông qua các chương trình quản trị mạng mà nó có thể hoạt động như bộ tìm đường hay một cầu nối. Nó có thể cho phép tìm đường cho gói tin rất nhanh trên các cổng của nó, thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

3.5.6. Bộ chuyển mạch (switch)

Chức năng chính của switch là cùng một lúc duy trì nhiều cầu nối giữa các thiết bị mạng bằng cách dựa vào một loại đường truyền xương sống (backbone) nội tại tốc độ cao. Switch có nhiều cổng, mỗi cổng có thể hỗ trợ toàn bộ Ethernet LAN hoặc Token Ring.

Bộ chuyển mạch kết nối một số LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng.

Switch là thiết bị giống như bridge nhưng nhiều port hơn cho phép ghép nối nhiều đoạn mạng với nhau. Switch cũng dựa vào bảng địa chỉ MAC để quyết định gói tin nào đi ra port nào nhằm tránh tình trạng giảm băng thông khi số máy trạm trong mạng tăng lên. Switch cũng hoạt động tại lớp hai trong mô hình OSI. Việc xử lý gói tin dựa trên phần cứng (chip).

Khi một gói tin đi đến Switch (hoặc Bridge), Switch (hoặc Bridge) sẽ thực hiện như sau:

- Kiểm tra địa chỉ nguồn của gói tin đã có trong bảng MAC chưa, nếu chưa có thì nó sẽ thêm địa chỉ MAC này và port nguồn (nơi gói tin đi vào Switch (hoặc Bridge)) vào trong bảng MAC.

- Kiểm tra địa chỉ đích của gói tin đã có trong bảng MAC chưa:

+ Nếu chưa có thì nó sẽ gởi gói tin ra tất cả các port (ngoại trừ port gói tin đi vào).

+ Nếu địa chỉ đích đã có trong bảng MAC:

+ Nếu port đích trùng với port nguồn thì Switch (hoặc Bridge) sẽ loại bỏ gói tin.

+ Nếu port đích khác với port nguồn thì gói tin sẽ được gởi ra port đích tương ứng.

Chú ý:

- Địa chỉ nguồn và địa chỉ đích được nói ở trên đều là địa chỉ MAC.
- Port nguồn là Port mà gói tin đi vào.
- Port đích là Port mà gói tin đi ra.

❖ Tóm tắt Chương 3

Trong chương này, một số nội dung chính được giới thiệu:

- Môi trường truyền dẫn
- Các kỹ thuật bấm cáp mạng
- Các thiết bị liên kết mạng

❖ Câu hỏi:

- Trắc nghiệm:

Câu 1: Để kết nối hai HUB với nhau ta sử dụng kiểu bấm cáp

A. Thẳng (straight-through) **B.** Chéo (cross-over)

C. Console **D.** Tất cả đều đúng

Câu 2: Đâu là chuẩn T568A của dây cáp xoắn đôi

A. Trắng xanh lá-Xanh lá-Trắng cam-Cam-Trắng xanh dương- Xanh dương-Trắng nâu-Nâu

B.Trắng xanh lá-Xanh lá-Trắng cam-Xanh dương-Trắng xanh dương-Cam-Trắng nâu-Nâu

C. Trắng cam-Xanh lá-Trắng xanh lá-Xanh dương-Trắng xanh dương-Cam-Trắng nâu-Nâu

D. Trắng xanh lá-Cam-Trắng cam-Xanh dương-Trắng xanh dương- Xanh lá-Trắng nâu-Nâu

Câu 3: Cáp đồng trục được sử dụng với đầu nối là:

A. RJ11 **B.** BNC

C. RJ45 **D.** SC

Câu 4: Môi trường truyền tin thông thường trong mạng máy tính là?

A. Các loại cáp như: cáp xoắn đôi, cáp đồng trục, cáp quang

B. Sóng điện từ

C. Sóng hồng ngoại

D.Tất cả môi trường nêu trên

Câu 5: Kỹ thuật dùng để nối kết nhiều máy tính với nhau trong phạm vi một văn phòng gọi là

A.LAN **B.** MAN

C. WAN **D.** Internet

Câu 6: Để nối Router và máy tính ta phải bấm cáp kiểu nào?

A.Thẳng **B.** Chéo

C. Kiểu nào cũng được **D.** Tất cả đều sai

- Tự luận:

1. Trình bày các loại cáp truyền mạng
2. Trình bày kỹ thuật bấm dây cáp mạng thẳng
3. Trình bày kỹ thuật bấm dây cáp mạng chéo
4. Trình bày các thiết bị liên kết mạng
5. Phân biệt Hub và Switch

CHƯƠNG 4 – ĐỊA CHỈ IP

❖ GIỚI THIỆU CHƯƠNG 4

Chương 4 là phần lý thuyết và thực hành các kiến thức cơ bản về địa chỉ IP.

❖ MỤC TIÊU CHƯƠNG 3

Sau khi học xong phần này, người học có khả năng:

➢ ***Về kiến thức:***

- Trình bày được khái niệm, cấu trúc của địa chỉ IP.
- Hiểu đượccác bước thực hiện xem và cài đặt địa chỉ IP cho máy tính.

➢ ***Về kỹ năng:***

- Nhận biết được các lớp địa chỉ IP.
- Thực hiện được cácbước thực hiện xem và cài đặt địa chỉ IP cho máy tính.

➢ ***Về năng lực tự chủ và trách nhiệm:***

- Ý thức được tầm quan trọng và ý nghĩa thực tiễn của địa chỉ IP trong cài đặt hệ thống mạng máy tính.
- Tích cực, chủ động và hợp tác trong học tập. Thể hiện sự nhiệt tình, trách nhiệm, tác phong nhanh nhẹn trong công việc.

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP CHƯƠNG 4

- Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp); yêu cầu người học thực hiện trả lời câu hỏi và bài tập Chương 4 (cá nhân hoặc nhóm).
- Đối với người học: chủ động đọc trước giáo trình (Chương 4) trước buổi học; hoàn thành đầy đủ bài tập Chương 4 theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.

❖ ĐIỀU KIỆN THỰC HIỆN CHƯƠNG 4

➢ ***Phòng học chuyên môn hóa/nhà xưởng:***

- Phòng học lý thuyết, thực hành được trang bị hệ thống đèn đủ ánh sáng.
- Bàn ghế cho sinh viên.
- Bàn ghế giáo viên, bảng, phấn.

➢ ***Trang thiết bị máy móc:***

- Máy tính, máy chiếu

➢ ***Học liệu, dụng cụ, nguyên vật liệu:***

- Giáo án, bài giảng.
- Giáo trình nội bộ và các tài liệu giảng dạy khác hỗ trợ bài giảng

➢ ***Các điều kiện khác:*** Không có

❖ KIỂM TRA VÀ ĐÁNH GIÁ CHƯƠNG 4

- **Nội dung:**

- ✓ Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức
- ✓ Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.
- ✓ Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ Điểm kiểm tra thường xuyên: Không có

✓ Kiểm tra định kỳ: Không có

NỘI DUNG CHƯƠNG 4

4.1. Địa chỉ IP

4.1.1. Khái niệm

Địa chỉ IP (IP là viết tắt của từ tiếng Anh: Internet Protocol) là một địa chỉ đơn nhất mà những thiết bị điện tử hiện nay đang sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet.

Bất kỳ thiết bị mạng nào bao gồm bộ định tuyến, bộ chuyển mạch mạng, máy vi tính, máy chủ hạ tầng, máy in, máy fax qua Internet, và vài loại điện thoại tham gia vào mạng đều có địa chỉ riêng, và địa chỉ này là đơn nhất trong phạm vi của một mạng cụ thể. Vài địa chỉ IP có giá trị đơn nhất trong phạm vi Internet toàn cầu, trong khi một số khác chỉ cần phải đơn nhất trong phạm vi một công ty.

Địa chỉ IP do Tổ chức cấp phát số hiệu Internet (IANA) quản lý và tạo ra. IANA nói chung phân chia những "siêu khối" đến Cơ quan Internet khu vực, rồi từ đó lại phân chia thành những khối nhỏ hơn đến nhà cung cấp dịch vụ Internet và công ty.

4.1.2. Cấu trúc của các địa chỉ IP

Sơ đồ địa chỉ hóa để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP 32 bits (32 bit IP address). Mỗi giao diện trong 1 máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn với nhiều mạng do vậy có thể có nhiều địa chỉ IP). Địa chỉ IP gồm 2 phần: địa chỉ mạng (netid) và địa chỉ máy (hostid). Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu thị dưới dạng thập phân, bát phân, thập lục phân hay nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (dotted decimal notation) để tách các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.

Do tổ chức và độ lớn của các mạng con (subnet) của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp, ký hiệu là A, B, C, D và E. Trong lớp A, B, C chứa địa chỉ có thể gán được. Lớp D dành riêng cho lớp kỹ thuật multicasting. Lớp E được dành những ứng dụng trong tương lai.

Netid trong địa chỉ mạng dùng để nhận dạng từng mạng riêng biệt. Các mạng liên kết phải có địa chỉ mạng (netid) riêng cho mỗi mạng. Ở đây các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D và 11110 - lớp E).

Ở đây ta xét cấu trúc của các lớp địa chỉ có thể gán được là lớp A, lớp B, lớp C.

Mạng lớp A: địa chỉ mạng (netid) là 1 Byte và địa chỉ host (hostid) là 3 byte.

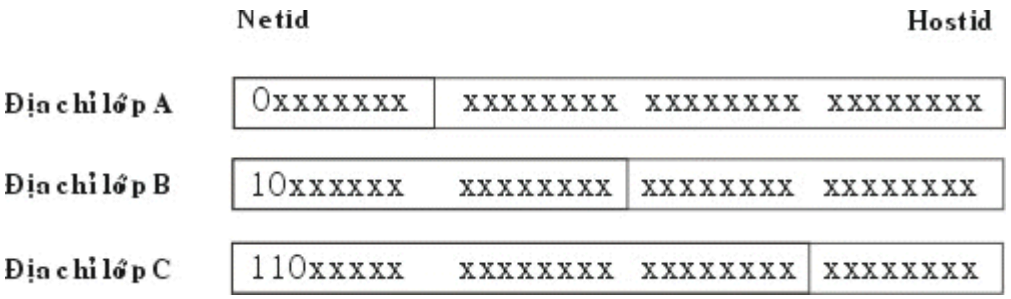
Mạng lớp B: địa chỉ mạng (netid) là 2 Byte và địa chỉ host (hostid) là 2 byte.

Mạng lớp C: địa chỉ mạng (netid) là 3 Byte và địa chỉ host (hostid) là 1 byte.

Lớp A cho phép định danh tới 126 mạng, với tối đa 16 triệu host trên mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn.

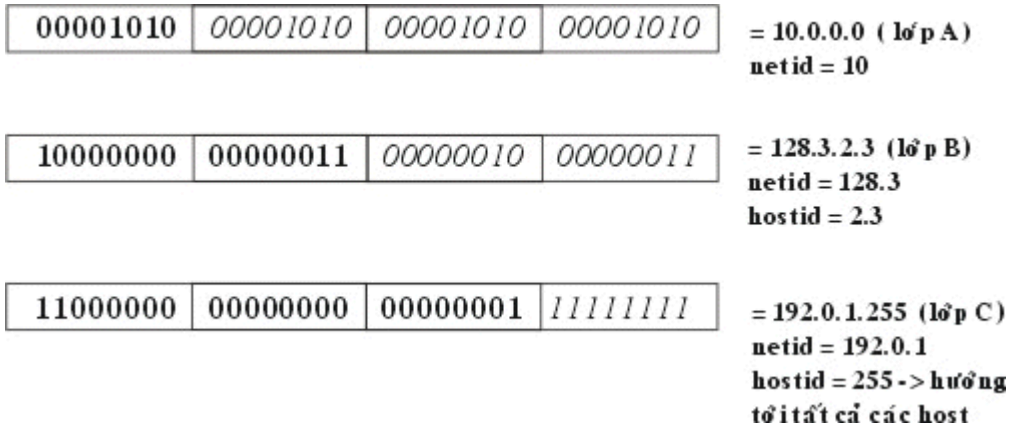
Lớp B cho phép định danh tới 16384 mạng, với tối đa 65534 host trên mỗi mạng.

Lớp C cho phép định danh tới 2 triệu mạng, với tối đa 254 host trên mỗi mạng. Lớp này được dùng cho các mạng có ít trạm.



Hình 4-1: Cấu trúc các lớp địa chỉ IP

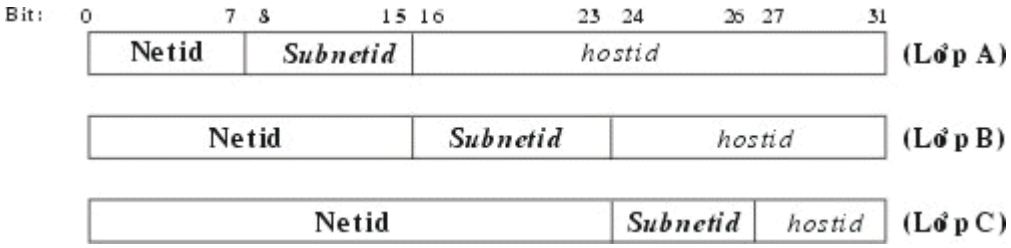
Một số địa chỉ có tính chất đặc biệt: Một địa chỉ có hostid = 0 được dùng để hướng tới mạng định danh bởi vùng netid. Ngược lại, một địa chỉ có vùng hostid gồm toàn số 1 được dùng để hướng tới tất cả các host nối vào mạng netid, và nếu vùng netid cũng gồm toàn số 1 thì nó hướng tới tất cả các host trong liên mạng



Hình 4-2: Ví dụ cấu trúc các lớp địa chỉ IP

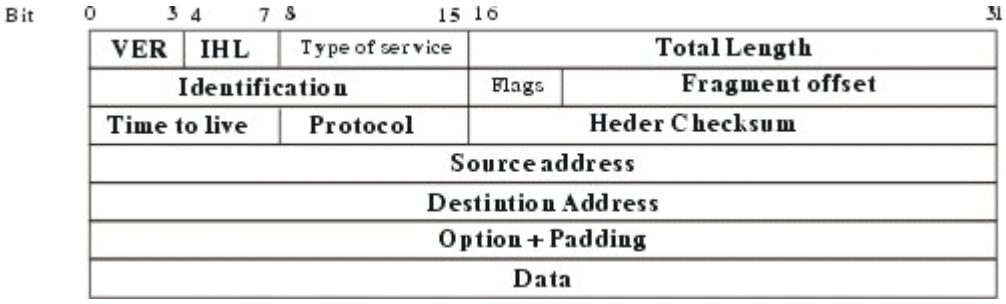
Cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.).

Trong nhiều trường hợp, một mạng có thể được chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnetid được lấy từ vùng hostid, cụ thể đối với lớp A, B, C như ví dụ sau:



Hình 4-3: Ví dụ địa chỉ khi bổ sung vùng subnetid

Đơn vị dữ liệu dùng trong IP được gọi là gói tin (datagram), có khuôn dạng



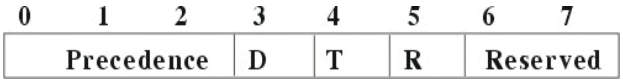
Hình 4-4: Dạng thức của gói tin IP

Ý nghĩa của thông số như sau:

- VER (4 bits): chỉ version hiện hành của giao thức IP hiện được cài đặt, Việc có chỉ số version cho phép có các trao đổi giữa các hệ thống sử dụng version cũ và hệ thống sử dụng version mới.

- IHL (4 bits): chỉ độ dài phần đầu (Internet header Length) của gói tin datagram, tính theo đơn vị từ (32 bits). Trường này bắt buột phải có vì phần đầu IP có thể có độ dài thay đổi tùy ý. Độ dài tối thiểu là 5 từ (20 bytes), độ dài tối đa là 15 từ hay là 60 bytes.

- Type of service (8 bits): đặc tả các tham số về dịch vụ nhằm thông báo cho mạng biết dịch vụ nào mà gói tin muốn được sử dụng, chẳng hạn ưu tiên, thời hạn chậm trễ, năng suất truyền và độ tin cậy. Hình sau cho biết ý nghĩ của trường 8 bits này.



- Precedence (3 bit): chỉ thị về quyền ưu tiên gửi datagram, nó có giá trị từ 0 (gói tin bình thường) đến 7 (gói tin kiểm soát mạng).

- D (Delay) (1 bit): chỉ độ trễ yêu cầu trong đó

+ D = 0 gói tin có độ trễ bình thường

+ D = 1 gói tin độ trễ thấp

- T (Throughput) (1 bit): chỉ độ thông lượng yêu cầu sử dụng để truyền gói tin với lựa chọn truyền trên đường thông suất thấp hay đường thông suất cao.

+ T = 0 thông lượng bình thường và

+ T = 1 thông lượng cao

- R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu

+ R = 0 độ tin cậy bình thường

+ R = 1 độ tin cậy cao

- Total Length (16 bits): chỉ độ dài toàn bộ gói tin, kể cả phần đầu tính theo đơn vị byte với chiều dài tối đa là 65535 bytes. Hiện nay giới hạn trên là rất lớn nhưng trong tương lai với những mạng Gigabit thì các gói tin có kích thước lớn là cần thiết.

- Identification (16 bits): cùng với các tham số khác (như Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng.

- Flags (3 bits): liên quan đến sự phân đoạn (fragment) các datagram, Các gói tin khi đi trên đường đi có thể bị phân thành nhiều gói tin nhỏ, trong trường hợp bị phân

đoạn thì trường Flags được dùng điều khiển phân đoạn và tái lắp ghép bó dữ liệu. Tùy theo giá trị của Flags sẽ có ý nghĩa là gói tin sẽ không phân đoạn, có thể phân đoạn hay là gói tin phân đoạn cuối cùng. Trường Fragment Offset cho biết vị trí dữ liệu thuộc phân đoạn tương ứng với đoạn bắt đầu của gói dữ liệu gốc. Ý nghĩa cụ thể của trường Flags là:

+ bit 0: reserved - chưa sử dụng, luôn lấy giá trị 0.

+ bit 1: (DF) = 0 (May Fragment) = 1 (Don't Fragment)

+ bit 2: (MF) = 0 (Last Fragment) = 1 (More Fragments)

- Fragment Offset (13 bits): chỉ vị trí của đoạn (fragment) ở trong datagram tính theo đơn vị 8 bytes, có nghĩa là phần dữ liệu mỗi gói tin (trừ gói tin cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội số của 8 bytes. Điều này có ý nghĩa là phải nhân giá trị của Fragment offset với 8 để tính ra độ lệch byte.

- Time to Live (8 bits): qui định thời gian tồn tại (tính bằng giây) của gói tin trong mạng để tránh tình trạng một gói tin bị quẩn trên mạng. Thời gian này được cho bởi trạm gửi và được giảm đi (thường qui ước là 1 đơn vị) khi datagram đi qua mỗi router của liên mạng. Thời lượng này giảm xuống tại mỗi router với mục đích giới hạn thời gian tồn tại của các gói tin và kết thúc những lần lặp lại vô hạn trên mạng. Sau đây là 1 số điều cần lưu ý về trường Time To Live:

+ Nút trung gian của mạng không được gởi 1 gói tin mà trường này có giá trị= 0.

+ Một giao thức có thể ấn định Time To Live để thực hiện cuộc ra tìm tài nguyên trên mạng trong phạm vi mở rộng.

+ Một giá trị cố định tối thiểu phải đủ lớn cho mạng hoạt động tốt.

- Protocol (8 bits): chỉ giao thức tầng trên kế tiếp sẽ nhận vùng dữ liệu ở trạm đích (hiện tại thường là TCP hoặc UDP được cài đặt trên IP). Ví dụ: TCP có giá trị trường Protocol là 6, UDP có giá trị trường Protocol là 17

- Header Checksum (16 bits): Mã kiểm soát lỗi của header gói tin IP.

- Source Address (32 bits): Địa chỉ của máy nguồn.

- Destination Address (32 bits): địa chỉ của máy đích

- Options (độ dài thay đổi): khai báo các lựa chọn do người gửi yêu cầu (tuỳ theo từng chương trình).

- Padding (độ dài thay đổi): Vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits.

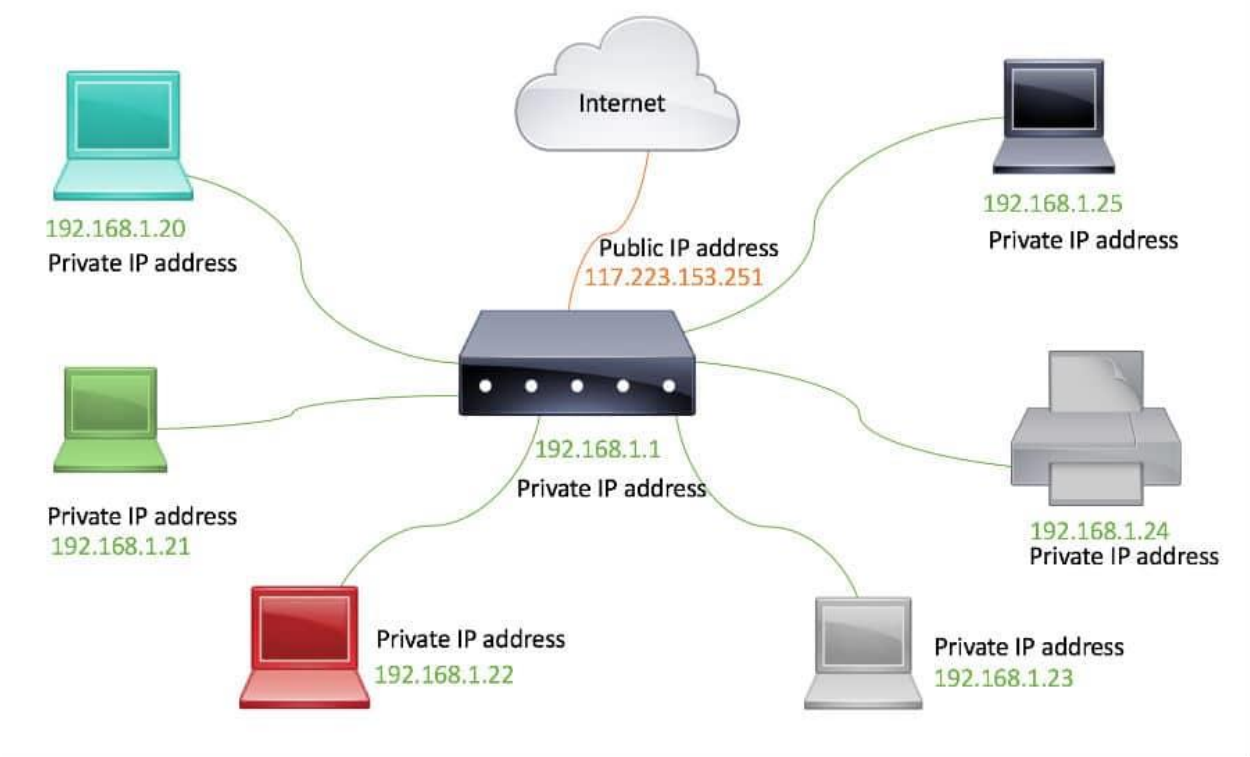
- Data (độ dài thay đổi): Trên một mạng cục bộ như vậy, hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm.

4.1.3. Phân loại IP

Tính đến nay có 4 loại hình IP thông dụng nhất là IP Private, IP Public, IP tĩnh và IP động. Mỗi loại IP có thể là địa chỉ IPv4 hoặc địa chỉ IPv6.

IP Private

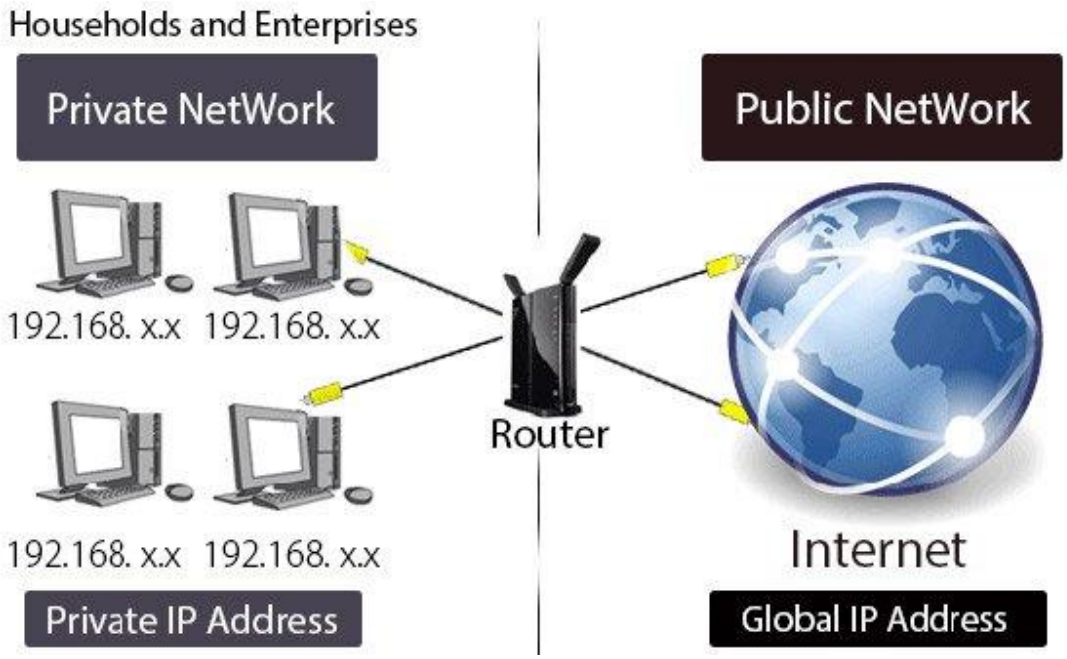
IP private còn được gọi là IP nội bộ. Đây là dãy các IP chỉ được sử dụng cho những máy tính thuộc một mạng nội bộ như mạng nhà trường, công ty, tổ chức… IP Private hỗ trợ các máy tính trong hệ thống kết nối với nhau. Chúng sẽ không kết nối trực tiếp với các máy tính bên ngoài hệ thống. IP Private được thiết lập thủ công hoặc do router thiết lập tự động.



Hình 4-5: IP Private là địa chỉ sử dụng cho mạng lưới máy tính nội bộ

IP Public

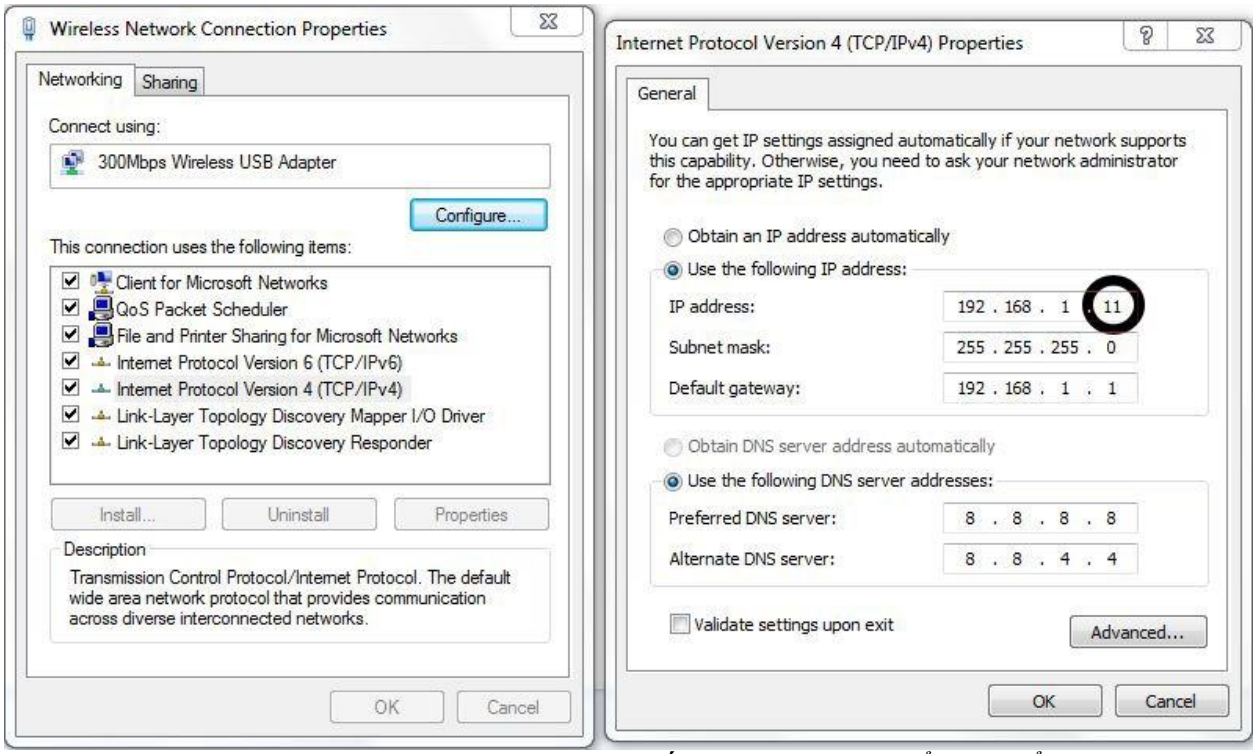
IP Public là địa chỉ IP cộng đồng. Đây là IP sử dụng trong mạng gia đình hoặc doanh nghiệp để kết nối Internet. Địa chỉ IP Public là yếu tố thiết yếu với bất kỳ phần cứng mạng có thể truy cập công khai nào. Ví dụ như router gia đình hoặc các server. Các thông số của IP Public cần được ghi nhớ chính xác. Đặc biệt khi thuê máy chủ để thiết lập kết nối chính xác cho website của mình.



Hình 4-6: IP Public thường được sử dụng trong mạng lưới gia đình hoặc doanh nghiệp

IP tĩnh (Static IP)

IP tĩnh là địa chỉ được định cấu hình thủ công cho thiết bị. IP này được gọi "tĩnh" do nó không hề thay đổi khác với DHCP thay đổi mỗi khi mất và kết nối lại.



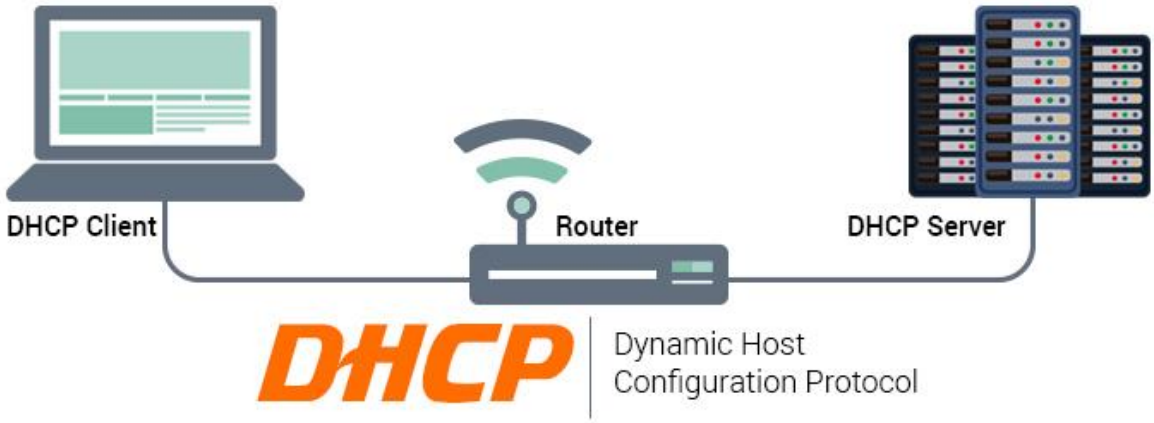
Hình 4-3: Địa chỉ IP tĩnh được cố định và không thể thay đổi

Địa chỉ IP tĩnh giúp kết nối Internet nhanh chóng không cần đợi cấp phát IP. IP tĩnh còn giúp tăng tốc độ tải website, download file torrent. IP tĩnh giữ đường truyền ổn định với máy tính nằm trong hệ thống mạng nội bộ.

Bất lợi lớn của IP tĩnh chính là cấu hình thủ công. Mọi thiết bị đều yêu cầu thiết lập địa chỉ IP tĩnh và cấu hình đúng router để giao tiếp với thiết bị đó. Điều này gây mất rất nhiều thời gian khi thiết lập.

IP động (Dynamic IP)

IP động là IP được gán tự động cho từng kết nối hoặc node của mạng. Ví dụ như điện thoại thông minh, máy tính,…… IP động hoạt động ngược lại so với IP tĩnh bằng cách sử dụng phương thức DHCP. Việc gán địa chỉ IP tự động này được thực hiện bằng giao thức DHCP và luôn được thay đổi mỗi khi ngắt và kết nối lại.



Hình 4-7: IP động có thể được tùy chỉnh bởi máy chủ DHCP

IP động mang nhiều ưu điểm như: tính linh hoạt, dễ cài đặt và dễ quản lý. Số lượng thiết bị kết nối sẽ ít bị giới hạn với IP động. Những thiết bị không cần thiết sẽ ngắt kết nối và giải phóng IP cho các thiết bị mới sử dụng.

IP động được ứng dụng rộng rãi nhất. Nó tồn tại khi các hộ gia đình sử dụng IP được gán tự động từ router. Tuy nhiên, mọi thiết bị sẽ yêu cầu IP của router để máy tính truy cập vào mạng. Địa chỉ IP động của router sẽ luôn thay đổi theo định kỳ. Điều này dẫn đến việc xung đột IP khi các máy mới vào sử dụng IP của máy đang dùng trong hệ thống mạng.

4.1.4. Cách tìm địa chỉ IP

Tìm địa chỉ IP nội bộ

Bước 1: Mở Start Menu. Vào Control panel.

Bước 2: Truy cập View network status and tasks.

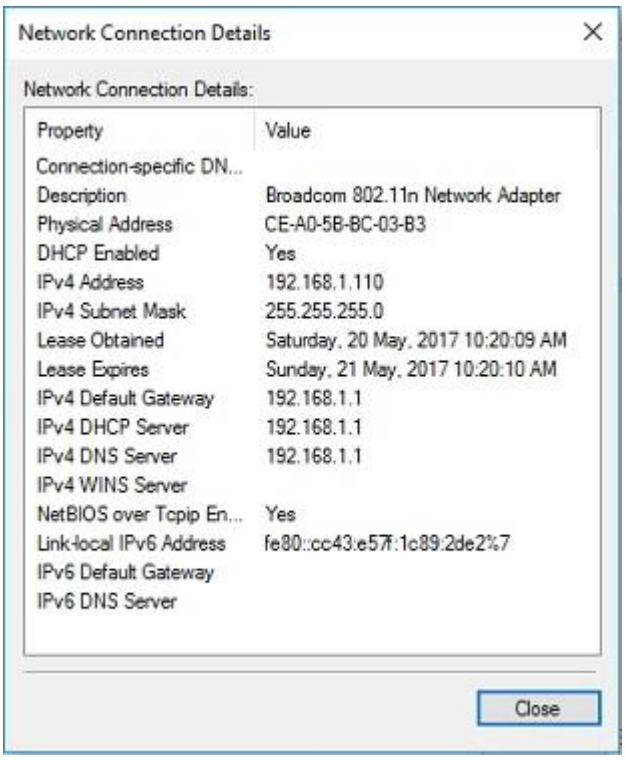
Bước 3: Nhấn vào phần mạng đang truy cập. Chọn Details.

Bước 4: Chú ý dòng IPv4 Address: đây là địa chỉ IP nội bộ trong hệ thống.

Có một cách khác giúp xác định địa chỉ IP trên máy tính nhanh hơn. Hãy sử dụng Command Prompt.

Bước 1: Nhấn Windows + R để mở Run. Nhập CMD

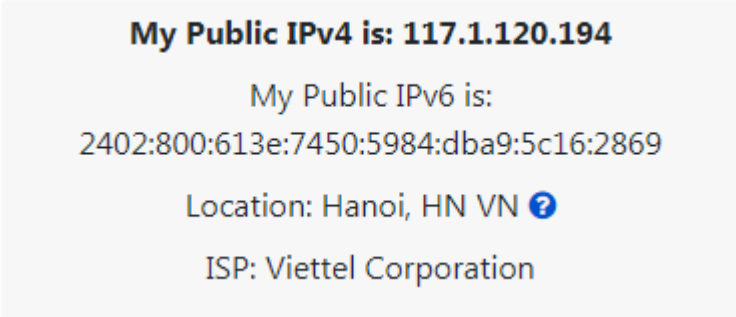
Bước 2: Gõ lệnh “ipconfig” để tìm IP. Chú ý theo dõi dòng IPv4 Address. Dòng đó chính là địa chỉ IP của máy tính đang sử dụng.



Hình 4-8: Địa chỉ IP nội bộ của máy vi tính

Tìm IP Public

Ngày nay, có rất nhiều công cụ để xác định địa chỉ IP Public. Trong đó, cách đơn giản nhất chính là truy cập vào địa chỉ **whatismyip.com**. Hệ thống của website sẽ cho biết địa chỉ IP Public đang sử dụng. Ngoài ra nó còn cho thấy địa chỉ đang ở đâu trên bản đồ, nhà cung cấp là ai?



Hình 4-9: Địa chỉ IP Public

4.1.5. Ưu và nhược điểm của địa chỉ IP

Ưu điểm

Là một giao thức kết nối giúp bạn có thể truy cập được internet cũng như trò chuyện thông qua các địa chỉ IP.

Giúp việc truy cập internet dễ dàng hơn cũng như quản lý hệ thống mạng của người dùng đơn giản hơn khi mà mỗi máy tính, thiết bị đề có một địa chỉ IP riêng biệt.

Là một sự phát triển vượt bậc của ngành công nghệ mạng.

Nhược điểm

Dễ dàng bị khai thác các thông tin các nhân thông qua địa chỉ IP nếu bị hacker xâm nhập, phá. hoại

Bất cứ một hoạt động truy cập nào cũng sẽ bị lưu lại địa chỉ IP.

4.2. Một số khái niệm và thuật ngữ liên quan

Địa chỉ mạng (Network Address): là địa chỉ IP mà giá trị của tất cả các bits ở phần nhận dạng máy tính đều là 0, được sử dụng để xác định một mạng.

Ví dụ : 10.0.0.0; 172.18.0.0 ; 192.1.1.0

Địa chỉ quảng bá (Broadcast Address) : Là địa chỉ IP mà giá trị của tất cả các bits ở phần nhận dạng máy tính đều là 1, được sử dụng để chỉ tất cả các máy tính trong mạng.

Ví dụ : 10.255.255.255, 172.18.255.255, 192.1.1.255

Mặt nạ mạng chuẩn (Netmask) : Là địa chỉ IP mà giá trị của các bits ở phần nhận dạng mạng đều là 1, các bits ở phần nhận dạng máy tính đều là 0. Như vậy ta có 3 mặt nạ mạng tương ứng cho 3 lớp mạng A, B và C là :

+ Mặt nạ mạng lớp A : 255.0.0.0

+ Mặt nạ mạng lớp B : 255.255.0.0

+ Mặt nạ mạng lớp C : 255.255.255.0

Ta gọi chúng là các mặt nạ mạng mặc định (Default Netmask)

Lưu ý : Địa chỉ mạng, địa chỉ quảng bá, mặt nạ mạng không được dùng để đặt địa chỉ cho các máy tính

Địa chỉ mạng 127.0.0.0 là địa chỉ được dành riêng để đặt trong phạm vi một máy tính. Nó chỉ có giá trị cục bộ (trong phạm vi một máy tính). Thông thường khi cài đặt giao thức IP thì máy tính sẽ được gián địa chỉ 127.0.0.1. Địa chỉ này thông thường để kiểm tra xem giao thức IP trên máy hiện tại có hoạt động không.

Địa chỉ dành riêng cho mạng cục bộ không nối kết trực tiếp Internet: Các mạng cục bộ không nối kết trực tiếp vào mạng Internet có thể sử dụng các địa chỉ mạng sau để đánh địa chỉ cho các máy tính trong mạng của mình :

- Lớp A : 10.0.0.0

- Lớp B : 172.16.0.0 đến 172.32.0.0

- Lớp C : 192.168.0.0

Ý nghĩa của Netmask

Với một địa chỉ IP và một Netmask cho trước, ta có thể dùng phép toán AND BIT để tính ra được địa chỉ mạng mà địa chỉ IP này thuộc về. Công thức như sau :

Network Address = IP Address & Netmask

Ví dụ : Cho địa chỉ IP = 198.53.147.45 và Netmask = 255.255.255.0. Ta thực hiện phép toán AND BIT (&) hai địa chỉ trên:

	Biểu diễn thập phân	Biểu diễn nhị phân

IP Address	198.53.147.45	11000110 00101101	00110101	10010011
Netmask	255.255.255.0	11111111 00000000	11111111	11111111
Network Address	198.53.147.0	11000110 00000000	00110101	10010011

4.3. Địa chỉ IPv4

4.3.1. Thành phần và hình dạng của địa chỉ Ipv4

Địa chỉ IP đang được sử dụng hiện tại (IPv4) có 32 bit chia thành 4 Octet (mỗi Octet có 8 bit, tương đương 1 byte) cách đếm đều từ trái qua phải bit 1 cho đến bit 32, các Octet tách biệt nhau bằng dấu chấm (.), bao gồm có 3 thành phần chính.

Bit 1.....Bit 32

+ Bit nhận dạng lớp (Class bit)

+ Địa chỉ của đường mạng (Net ID)

+ Địa chỉ của máy tính (Host ID).

Bit nhận dạng lớp (Class bit) để phân biệt địa chỉ ở lớp nào.

- Địa chỉ Internet biểu hiện ở dạng bit nhị phân:

x y x y x y x y. x y x y x y x y. x y x y x y x y. x y x y x y x y

x, y = 0 hoặc 1.

Ví dụ:

0	0 1 0 1 10.	0 1 1 1 1 0 1 1.	0 1 1 0 1 1 1 0.	1 1 1 0 0 0 0 0
Bit nhận dạng	Octet 1	Octet 2	Octet 3	Octet 4

- Địa chỉ Internet biểu hiện ở dạng thập phân:

xxx.xxx.xxx.xxx

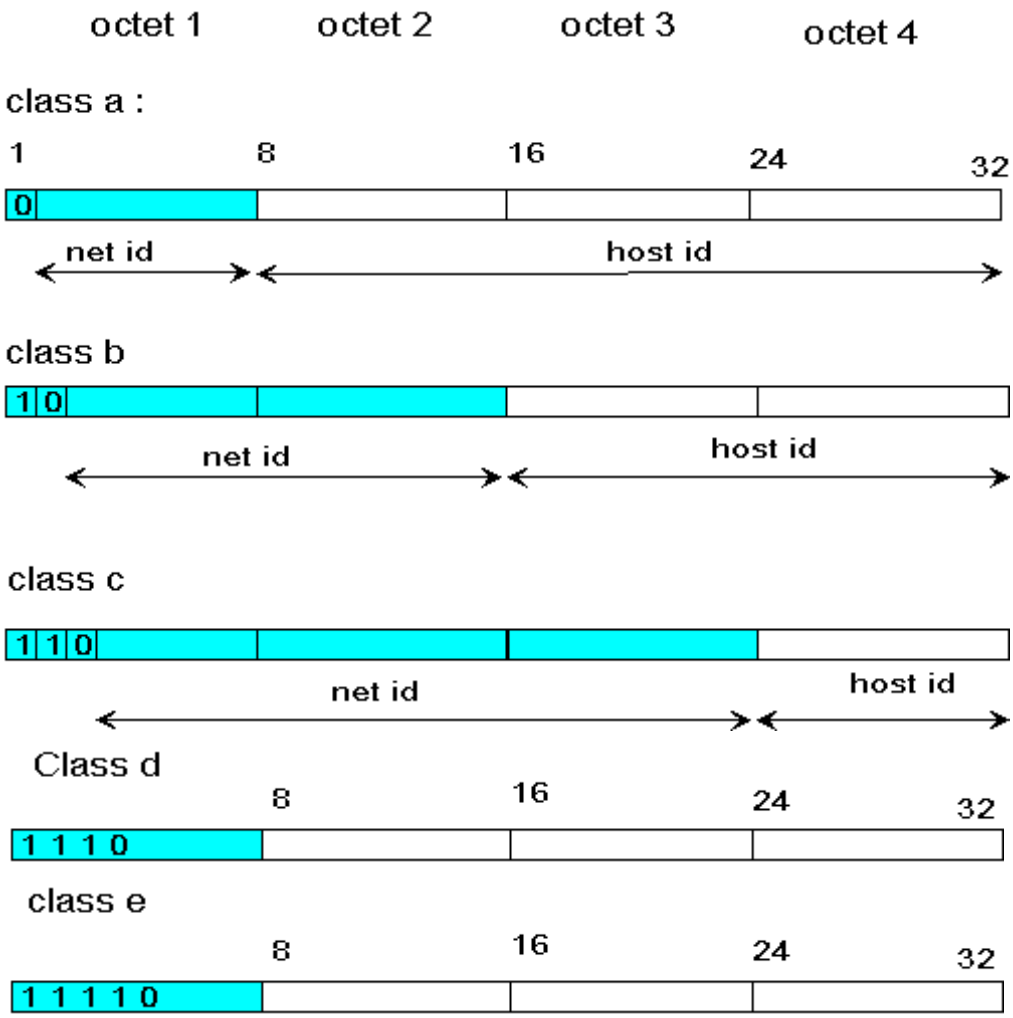
x là số thập phân từ 0 đến 9

Ví dụ: 146. 123. 110. 224

Dạng viết đầy đủ của địa chỉ IP là 3 con số trong từng Octet. Ví dụ: địa chỉ IP thường thấy trên thực tế có thể là 53.143.10.2 nhưng dạng đầy đủ là 053.143.010.002.

4.3.2. Các lớp địa chỉ IPv4

Địa chỉ IPv4 chia ra 5 lớp A,B,C, D, E. Hiện tại đã dùng hết lớp A,B và gần hết lớp C, còn lớp D và E Tổ chức internet đang để dành cho mục đích khác không phân, nên chúng ta chỉ nghiên cứu 3 lớp đầu.



Qua cấu trúc các lớp địa chỉ IP chúng ta có nhận xét sau:

+ Bit nhận dạng là những bit đầu tiên - của lớp A là 0, của lớp B là 10, của lớp C là 110.

+ Lớp D có 4 bit đầu tiên để nhận dạng là 1110, còn lớp E có 5 bít đầu tiên để nhận dạng là 11110.

+ Địa chỉ lớp A: Địa chỉ mạng ít và địa chỉ máy chủ trên từng mạng nhiều.

+ Địa chỉ lớp B: Địa chỉ mạng vừa phải và địa chỉ máy chủ trên từng mạng vừa phải.

+ Địa chỉ lớp C: Địa chỉ mạng nhiều, địa chỉ máy chủ trên từng mạng ít.

Địa chỉ lớp	Vùng địa chỉ lý thuyết	Số mạng tối đa sử dụng	Số máy chủ tối đa trên từng mạng
A	Từ 0.0.0.0 đến 127.0.0.0	126	16777214
B	Từ 128.0.0.0 đến 191.255.0.0	16382	65534
C	Từ 192.0.0.0 đến 223.255.255.0	2097150	254
D	Từ 224.0.0.0 đến 240.0.0.0	Không phân	
E	Từ 241.0.0.0 đến 255.0.0.0	Không phân	

Bảng 4-1 Các lớp địa chỉ IP

Địa chỉ lớp	Vùng địa chỉ sử dụng	Bit nhận dạng	Số bit dùng để phân cho mạng
A	Từ 1 đến 127	0	7
B	Từ 128.1 đến 191.254	10	14
C	Từ 192.0.1 đến 223.255.254	110	21
D		1110	---
E		11110	---

Bảng 4-2 Bit nhận dạng các lớp

Như vậy nếu chúng ta thấy 1 địa chỉ IP có 4 nhóm số cách nhau bằng dấu chấm, nếu thấy nhóm số thứ nhất nhỏ hơn 126 biết địa chỉ này ở lớp A, nằm trong khoảng 128 đến 191 biết địa chỉ này ở lớp B và từ 192 đến 223 biết địa chỉ này ở lớp C.

4.4. Địa chỉ IPv6

4.4.1. Giao thức liên mạng thế hệ mới (IPv6)

Giao thức IPv4 đã được coi là nền tảng cho mạng Internet với những tính chất ưu việt của nó, tuy nhiên với sự bùng nổ về Internet giao thức IPv4 đã bộc lộ một số yếu điểm về tính năng, trong đó nổi bật là:

- Thiếu hụt về tính năng xác thực, an ninh của gói tin trên mạng. Khả năng mở rộng hạn chế.

- Thiếu hụt không gian địa chỉ. Với sự phát triển của mạng Internet, không gian địa chỉ IP có thể sử dụng thực sự là rất nhỏ do các địa chỉ lớp A được dành chủ yếu cho các công ty cung cấp dịch vụ lớn tại Mỹ và rất hạn chế trong việc cấp phát. Các địa chỉ lớp B nhanh chóng bị sử dụng hết do nó cung cấp số địa chỉ vừa phải. Hiện nay nhiều yêu cầu chỉ được đáp ứng bằng các địa chỉ lớp C với số địa chỉ rất hạn chế.

- Sự gia tăng số lượng các chỉ mục trong bảng định tuyến do cơ chế định tuyến không phân cấp dẫn đến yêu cầu nâng cấp các router và và định tuyến không hiệu quả.

- Ngày nay, với các nhu cầu kết nối vào mạng Internet của các dịch vụ khác như điện thoại di động, truyền hình số,… đòi hỏi giao thức IPv4 cần có các sửa đổi để đáp ứng các nhu cầu mới.

Trước những nhu cầu này, giao thức liên mạng thế hệ mới IPv6 đã ra đời nhằm thay thế cho IPv4, nhưng cho đến nay IPv6 vẫn chỉ mới chủ yếu là đang trong quá trình thử nghiệm và hoàn thiện. Trong khuôn khổ giáo trình cũng đề cập một cách tổng quát về giao thức liên mạng thế hệ mới IPv6.

4.4.2. Một số đặc điểm mới của IPv6:

- Khuôn dạng header mới: Header của IPv6 được thiết kế để giảm chi phí đến mức tối thiểu. Điều này đạt được bằng cách chuyển các trường lựa chọn sang các header mở rộng được đặt phía sau của IPv6 header. Khuôn dạng mới của IPv6 tạo ra sự xử lý hiệu quả hơn tại các router.

- Header của IPv4 và IPv6 không thể xử lý chung. Một trạm hay một router phải cài đặt cả IPv4 và IPv6 để có thể xử lý được cả hai khuôn dạng header này. Header của IPv6 chỉ có kích thước gấp 2 lần header của IPv4 mặc dù không gian địa chỉ của IPv6 lớn gấp 4 lần không gian địa chỉ IPv4.

- Không gian địa chỉ lớn: IPv6 có địa chỉ nguồn và đích dài 128 bit. Mặc dù 128 bit có thể tạo ra hơn 3.4x1038 tổ hợp, không gian địa chỉ của IPv6 được thiết kế cho phép phân bổ địa chỉ và mạng con từ trục xương sống Internet đến từng mạng con trong một tổ chức.

- Hiện tại chỉ một lượng nhỏ các địa chỉ hiện đang được phân bổ để sử dụng bởi các trạm, vẫn còn dư thừa rất nhiều địa chỉ sẵn sàng cho việc sử dụng trong tương lai.

- Hiệu quả, phân cấp địa chỉ hóa và hạ tầng định tuyến: Các địa chỉ toàn cục của IPv6 được thiết kế để tạo ra mọt hạ tầng định tuyến hiệu quả, phân cấp và có thể tổng quát hóa dựa trên sự phân cấp thường thấy của các nhà cung cấp dịch vụ (ISP) trên thực tế.

- Hỗ trợ chất lượng dịch vụ (QoS) tốt hơn: Các trường mới trong header của IPv6 định ra cách thức xử lý và định danh trên mạng. Giao thông trên mạng được định danh nhờ trường gán nhãn luồng (Flow Label) cho phép router có thể nhận ra và cung cấp các xử lý đặc biệt đối với các gói tin thuộc về một luồng nhất định, một chuẩn các gói tin giữa nguồn và đích.

Do giao thông mạng được xác định trong header, các dịch vụ QoS có thể được thực hiện ngay cả khi phần dữ liệu được mã hóa theo IPSec.

- Khả năng mở rộng: IPv6 có thể dễ dàng mở rộng thêm các tính năng mới bằng việc thêm các header mới sau header IPv6.

4.4.3. Kiến trúc địa chỉ trong IPv6:

Không gian địa chỉ:

- IPv6 sử dụng địa chỉ có độ dài lớn hơn IPv4 (128 bit so với 32 bit) do đó cung cấp không gian địa chỉ lớn hơn rất nhiều. Trong khi không gian địa chỉ 32 bit của IPv4 cho phép khoảng 4 tỷ địa chỉ, không gian địa chỉ của IPv6 có thể có khoảng 3.4x1038 địa chỉ. Số lượng địa chỉ này rất lớn, hỗ trợ khoảng 6.5x1023 địa chỉ trên mỗi mét vuông bề mặt trái đất. Địa chỉ IPv6 128 bit được chia thành các miền phân cấp theo trật tự trên Internet.

Nó tạo ra nhiều mức phân cấp và linh hoạt trong địa chỉ hóa và định tuyến còn đang thiếu trong IPv4.

- Không gian địa chỉ IPv6 được chia trên cơ sở các bit đầu trong địa chỉ. Trường có độ dài thay đổi bao gồm các bit đầu tiên trong địa chỉ gọi là tiền tố định dạng (Format Prefix) FP.

- Ban đầu chỉ mới có 15% lượng địa chỉ được sử dụng, 85% còn lại để dùng trong tương lai.

- Các tiền tố định dạng từ 001 đến 111, ngoại trừ kiểu địa chỉ multicast (1111 1111) đều bắt buộc có định danh giao diện theo khuôn dạng EUI-64.

- Các địa chỉ dự trữ không lẫn với các địa chỉ chưa cấp phát. Chúng chiếm 1/256 không gian địa chỉ (FP = 0000 0000) và dùng cho các địa chỉ chưa chỉ định, địa chỉ quay vòng và các địa chỉ IPv6 có nhúng IPv4

Cú pháp địa chỉ:

Các địa chỉ IPv6 dài 128 bit, khi viết mỗi nhóm 16 bit được biểu diễn thành một số nguyên không dấu dưới dạng hệ 16 và được phân tách bởi dấu hai chấm (:),

Ví dụ: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Trên thực tế địa chỉ IPv6 thường có nhiều số 0, ví dụ địa chỉ:

1080:0000:0000:0000:0008:0800:200C:417A. Do đó cơ chế nén địa chỉ được dùng để biểu diễn dễ dàng hơn các loại địa chỉ dạng này. Ta không cần viết các số 0 ở đầu mỗi nhóm, ví dụ 0 thay cho 0000, 20 thay cho 0020.

Địa chỉ trong ví dụ trên sẽ trở thành 1080:0:0:0:8:800:200C:417A.

Hơn nữa ta có thể sử dụng ký hiệu :: để chỉ một chuỗi số 0. Địa chỉ trong ví dụ trên sẽ trở thành: 1080::8:800:200C:417A. Do địa chỉ IPv6 có độ dài cố định, ta có thể tính được số các bit 0 mà ký hiệu đó biểu diễn.

Tiền tố địa chỉ IPv6 được biểu diễn theo ký pháp CIDR như IPv4 như sau:

IPv6-address/prefix length trong đó IPv6-address là bất kỳ kiểu biểu diễn nào, còn prefix length là độ dài tiền tố theo bit.

Ví dụ: biểu diễn mạng con có tiền tố 80 bit: 1080:0:0:0:8::/80.

Với node address: 12AB:0:0:CD30:123:4567:89AB:CDEF,

prefix: 12AB:0:0:CD30::/60 có thể viết tắt thành

12AB:0:0:CD30:123:4567:89AB:CDEF/60

❖ Tóm tắt Chương 4

Trong chương này, một số nội dung chính được giới thiệu:

- Khái niệm địa chỉ IP

- Cấu trúc, Phân loại địa chỉ IP

- Địa chỉ IPv4 và IPv6

❖ Câu hỏi:

- Trắc nghiệm:

Câu 1: Đâu là địa chỉ IP lớp C?

A. 10.1.1.10 **B.** 224.1.1.10

C. 128.1.1.10 **D.** 192.1.1.10

Câu 2: Đâu là địa chỉ IP lớp B?

A. 10.1.1.10 **B.** 224.1.1.10

C. 128.1.1.10 **D.** 192.1.1.10

Câu 3: Đâu là địa chỉ IP lớp A?

A. 10.1.1.10 **B.** 224.1.1.10

C. 128.1.1.10 **D.** 192.1.1.10

Câu 4: Địa chỉ IP nào sau đây đặt được cho máy tính?

A. 192.168.0.0 **B.** 192.168.1.255

C. 192.168.0.255 **D.** 192.168.1.2

Câu 5: Đâu là địa chỉ mặt nạ mạng (Subnet Mask) của IP lớp B?

A. 255.255.0.0 **B.** 255.255.255.0

C. 255.0.0.0 **D.** 255.255.255.255

- Tự luận:

1. Trình bày cấu trúc của các địa chỉ IP
2. Phân loại các loại hình IP
3. Trình bày thành phần và hình dạng của địa chỉ IPv4
4. Trình bày các lớp địa chỉ IPv4
5. So sánh IPv4 header và IPv6 header
6. Lớp địa chỉ IPv6, biểu diễn, các loại địa chỉ IPv6
7. So sánh địa chỉ IPv4 và địa chỉ IPv6

CHƯƠNG 5: AN TOÀN MẠNG

❖ GIỚI THIỆU CHƯƠNG 5

Chương 5 là phần lý thuyết các kiến thức tổng quan về an ninh mạng.

❖ MỤC TIÊU CHƯƠNG 5

Sau khi học xong phần này, người học có khả năng:

➢ ***Về kiến thức:***

- Trình bày được các kiến thức tổng quan về an toàn mạng.
- Hiểu đượcmột số phương thức tấn công và các biện pháp bảo vệ an toàn mạng.

➢ ***Về kỹ năng:***

- Nhận biết được một sốphương thức tấn công và các biện pháp bảo vệ an toàn mạng.
- Thực hiện được các cài đặt cơ bản bảo đảm an toàn hệ thống mạng nội bộ.

➢ ***Về năng lực tự chủ và trách nhiệm:***

- Ý thức được tầm quan trọng và ý nghĩa thực tiễn của an toàn mạng trong hệ thống mạng máy tính.
- Tích cực, chủ động và hợp tác trong học tập. Thể hiện sự nhiệt tình, trách nhiệm, tác phong nhanh nhẹn trong công việc.

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP CHƯƠNG 5

- Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp); yêu cầu người học thực hiện trả lời câu hỏi và bài tập Chương 5 (cá nhân hoặc nhóm).
- Đối với người học: chủ động đọc trước giáo trình (Chương 5) trước buổi học; hoàn thành đầy đủ bài tập Chương 5 theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.

❖ ĐIỀU KIỆN THỰC HIỆN CHƯƠNG 3

➢ ***Phòng học chuyên môn hóa/nhà xưởng:***

- Phòng học lý thuyết, thực hành được trang bị hệ thống đèn đủ ánh sáng.
- Bàn ghế cho sinh viên.
- Bàn ghế giáo viên, bảng, phấn.

➢ ***Trang thiết bị máy móc:***

- Máy tính, máy chiếu

➢ ***Học liệu, dụng cụ, nguyên vật liệu:***

- Giáo án, bài giảng.
- Giáo trình nội bộ và các tài liệu giảng dạy khác hỗ trợ bài giảng

➢ ***Các điều kiện khác:*** Không có

❖ KIỂM TRA VÀ ĐÁNH GIÁ CHƯƠNG 5

- **Nội dung:**

✓ Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức

✓ Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.

✓ Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ Điểm kiểm tra thường xuyên: Không có

✓ Kiểm tra định kỳ: 01 bài kiểm tra (hình thức: trắc nghiệm + tự luận)

NỘI DUNG CHƯƠNG 5

5.1. Tổng quan về an toàn mạng

5.1.1. An toàn mạng là gì?

Mục tiêu của việc kết nối mạng là để nhiều người sử dụng, từ những vị trí địa lý khác nhau có thể sử dụng chung tài nguyên, trao đổi thông tin với nhau. Do đặc điểm nhiều người sử dụng lại phân tán về mặt vật lý nên việc bảo vệ các tài nguyên thông tin trên mạng, tránh sự mất mát, xâm phạm là cần thiết và cấp bách. An toàn mạng có thể hiểu là cách bảo vệ, đảm bảo an toàn cho tất cả các thành phần mạng bao gồm dữ liệu, thiết bị, cơ sở hạ tầng mạng và đảm bảo mọi tài nguyên mạng được sử dụng tương ứng với một chính sách hoạt động được ấn định và với chỉ những người có thẩm quyền tương ứng.

An toàn mạng bao gồm:

Xác định chính xác các khả năng, nguy cơ xâm phạm mạng, các sự cố rủi ro đối với thiết bị, dữ liệu trên mạng để có các giải pháp phù hợp đảm bảo an toàn mạng.

Đánh giá nguy cơ tấn công của Hacker đến mạng, sự phát tán virus... Phải nhận thấy an toàn mạng là một trong những vấn đề cực kỳ quan trọng trong các hoạt động, giao dịch điện tử và trong việc khai thác sử dụng các tài nguyên mạng.

Một thách thức đối với an toàn mạng là xác định chính xác cấp độ an toàn cần thiết cho việc điều khiển hệ thống và các thành phần mạng. Đánh giá các nguy cơ, các lỗ hổng khiến mạng có thể bị xâm phạm thông qua cách tiếp cận có cấu trúc. Xác định những nguy cơ ăn cắp, phá hoại máy tính, thiết bị, nguy cơ virus, bọ gián điệp.., nguy cơ xoá, phá hoại CSDL, ăn cắp mật khẩu,... nguy cơ đối với sự hoạt động của hệ thống như nghẽn mạng, nhiễu điện tử...Khi đánh giá được hết những nguy cơ ảnh hưởng tới an ninh mạng thì mới có thể có được những biện pháp tốt nhất để đảm bảo an ninh mạng.

Sử dụng hiệu quả các công cụ bảo mật (ví dụ như Firewall ...) và những biện pháp, chính sách cụ thể chặt chẽ.

Về bản chất có thể phân loại các vi phạm thành hai loại vi phạm thụ động và vi phạm chủ động. Thụ động và chủ động được hiểu theo nghĩa có can thiệp vào nội dung và luồng thông tin có bị tráo đổi hay không. Vi phạm thụ động chỉ nhằm mục đích nắm bắt được thông tin. Vi phạm chủ động là thực hiện sự biến đổi, xoá bỏ hoặc thêm thông tin ngoại lai để làm sai lệch thông tin gốc nhằm mục đích phá hoại. Các hành động vi phạm thụ động thường khó có thể phát hiện nhưng có thể ngăn chặn hiệu quả. Trái lại vi phạm chủ động rất dễ phát hiện nhưng lại khó ngăn chặn.

5.1.2. Các đặc trưng kỹ thuật của an toàn mạng

-Xác thực (Authentification): Kiểm tra tính xác thực của một thực thể giao tiếp trên mạng. Một thực thể có thể là một người sử dụng, một chương trình máy tính, hoặc một thiết bị phần cứng. Các hoạt động kiểm tra tính xác thực được đánh giá là quan trọng nhất trong các hoạt động của một phương thức bảo mật. Một hệ thống thông thường phải thực hiện kiểm tra tính xác thực của một thực thể trước khi thực thể đó thực hiện kết nối với hệ thống. Cơ chế kiểm tra tính xác thực của các phương thức bảo mật dựa vào 3 mô hình chính sau:

+ Đối tượng cần kiểm tra cần phải cung cấp những thông tin trước, ví dụ như Password, hoặc mã số thông số cá nhân PIN (Personal Information Number).

+ Kiểm tra dựa vào mô hình những thông tin đã có, đối tượng kiểm tra cần phải thể hiện những thông tin mà chúng sở hữu, ví dụ như Private Key, hoặc số thẻ tín dụng.

+ Kiểm tra dựa vào mô hình những thông tin xác định tính duy nhất, đối tượng kiểm tra cần phải có những thông tin để định danh tính duy nhất của mình ví dụ như thông qua giọng nói, dấu vân tay, chữ ký ...

Có thể phân loại bảo mật trên VPN theo các cách sau: mật khẩu truyền thống hay mật khẩu một lần; xác thực thông qua các giao thức (PAP, CHAP, RADIUS…) hay phần cứng (các loại thẻ card: smart card, token card, PC card), nhận diện sinh trắc học (dấu vân tay, giọng nói, quét võng mạc...).

- Tính khả dụng (Availability): Tính khả dụng là đặc tính mà thông tin trên mạng được các thực thể hợp pháp tiếp cận và sử dụng theo yêu cầu, khi cần thiết bất cứ khi nào, trong hoàn cảnh nào. Tính khả dụng nói chung dùng tỷ lệ giữa thời gian hệ thống được sử dụng bình thường với thời gian quá trình hoạt động để đánh giá. Tính khả dụng cần đáp ứng những yêu cầu sau: Nhận biết và phân biệt thực thể, khống chế tiếp cận (bao gồm cả việc khống chế tự tiếp cận và khống chế tiếp cận cưỡng bức), khống chế lưu lượng (chống tắc nghẽn..), khống chế chọn đường (cho phép chọn đường nhánh, mạch nối ổn định, tin cậy), giám sát tung tích (tất cả các sự kiện phát sinh trong hệ thống được lưu giữ để phân tích nguyên nhân, kịp thời dùng các biện pháp tương ứng).

-Tính bảo mật (Confidentialy): Tính bảo mật là đặc tính tin tức không bị tiết lộ cho các thực thể hay quá trình không được uỷ quyền biết hoặc không để cho các đối tượng đó lợi dụng. Thông tin chỉ cho phép thực thể được uỷ quyền sử dụng. Kỹ thuật bảo mật thường là phòng ngừa dò la thu thập (làm cho đối thủ không thể dò la thu thập được thông tin), phòng ngừa bức xạ (phòng ngừa những tin tức bị bức xạ ra ngoài bằng nhiều đường khác nhau, tăng cường bảo mật thông tin (dưới sự khống chế của khoá mật mã), bảo mật vật lý (sử dụng các phương pháp vật lý để đảm bảo tin tức không bị tiết lộ).

-Tính toàn vẹn (Integrity): Là đặc tính khi thông tin trên mạng chưa được uỷ quyền thì không thể tiến hành biến đổi được, tức là thông tin trên mạng khi đang lưu giữ hoặc trong quá trình truyền dẫn đảm bảo không bị xoá bỏ, sửa đổi, giả mạo, làm rối loạn trật tự, phát lại, xen vào một cách ngẫu nhiên hoặc cố ý và những sự phá hoại khác. Những nhân tố chủ yếu ảnh hưởng tới sự toàn vẹn thông tin trên mạng gồm: sự cố thiết bị, sai mã, bị tác động của con người, virus máy tính…

Một số phương pháp bảo đảm tính toàn vẹn thông tin trên mạng:

+ Giao thức an toàn có thể kiểm tra thông tin bị sao chép, sửa đổi hay sao chép. Nừu phát hiện thì thông tin đó sẽ bị vô hiệu hoá.

+ Phương pháp phát hiện sai và sửa sai. Phương pháp sửa sai mã hoá đơn giản nhất và thường dùng là phép kiểm tra chẵn - lẻ.

+ Biện pháp kiểm tra mật mã ngăn ngừa hành vi xuyên tạc và cản trở truyền tin.

+ Chữ ký điện tử: bảo đảm tính xác thực của thông tin.

+ Yêu cầu cơ quan quản lý hoặc trung gian chứng minh tính chân thực của thông tin.

- Tính khống chế (Accountlability): Là đặc tính về năng lực khống chế truyền bá và nội dung vốn có của tin tức trên mạng.

-Tính không thể chối cãi (Nonreputation): Trong quá trình giao lưu tin tức trên mạng, xác nhận tính chân thực đồng nhất của những thực thể tham gia, tức là tất cả các thực thể tham gia không thể chối bỏ hoặc phủ nhận những thao tác và cam kết đã được thực hiện.

5.1.3. Các lỗ hổng và điểm yếu của mạng

- Các lỗ hổng bảo mật hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng tồn tại trong các dịch vụ như Sendmail, Web,Ftp ... và trong hệ điều hành mạng như trong Windows NT, Windows 95, UNIX; hoặc trong các ứng dụng. Các loại lỗ hổng bảo mật trên một hệ thống được chia như sau:

+ **Lỗ hổng loại C**: cho phép thực hiện các phương thức tấn công theo kiểu từ chối dịch vụ DoS (Dinal of Services). Mức nguy hiểm thấp, chỉ ảnh hưởng chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống, không phá hỏng dữ liệu hoặc chiếm quyền truy nhập.

+ **Lổ hổng loại B**: cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ. Mức độ nguy hiểm trung bình, những lỗ hổng này thường có trong các ứng dụng trên hệ thống, có thể dẫn đến hoặc lộ thông tin yêu cầu bảo mật.

+ **Lỗ hổng loại A**: Các lỗ hổng này cho phép người sử dụng ở ngoài cho thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

- Các phương thức tấn công mạng: Kẻ phá hoại có thể lợi dụng những lỗ hổng trên để tạo ra những lỗ hổng khác tạo thành một chuỗi những lỗ hổng mới. Để xâm nhập vào hệ thống, kẻ phá hoại sẽ tìm ra các lỗ hổng trên hệ thống, hoặc từ các chính sách bảo mật, hoặc sử dụng các công cụ dò xét (như SATAN, ISS) để đạt được quyền truy nhập. Sau khi xâm nhập, kẻ phá hoại có thể tiếp tục tìm hiểu các dịch vụ trên hệ thống, nắm bắt được các điểm yếu và thực hiện các hành động phá hoại tinh vi hơn.

5.1.4. Các biện pháp phát hiện hệ thống bị tấn công

Không có một hệ thống nào có thể đảm bảo an toàn tuyệt đối, mỗi một dịch vụ đều có những lỗ hổng bảo mật tiềm tàng. Người quản trị hệ thống không những nghiên cứu, xác định các lỗ hổng bảo mật mà còn phải thực hiện các biện pháp kiểm tra hệ thống có dấu hiệu tấn công hay không. Một số biện cụ thể:

- Kiểm tra các dấu hiệu hệ thống bị tấn công: Hệ thống thường bị treo hoặc bị Crash bằng những thông báo lỗi không rõ ràng. Khó xác định nguyên nhân do thiếu thông tin liên quan. Trước tiên, xác định các nguyên nhân có phải phần cứng hay không, nếu không phải hãy nghĩ đến khả năng máy bị tấn công.

- Kiểm tra các tài khoản người dùng mới lạ, nhất là ID của tài khoản đó bằng không.

- Kiểm tra sự xuất hiện các tập tin lạ. Người quản trị hệ thống nên có thói quen đặt tên tập theo mẫu nhất định để dễ dàng phát hiện tập tin lạ. Dùng các lệnh Ls-l để kiểm tra

thuộc tính Setuid và Setgid đối với những tập tinh đáng chú ý, đặc biệt là các tập tin Scripts.

- Kiểm tra thời gian thay đổi trên hệ thống, đặc biệt là các chương trình Login, Sh hoặc các Scripts khởi động ...

- Kiểm tra hiệu năng của hệ thống: Sử dụng các tiện ích theo dõi tài nguyên và các tiến trình đang hoạt động trên hệ thống như Ps hoặc Top ...

- Kiểm tra hoạt động của các dịch vụ hệ thống cung cấp: Một trong các mục đích tấn công là làm cho tê liệt hệ thống (hình thức tấn công DoS). Sử dụng các lệnh như Ps, Pstat, các tiện ích về mạng để phát hiện nguyên nhân trên hệ thống.

- Kiểm tra truy nhập hệ thống bằng các Account thông thường, đề phòng trường hợp các Âccount này bị truy nhập trái phép và thay đổi quyền hạn mà người sử dụng hợp pháp không kiểm soát được.

- Kiểm tra các file liên quan đến cấu hình mạng và dịch vụ như /etc/inetd.conf; bỏ các dịch vụ không cần thiết; đối với những dịch vụ không cần thiết chạy dưới quyền Root thì không chạy bằng các quyền yếu hơn; ví dụ Fingerd chỉ chạy với quyền Nobody.

- Kiểm tra các phiên bản của Sendmail, /bin/mail, ftp, fingerd; tham gia các nhóm tin về bảo mật để có thông tin về lỗ hổng của dịch vụ sử dụng

- Các biện pháp này kết hợp với nhau tạo nên một chính sách về bảo mật đối với hệ thống. Chi tiết về phương thức và kế hoạch xây dựng một chính sách bảo mật sẽ được trình bày trong phần ba - xây dựng chính sách bảo mật.

5.2. Một số phương thức tấn công mạng phổ biến

5.2.1. Scanner

Kẻ phá hoạt sử dụng chương trình Scanner tự động rà soát và có thể phát hiện ra những điểm yếu lỗ hổng về bảo mật trên một Server ở xa Scanner là một chương trình trên một trạm làm việc tại cục bộ hoặc trên một trạm ở xa.

Các chương trình Scanner có thể rà soát và phát hiện các số hiệu cổng (Port) sử dụng trong giao thức TCP/UDP của tầng vận chuyển và phát hiện những dịch vụ sử dụng trên hệ thống đó, nóghi lại những đáp ứng (Response) của hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra. Dựa vào những thông tin này, những kẻ tấn công có thể tim ra những điểm yếu trên hệ thống. Chương trình Scanner có thể hoạt động được trong môi trường TCP/IP, hệ điều hành UNIX, và các máy tính tương thích IBM, hoặc dòng máy Macintosh.

Các chương trình Scanner cung cấp thông tin về khả năng bảo mật yếu kém của một hệ thống mạng. Những thông tin này là hết sức hữu ích và cần thiết đối với người quản trị mạng, nhưng hết sức nguy hiểm khi những kẻ phá hoại có thông tin này.

5.2.2. Bẻ khoá (Password Cracker)

Chương trinh bẻ khoá Password là chương trình có khả năng giải mã một mật khẩu đã được mã hoá hoặc có thể vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống. Hầu hết việc mã hoá các mật khẩu được tạo ra từ một phương thức mã hoá. Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu.Có thể thay thế phá khoá trên một hệ thống phần tán, đơn giản hơn so với việc phá khoá trên một Server cục bộ.

Một danh sách các từ được tạo ra và thực hiện mã hoá từng từ. Sau mỗi lần mã hoá, sẽ so sánh với mật khẩu (Password) đã mã hoá cần phá. Nếu không trùng hợp, quá trình lại quay lại. Phương thức bẻ khoá này gọi là Bruce-Force. Phương pháp này tuy không chuẩn tắc nhưng thực hiện nhanh vì dựa vào nguyên tắc khi đặt mật khẩu người sử dụng cũng thương tuân theo một số qui tắc để thuận tiện khi sử dụng.

Thông thường các chương trình phá khoá thường kết hợp một số thông tin khác trong quá trình dò mật khẩu như: thông tin trong tập tin /etc/passwd, từ điển và sử dụng các từ lặp các từ liệt kê tuần tự, chuyển đổi cách phát âm của một từ ...

Biện pháp khắc phục là cần xây dựng một chính sách bảo vệ mật khẩu đúng đắn.

5.2.3. Trojans

Một chương trình Trojan chạy không hợp lệ trên một hệ thống với vai trò như một chương trình hợp pháp. Nó thực hiện các chức năng không hợp pháp. Thông thường, Trojans có thể chạy được là do các chương trình hợp pháp đã bị thay đổi mã bằng những mã bất hợp pháp. Virus là một loại điển hình của các chương trình Trojans, vì các chương trình virus che dấu các đoạn mã trong những chương trình sử dụng hợp pháp. Khi chương trình hoạt động thì những đoạn mã ẩn sẽ thực hiện một số chức năng mà người sử dụng không biết.

Trojan có nhiều loại khác nhau. Có thể là chương trình thực hiện chức năng ẩn dấu, có thể là một tiện ích tạo chỉ mục cho file trong thư mục, hoặc một đoạn mã phá khoá, hoặc cố thể là một chương trình xử lý văn bản hoặc một tiện ích mạng...

Trojan có thể lây lan trên nhiều môi trường hệ điều hành khác nhau. Đặc biệt thường lây lan qua một số dịch vụ phổ biến như Mail, FTP... hoặc qua các tiện ích, chương trình miễn phí trên mạng Internet. Hầu hết các chương trình FTP Server đang sử dụng là những phiên bản cũ, có nguy cơ tiềm tàng lây lan Trojans.

Đánh giá mức độ phá hoại của Trojans là hết sức khó khăn. Trong một số trường hợp, nó chỉ làm ảnh hương đến các truy nhập của ngwời sử dụng. Nghiêm trọng hơn, nó là những kẻ tán công lỗ hổng bảo mật mạng. Khi kẻ tấn công chiếm được quyền Root trên hệ thống, nó có thể pháhuỷ toàn bộ hoặc một phần của hệ thống. Chúng sử dụng các quyền Root để thay đổi logfile, cài đặt các chương trình Trojans khác mà người quản trị không thể phát hiện được và người quản trị hệ thống đó chỉ còn cách là cài đặt lại toàn bộ hệ thống

5.2.4. Sniffer

Sniffer theo nghĩa đen là ”đánh hơi” hoặc ”ngửi”. Là các công cụ (có thể là phần cứng hoặc phần mềm) "tóm bắt" các thông tin lưu chuyển trên mạng để "đánh hơi" những thông tin có giá trị trao đổi trên mạng. Hoạt động của Sniffer cũng giống như các chương trình "tóm bắt" các thông tin gõ từ bàn phím (Key Capture). Tuy nhiên các tiện ích Key Capture chỉ thực hiện trên một trạm làm việc cụ thể, Sniffer có thể bắt được các thông tin trao đổi giữa nhiều trạm làm việc với nhau. Các chương trình Sniffer hoặc các thiết bị Sniffer có thể ”ngửi” các giao thức TCP, UDP, IPX .. ở tầng mạng. Vì vậy nó có thể tóm bắt các gói tin IP Datagram và Ethernet Packet. Mặt khác, giao thức ở tầng IP được định nghĩa tường minh và cấu trúc các trường Header rõ ràng, nên việc giải mã các gói tin không khó khăn lắm. Mục đích của các chương trình Sniffer là thiết lập chế độ dùng chung (Promiscuous) trên các Card mạng Ethernet, nơi các gói tin trao đổi và "tóm bắt" các gói tin tại đây.

5.3. Biện pháp đảm bảo an ninh mạng

Thực tế không có biện pháp hữu hiệu nào đảm bảo an toàn tuyệt đối cho mạng. Hệ thống bảo vệ dù có chắc chắn đến đâu thì cũng có lúc bị vô hiệu hoá bởi những kẻ phá hoại điêu luyện. Có nhiều biện pháp đảm bảo an ninh mạng.

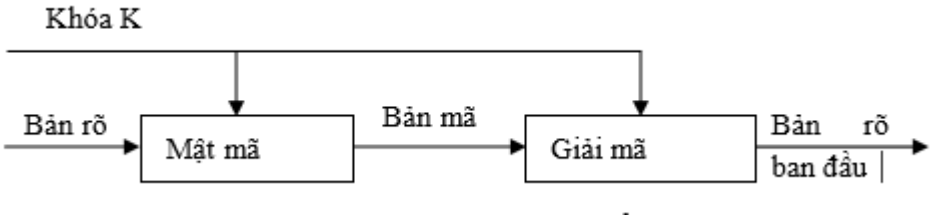
5.3.1. Tổng quan về bảo vệ thông tin bằng mật mã (Cryptography)

Mật mã là quá trình chuyển đổi thông tin gốc sang dạng mã hóa (Encryption). Có hai cách tiếp cận để bảo vệ thông tin bằng mật mã: theo đường truyền (Link Oriented Security) và từ mút- đến-mút (End-to-End).

Trong cách thứ nhất, thông tin được mã hoá để bảo vệ trên đường truyền giữa 2 nút không quan tâm đến nguồn và đích của thông tin đó. Ưu điểm của cách này là có thể bí mật được luồng thông tin giữa nguồn và đích và có thể ngăn chặn được toàn bộ các vi phạm nhằm phân tích thông tin trên mạng. Nhược điểm là vì thông tin chỉ được mã hoá trên đường truyền nên đòi hỏi các nút phải được bảo vệ tốt.

Ngược lại, trong cách thứ hai, thông tin được bảo vệ trên toàn đường đi từ nguồn tới đích. Thông tin được mã hoá ngay khi mới được tạo ra và chỉ được giải mã khi đến đích. Ưu điểm của tiếp cận này là người sử dụng có thể dùng nó mà không ảnh hưởng gì đến người sử dụng khác. Nhược điểm của phương pháp là chỉ có dữ liệu người sử dụng được mã hoá, còn thông tin điều khiển phải giữ nguyên để có thể xử lý tại các node.

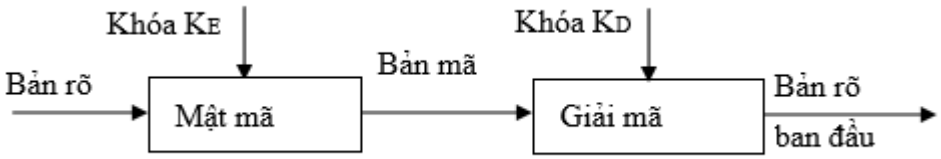
Giải thuật DES mã hoá các khối 64 bits của văn bản gốc thành 64 bits văn bản mật bằng một khoá. Khoá gồm 64 bits trong đó 56 bits được dùng mã hoá và 8 bits còn lại được dùng để kiểm soát lỗi. Một khối dữ liệu cần mã hoá sẽ phải trải qua 3 quá trình xử lý: Hoán vị khởi đầu, tính toán phụ thuộc khoá và hoán vị đảo ngược hoán vị khởi đầu.



Hình 5-1: Mô hình mật mã đối xứng

Phương pháp sử dụng khoá công khai (Public key): Các phương pháp mật mã chỉ dùng một khoá cho cả mã hoá lẫn giải mã đòi hỏi người gửi và người nhận phải biết khoá và giữ bí mật. Tồn tại chính của các phương pháp này là làm thế nào để phân phối khoá một cách an toàn, đặc biệt trong môi trường nhiều người sử dụng. Để khắc phục, người ta thường sử dụng phương pháp mã hoá 2 khoá, một khoá công khai để mã hoá và một mã bí mật để giải mã. Mặc dù hai khoá này thực hiện các thao tác ngược nhau nhưng không thể suy ra khoá bí mật từ khoá công khai và ngược lại nhờ các hàm toán học đặc biệt gọi là các hàm sập bẫy một chiều (trap door one-way functions). Đặc điểm các hàm này là phải biết được cách xây dựng hàm thì mới có thể suy ra được nghịch đảo của nó.

Giải thuật RSA dựa trên nhận xét sau: phân tích ra thừa số của tích của 2 số nguyên tố rất lớn cực kỳ khó khăn. Vì vậy, tích của 2 số nguyên tố có thể công khai, còn 2 số nguyên tố lớn có thể dùng để tạo khoá giải mã mà không sợ bị mất an toàn. Trong giải thuật RSA mỗi trạm lựa chọn ngẫu nhiên 2 số nguyên tố lớn p và q và nhân chúng với nhau để có tích n=pq (p và q được giữ bí mật).



Hình 5.2: Mô hình mật mã không đối xứng

5.3.2. Firewall

Firewall là một hệ thống dùng để tăng cường khống chế truy xuất, phòng ngừa đột nhập bên ngoài vào hệ thống sử dụng tài nguyên của mạng một cách phi pháp. Tất cả thông tin đến và đi nhất thiết phải đi qua Firewall và chịu sự kiểm tra của bức tường lửa. Nói chung Firewall có 5 chức năng lớn sau:

- Lọc gói dữ liệu đi vào/ra mạng lưới.

- Quản lý hành vi khai thác đi vào/ra mạng lưới

- Ngăn chặn một hành vi nào đó.

- Ghi chép nội dung tin tức và hoạt động thông qua bức tường lửa.

- Tiến hành đo thử giám sát và cảnh báo sự tấn công đối với mạng lưới.

- Ưu điểm và nhược điểm của bức tường lửa:

- Ưu điểm chủ yếu của việc sử dụng Firewall để bảo vệ mạng nội bộ. Cho phép người quản trị mạng xác định một điểm khống chế ngăn chặn để phòng ngừa tin tặc, kẻ phá hoại, xâm nhập mạng nội bộ. Cấm không cho các loại dịch vụ kém an toàn ra vào mạng, đồng thời chống trả sự công kích đến từ các đường khác. Tính an toàn mạng được củng cố trên hệ thống Firewall mà không phải phân bố trên tất cả máy chủ của mạng. Bảo vệ những dịch vụ yếu kém trong mạng. Firewall dễ dàng giám sát tính an toàn mạng và phát ra cảnh bảo. Tính an toàn tập trung. Firewall có thể giảm đi vấn đề không gian địa chỉ và che dấu cấu trúc của mạng nội bộ. Tăng cường tính bảo mật, nhấn mạnh quyền sở hữu. Firewall được sử dụng để quản lý lưu lượng từ mạng ra ngoài, xây dựng phương án chống nghẽn.

Nhược điểm là hạn chế dịch vụ có ích, vì để nâng cao tính an toàn mạng, người quản trị hạn chế hoặc đóng nhiều dịch vụ có ích của mạng. Không phòng hộ được sự tấn công của kẻ phá hoại trong mạng nội bộ, không thể ngăn chăn sự tấn công thông qua những con đường khác ngoài bức tường lửa. Firewall Internet không thể hoàn toàn phòng ngừa được sự phát tán phần mềm hoặc tệp đã nhiễm virus.

5.3.3. Các loại Firewall

Firewall lọc gói thường là một bộ định tuyến có lọc. Khi nhận một gói dữ liệu, nó quyết định cho phép qua hoặc từ chối bằng cách thẩm tra gói tin để xác định quy tắc lọc gói dựa vào các thông tin của Header để đảm bảo quá trình chuyển phát IP.

Firewall cổng mạng hai ngăn là loại Firewall có hai cửa nối đến mạng khác. Ví dụ một cửa nối tới một mạng bên ngoài không tín nhiệm còn một cửa nối tới một mạng nội bộ có thể tín nhiệm. Đặc điểm lớn nhất Firewall loại này là gói tin IP bị chặn lại.

Firewall che chắn (Screening) máy chủ bắt buộc có sự kết nối tới tất cả máy chủ bên ngoài với máy chủ kiên cố, không cho phép kết nối trực tiếp với máy chủ nội bộ. Firewall che chắn máy chủ là do bộ định tuyến lọc gói và máy chủ kiên cố hợp thành. Hệ thống Firewall có cấp an toàn cao hơn so với hệ thống Firewall lọc gói thông thường vì nó đảm bảo an toàn tầng mạng (lọc gói) và tầng ứng dụng (dịch vụ đại lý).

Firewall che chắn mạng con: Hệ thống Firewall che chắn mạng con dùng hai bộ định tuyến lọc gói và một máy chủ kiên cố, cho phép thiết lập hệ thống Firewall an toàn nhất, vì nó đảm bảo chức năng an toàn tầng mạng và tầng ứng dụng.

5.3.4. Kỹ thuật Fire wall

Lọc khung (Frame Filtering): Hoạt động trong tầng 2 của mô hình OSI, có thể lọc, kiểm tra được ở mức bit và nội dung của khung tin (Ethernet/802.3, Token Ring 802.5, FDDI,...). Trong tầng này các khung dữ liệu không tin cậy sẽ bị từ chối ngay trước khi vào mạng

Lọc gói (Packet Filtering): Kiểu Firewall chung nhất là kiểu dựa trên tầng mạng của mô hình OSI. Lọc gói cho phép hay từ chối gói tin mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các quy định của lọc Packet hay không. Các quy tắc lọc Packet dựa vào các thông tin trong Packet Header.

Nếu quy tắc lọc Packet được thoả mãn thì gói tin được chuyển qua Firewall. Nếu không sẽ bị bỏ đi. Như vậy Firewall có thể ngăn cản các kết nối vào hệ thống, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép.

Một số Firewall hoạt động ở tầng mạng (tương tự như một Router) thường cho phép tốc độ xử lý nhanh vì chỉ kiểm tra địa chỉ IP nguồn mà không thực hiện lệnh trên Router, không xác định địa chỉ sai hay bị cấm. Nó sử dụng địa chỉ IP nguồn làm chỉ thị, nếu một gói tin mang địa chỉ nguồn là địa chỉ giả thì nó sẽ chiếm được quyền truy nhập vào hệ thống. Tuy nhiên có nhiều biện pháp kỹ thuật có thể được áp dụng cho việc lọc gói tin nhằm khắc phục nhược điểm trên, ngoài trường địa chỉ IP được kiểm tra, còn có các thông tin khác được kiểm tra với các quy tắc được tạo ra trên Firewall, các thông tin này có thể là thời gian truy nhập, giao thức sử dụng, cổng ...

Firewall kiểu Packet Filtering có 2 loại:

- Packet filtering Fire wall: Hoạt động tại tầng mạng của mô hình OSI hay tầng IP trong mô hình TCP/IP. Kiểu Firewall này không quản lý được các giao dịch trên mạng.

- Circuit Level Gateway: Hoạt động tại tầng phiên (Session) của mô hình OSI hay tầng TCP trong mô hình TCP/IP. Là loại Firewall xử lý bảo mật giao dịch giữa hệ thống và người dùng cuối (VD: kiểm tra ID, mật khẩu...) loại Firewall cho phép lưu vết trạng thái của người truy nhập.

5.3.5. Kỹ thuật Proxy

Là hệ thống Firewall thực hiện các kết nối thay cho các kết nối trực tiếp từ máy khách yêu cầu.Proxy hoạt động dựa trên phần mềm. Khi một kết nối từ một người sử dụng nào đó đến mạng sử dụng Proxy thì kết nối đó sẽ bị chặn lại, sau đó Proxy sẽ kiểm tra các trường có liên quan đến yêu cầu kết nối. Nếu việc kiểm tra thành công, có nghĩa là các trường thông tin đáp ứng được các quy tắc đã đặt ra, nó sẽ tạo một cầu kết nối giữa hai node với nhau. Ưu điểm của kiểu Firewall loại này là không có chức năng chuyển

tiếp các gói tin IP, và có thể điều khiển một cách chi tiết hơn các kết nối thông qua Firewall. Cung cấp nhiều công cụ cho phép ghi lại các quá trình kết nối. Các gói tin chuyển qua Firewall đều được kiểm tra kỹ lưỡng với các quy tắc trên Firewall, điều này phải trả giá cho tốc độ xử lý.

Khi một máy chủ nhận các gói tin từ mạng ngoài rồi chuyển chúng vào mạng trong, sẽ tạo ra một lỗ hổng cho các kẻ phá hoại (Hacker) xâm nhập từ mạng ngoài vào mạng trong. Nhược điểm của kiểu Firewall này là hoạt động dựa trên trình ứng dụng uỷ quyền (Proxy).

❖ Tóm tắt Chương 5

Trong chương này, một số nội dung chính được giới thiệu:

- Tổng quan về an toàn mạng
- Một số phương thức tấn công mạng phổ biến
- Biện pháp đảm bảo an ninh mạng

❖ Câu hỏi:

1. Tổng quan về an toàn mạng
2. An toàn mạng là gì
3. Các đặc trưng kỹ thuật của an toàn mạng
4. Xác thực (Authentification), Tính khả dụng (Availability), Tính bảo mật (Confidentialy), Tính toàn vẹn (Integrity), Tính khống chế (Accountlability)
5. Các lỗ hổng và điểm yếu của mạng: Lỗ hổng loại C, Lổ hổng loại B, Lỗ hổng loại A
6. Các phương thức tấn tân công mạng
7. Các biện pháp phát hiện hệ thống bị tấn công
8. Một số phương thức tấn công mạng phổ biến: Scanner, Bẻ khoá (Password Cracker), Trojans, Sniffer
9. Tổng quan về bảo vệ thông tin bằng mật mã (Cryptography)
10. Firewall, ưu điểm và nhược điểm của Fire wall
11. Các loại Firewall
12. Kỹ thuật Fire wall

TÀI LIỆU THAM KHẢO

[1] **Ts. Phạm Thế Quế**, Sách hướng dẫn học tập Mạng máy tính, 2006

[2] **Hồ Đắc Phương**, Nhập môn Mạng máy tính, Nhà xuất bản Giáo dục Việt Nam

[3] **Khoa Công nghệ Thông tin**, Giáo trình nhập môn Mạng máy tính, Trường Trung cấp Kinh tế Kỹ thuật Quang Trung.