Chương 5

CÁC KHÁI NIỆM VÀ CÁC KỸ THUẬT MẠNG LAN

Mạng cục bộ LAN cho phép các thiết bị độc lập truyền thông trực tiếp với nhau trong không gian hẹp. Có 4 kiểu kỹ thuật LAN là Ethernet, Token Bus, Token Ring của IEEE và FDDI của ANSI, được quy định và phân biệt tại lớp 2 của môi trường OSI.

5.1. CÁC CHUẨN LAN

5.1.1. LỚP 2

Lớp 2 cung cấp khả năng truy xuất vào môi trường mạng và truyền dẫn vật lý qua môi trường, cho phép dữ liệu định vị được đích của mạng.

Trong khi lớp 1 chỉ liên quan đến các môi trường truyền tín hiệu, các luồng bit, các thành phần đưa dữ liệu vào môi trường và các cấu hình khác nhau thì lớp 2 có nhiệm vụ chính là đưa các giải pháp để liên kết dữ liệu. Vì lớp 1 không thể thông tin được với các lớp ở phía trên, lớp 2 làm nhiệm vụ này thông qua LLC (*Logical Link Control*). Lớp 1 không thể đặt tên hay nhận diện các máy tính thì lớp 2 dùng một quá trình đánh địa chỉ hay đặt tên cho các máy tính. Lớp 1 không thể quyết định được máy tính nào sẽ truyền dữ liệu từ một nhóm muốn truyền tại cùng thời điểm thì lớp 2 dùng hệ thống MAC (*Media Access Control*) để giải quyết việc này. Lớp 1 chỉ có thể làm việc với dòng các bit, còn lớp 2 có thể nhóm lại và tổ chức các bit thành các khung số liệu.

Institute of Electrical and Electronic Engineers (IEEE) là một tổ chức chuyên môn định ra các tiêu chuẩn mạng chuyên nghiệp. Các chuẩn IEEE (trong đó có IEEE 802.3 và IEEE 802.5) là các chuẩn LAN phổ biến nhất trên thế giới hiện nay. Các chuẩn IEEE chỉ liên quan đến hai lớp dưới cùng, do đó lớp liên kết dữ liệu được chia thành hai phần:

- Chuẩn 802.2 LLC không phụ thuộc kỹ thuật.
- Các phần riêng biệt, phụ thuộc kỹ thuật các phần này kết hợp chặt chẽ với khả năng kết nối của lớp 1.

IEEE chia lớp liên kết dữ liệu trong mô hình OSI thành hai lớp phụ:

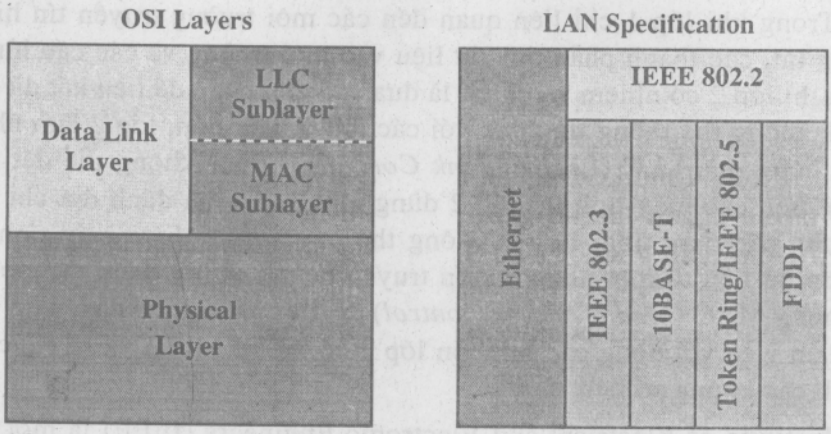
- Media Access Control (*MAC*): chuyển tiếp xuống môi trường.
- Logical Link Control (*LLC*): chuyển tiếp lên lớp mạng.

5.1.2. SO SÁNH MÔ HÌNH IEEE VỚI MÔ HÌNH OSI

Khi chuẩn IEEE xuất hiện, thoạt nhìn nó khác với mô hình OSI ở hai cách thể hiện. Nó định nghĩa lớp sở hữu của nó (LLC), bao gồm đơn vị dữ liệu giao thức PDU (*Protocol Data Unit*), các giao tiếp... và xuất hiện các chuẩn MAC 802.3 và 802.5, xuyên qua giao tiếp giữa lớp 1 và lớp 2.

Căn bản, mô hình OSI là một hướng dẫn thống nhất; IEEE xuất hiện sau để giải quyết những vấn đề mạng khi chúng được xây dựng. Chúng vẫn dùng mô hình OSI, nhưng điều lưu ý là chức năng của LLC và MAC trong lớp liên kết dữ liệu của OSI.

Một khác biệt khác giữa mô hình OSI và các chuẩn IEEE là NIC. NIC là nơi địa chỉ lớp 2 cư trú, nhưng trong nhiều kỹ thuật, NIC cũng có tranceiver (một thiết bị lớp 1) tích hợp trong nó và kết nối trực tiếp đến môi trường vật lý. Vì vậy sẽ là chính xác nếu đặc tính hóa NIC như là thiết bị của cả lớp 1 và lớp 2.



Hình 5.1. *So sánh và tương phản lớp 1 và lớp 2 của mô hình OSI với chuẩn kỹ thuật của LAN.*

5.2. LOGICAL LINK CONTROL - LLC (Điều khiển liên kết logic)

LLC giống nhau cho mọi LAN. MAC chứa một số khối riêng biệt, mỗi khối đại diện riêng cho từng LAN đang được sử dụng. Điểm mạnh của 802 là tính chất chia khối (*modularity*) để chuẩn hóa những cái chung và giữ lại những điểm riêng khác. Ví dụ 802.1 - liên kết mạng; 802.3 - LLC; các modul MAC: 802.3 - Ethernet-CSMA/CD, 802.4 - Token Bus, 802.5 - Token Ring...

LLC cho phép một phần của lớp datalink thực hiện chức năng một cách độc lập đối với các kỹ thuật có sẵn. Lớp này tạo ra tính linh hoạt trong việc phục vụ cho các giao thức lớp mạng trên nó, trong khi vẫn liên lạc hiệu quả với các kỹ thuật khác nhau bên dưới nó.

LLC là lớp phụ tham gia vào quá trình đóng gói. LLC nhận đơn vị dữ liệu giao thức lớp mạng, như là các gói IP, và thêm nhiều thông tin điều khiển vào để giúp phân phối gói IP đến đích của nó. Nó thêm hai thành phần địa chỉ của đặc tả 802.2: điểm truy xuất dịch vụ đích DSAP (*Destination Service Access Point*) và điểm truy xuất dịch vụ nguồn SSAP (*Source Service Access Point*). Nó đóng gói trở lại dạng IP, sau đó chuyển xuống lớp phụ MAC để tiến hành các kỹ thuật đóng gói tiếp theo. Ví dụ về kỹ thuật đặc biệt này có lẽ là một trong số Ethernet, Token Ring hay FDDI.

5.3. ĐÁNH ĐỊA CHỈ MAC

5.3.1. CÁC ĐỊA CHỈ MAC VÀ CÁC NIC

Mỗi máy tính có một cách tự định danh duy nhất, dù được gắn vào mạng hay không đều có một địa chỉ vật lý, hai địa chỉ vật lý không bao giờ giống nhau. Chúng được gọi là địa chỉ MAC là địa chỉ vật lý nằm trên NIC. Khi rời nhà máy, nhà sản xuất phần cứng gán địa chỉ vật lý cho mỗi NIC bằng cách lập trình vào một chip của NIC. Nếu NIC được thay thế thì địa chỉ vật lý của trạm cũng thay đổi theo và tương ứng có một địa chỉ vật lý mới. Địa chỉ MAC được viết dưới dạng số Hex, với hai dạng chính: 0000.0c12.3456 hay 00-00-0c-12-34-56.

5.3.2. NIC DÙNG CÁC ĐỊA CHỈ MAC NHƯ THẾ NÀO

Ethernet và 802.3 LAN là các mạng quảng bá. Tất cả các trạm đều thấy frame truyền. Mỗi trạm phải kiểm tra mỗi frame để xác định xem nó có phải là đích của frame hay không.

Khi thiết bị nguồn gửi dữ liệu lên mạng, một phần quan trọng trong quá trình gói (tách) frame tại lớp 2 là thêm địa chỉ MAC nguồn và đích vào. Khi dữ liệu lan truyền, NIC trên mỗi thiết bị mạng kiểm tra xem địa chỉ MAC của nó có trùng với địa chỉ vật lý đích được mang trong dữ liệu hay không. Nếu không trùng, NIC loại bỏ frame.

Khi dữ liệu đi ngang qua máy đích của nó, NIC của trạm này sẽ copy và lấy dữ liệu ra để cung cấp cho máy tính.

5.3.3. HẠN CHẾ CỦA ĐỊA CHỈ MAC

Địa chỉ MAC là yếu tố sống còn để thực hiện chức năng của một mạng máy tính. Nó cung cấp phương thức để các máy tính có thể tự nhận dạng, cung cấp cho các host một tên cố định và duy nhất. Tối đa 16^{12} địa chỉ có thể. Địa chỉ MAC có một khuyết điểm chính là không có cấu trúc và được xem như không gian địa chỉ phẳng. Khi mà một mạng máy tính lớn, khuyết điểm này trở thành một vấn đề thực tế.

5.3.4. ĐIỀU KHIỂN TRUY XUẤT MÔI TRƯỜNG (MAC)

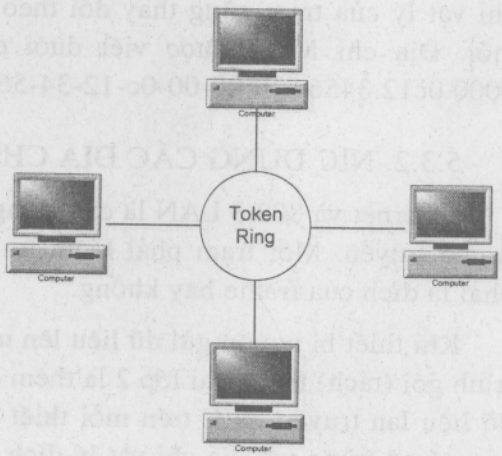
MAC liên hệ đến các giao thức dùng để xác định máy tính nào trên môi trường chia sẻ (miền đụng độ-collision) được phép truyền dữ liệu. Có hai loại MAC tổng quát: deterministic (lấy lượt) và non-deterministic (vào trước được phục vụ trước).

1. Các giao thức MAC lấy lượt

Tình huống này tương tự như giao thức liên kết dữ liệu Token Ring, các host riêng biệt được sắp xếp theo một vòng tròn. Một *token* (thẻ) đặc biệt chạy trên vòng. Khi một host muốn truyền dữ liệu, nó bắt lấy token, truyền dữ liệu trong một thời gian nhất định, sau đó đặt token trở lại vòng, để chuyển đi hoặc bị tóm bởi các host khác.

2. Các giao thức MAC không lấy lượt

Các giao thức MAC không lấy lượt dùng tiếp cận first-come, first-served (FCFS), cho phép bất cứ trạm nào cũng có thể truyền dữ liệu vào bất cứ lúc nào. Điều này dẫn đến sự đụng độ. Có thể phát hiện bằng cách lắng nghe trong khi truyền, sử dụng giao thức MAC *đa truy nhập cảm nhận sóng mang có phát hiện đụng độ* CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*).



***Hình 5.2**. Token Ring.*

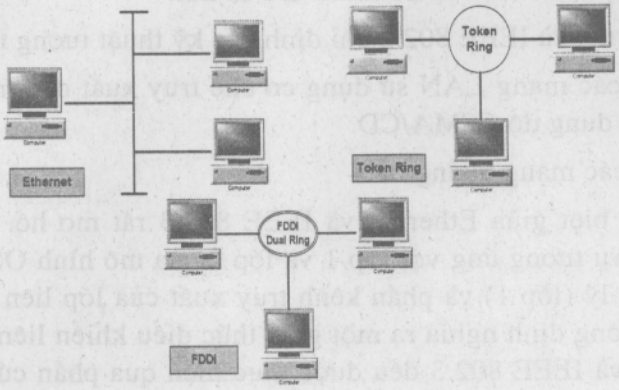
5.3.5. BA KỸ THUẬT MAC

Có 3 kỹ thuật ở lớp 2 là Token Ring, FDDI và Ethernet.

Ethernet: Cấu hình bus logic (thông tin chạy trên một bus tuyến tính) và cấu hình sao hay sao mở rộng.

Token Ring: Cấu hình ring logic (luồng thông tin được điều khiển trên một ring) và cấu hình sao vật lý.

FDDI: Cấu hình ring logic và cấu hình ring đôi về mặt vật lý (nối dây ring đôi).



***Hình 5.3.** Các kỹ thuật LAN thông dụng.*

5.4. ETHERNET

Công nghệ ETHERNET hiện đang là một trong các công nghệ được sử dụng rộng rãi nhất với các giao thức mạng tầng thấp. Trong phần này, chúng tôi sẽ giới thiệu sơ bộ về ETHERNET đến với bạn đọc

5.4.1. SO SÁNH ETHERNET VÀ IEEE 802.3

Ethernet là kỹ thuật mạng cục bộ được sử dụng rộng rãi nhất, được thiết kế lắp vào khoảng trống giữa các mạng cự ly dài tốc độ thấp và các mạng văn phòng tốc độ cao cự ly rất giới hạn. Ethernet phù hợp với môi trường phải mang tải nặng, rời rạc hay không thường xuyên có tốc độ dữ liệu đỉnh khá cao.

Vào đầu thập niên 80 thế kỷ XX, tại Palo Alto, California có Trung tâm nghiên cứu Palo Alto (PARC), là nơi phiên bản nguyên thuỷ của ETHERNET ra đời. PARC là trung tâm nghiên cứu thuộc hãng Xerox. Vào năm 1970, Xerox nghiên cứu hướng đi trong tương lai của mình. Công việc kinh doanh của Hãng bao gồm: thiết kế, sản xuất và cung cấp máy photocopy. Xerox có nhiều kiến thức và các công nghệ đi kèm cho các sản phẩm đó. Tương tự như vậy, hãng cũng có hiểu rằng văn phòng tương lai

phải là văn phòng trang bị máy tính và các thiết bị đầu cuối, theo đó các nhu cầu về máy photocopy sẽ giảm đi, chính vì vậy mà PARC đã ra đời. Vào năm 1973, một thành viên của PARC là Bob Metcalfe đã tập trung vào giải quyết vấn đề cơ bản của mạng, đó là thời gian cần để chuyển dữ liệu từ máy tính đến máy in. Vấn đề "thắt nút cổ chai" không nằm ở máy tính cũng như máy in, thắt nút cổ chai đã làm thời gian chuyển dữ liệu từ máy tính đến máy in mất hơn 10 phút với đường kết nối cao. Điều đó đã được nghiên cứu khắc phục và thế là ETHERNET ra đời.

Ethernet và IEEE 802.3 chỉ định các kỹ thuật tương tự nhau:

- Là các mạng LAN sử dụng cơ chế truy xuất cảm nhận sóng mang có phát hiện đụng độ CSMA/CD.

- Là các mạng quảng bá.

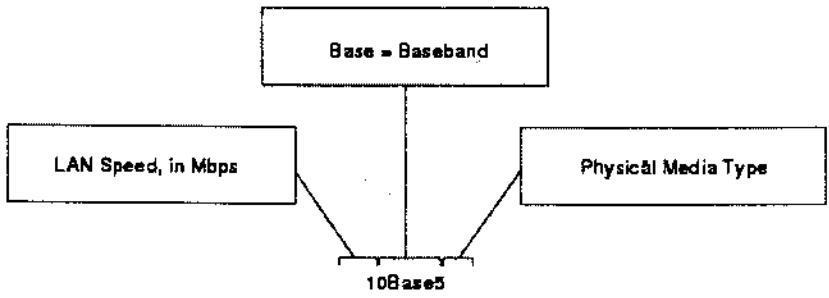
Khác biệt giữa Ethernet và IEEE 802.3 rất mơ hồ. Ethernet cung cấp các dịch vụ tương ứng với lớp 1 và lớp 2 của mô hình OSI. IEEE 802.3 đặc tả lớp vật lý (lớp 1) và phần kênh truy xuất của lớp liên kết dữ liệu (lớp 2) nhưng không định nghĩa ra một giao thức điều khiển liên kết logic LLC. Cả Ethernet và IEEE 802.3 đều được thực hiện qua phần cứng. Thông thường, phần vật lý của các giao thức này là một card giao tiếp trong máy tính hoặc một mạch trên bản mạch chính của máy tính.

5.4.2. HỌ ETHERNET

Ethernet quy định hai lĩnh vực:

- *Baseband* quy định tín hiệu số (mã Manchester), IEEE chia làm các chuẩn: 10Base5, 10Base2, 10Base-T, 1Base5 và 100Base-T, 100Base-TX, 10Base-FL, 100Base-FX, 1000Base-T. Số đầu (*10, 100...*) là tốc độ dữ liệu Mbps. Ký tự cuối (*5, T....*) là độ dài cáp cực đại hoặc loại cáp, số cuối cùng X có nghĩa loại chuẩn hoạt động được ở mode song công (full duplex)

- *Broadband* quy định tín hiệu tương tự (mã PSK). IEEE chỉ quy định một chuẩn 10Broad36.



***Hình 5.4.** Quy ước đặt tên mạng của IEEE.*

Bảng 5.1. Quy định các chuẩn họ Ethernet.

Type	Medium	Maximum Bandwidth	Maximum Segment Length	Physical Topology	Logical Topology
10BASE5	Thick Coat	10 Mbps	500 m	Bus	Bus
10BASE-T	CAT 5 UTP	10 Mbps	100 m	Extended Star	Bus
10BASE-FL	Multimode Optical Fiber	10 Mbps	2000 m	Star	Bus
100BASE-TX	CAT 5 UTP	100 Mbps	100 m	Star	Bus
100BASE-FX	Multimode Optical Fiber	100 Mbps	2000 m	Star	Bus
1000BASE-T	CAT 5 UTP	1000 Mbps	100 m	Star	Bus

5.4.3. KHUÔN DẠNG FRAME CỦA ETHERNET

Tại lớp liên kết dữ liệu, cấu trúc frame gần như đồng nhất cho tất cả các tốc độ của Ethernet từ 10 đến 10000Mbps. Tuy nhiên, tại lớp vật lý hầu như tất cả các phiên bản của Ethernet đều khác nhau về cơ bản với mỗi tốc độ đều có một tập riêng về các nguyên tắc thiết kế kiến trúc.

Trong phiên bản Ethernet được phát triển bởi DIX, trước IEEE 802.3, Preamble và Start Frame Delimiter (SFD) được kết hợp trong một field, cho dù mẫu nhị phân là đồng dạng. Length/Type field chỉ được liệt kê là Length trong các phiên bản đầu của IEEE và chỉ là Type trong phiên bản DIX. Việc sử dụng hai field này được kết hợp một cách chính thức trong phiên bản sau cùng của IEEE, khi cả hai đều phổ biến trong công nghệ.

Bảng 5.2. Khuôn dạng frame của Ethernet và IEEE 802.3.

Ethernet						
7	1	6	6	2	46-1500	4
Preamble	Start of frame delimiter	Destination Address	Source Address	Type	Data	Frame Check Sequence
IEEE 802.3						
7	1	6	6	2	64-1500	4
Preamble	Start of frame delimiter	Destination Address	Source Address	Length	Data	Frame Check Sequence

Ethernet II Type được kết hợp trong định nghĩa frame 802.3 hiện hành. Node tiếp nhận phải xác định giao thức cao hơn nào hiện diện trong mỗi frame đến bằng cách kiểm tra Length/Type field. Nếu giá trị của hai octet là bằng nhau hay lớn hơn 0x600, thì frame được biên dịch theo mã Ethernet II được chỉ định.

Vài field được phép hay được yêu cầu trong một 802.3 Ethernet là:

- Preamble
- Start Frame delimiter.
- Destination Address.
- Source Address.
- Length/Type
- Data và Pad (Số liệu và byte nhồi)
- FCS.
- Extension (mở rộng)

Preamble là một mẫu chứa các bit 1 và 0 xen kẽ nhau được dùng để đồng bộ trong hoạt động truyền bất đồng bộ từ 10Mbps trở xuống. Các phiên bản nhanh hơn của Ethernet là đồng bộ thì thông tin định thời này là dư thừa nhưng vẫn được giữ lại nhằm mục đích tương thích.

Start Frame Delimiter gồm một file dài một octet đánh dấu kết thúc phần thông tin định thời và chứa tuần tự bit 10101011.

Trường (Field) địa chỉ đích (Destination address) chứa địa chỉ MAC đích. Địa chỉ đích có thể là unicast, multicast hay broadcast.

Field địa chỉ nguồn (Source address) chứa địa chỉ MAC của nguồn. Địa chỉ đích có thể là unicats của node Ethernet truyền. Tuy nhiên có một số giao thức ảo gia tăng không ngừng sử dụng và đôi khi chia sẻ một địa chỉ MAC nguồn để nhận diện một thực thể ảo.

Field length/Type hỗ trợ cho hai mục đích sử dụng khác nhau. Nếu giá trị là nhỏ hơn 0x600 thì đó là giá trị chỉ chiều dài frame. Sử dụng như là field chỉ chiều dài ở những nơi đã có lớp LLC cung cấp sự nhận diện giao thức. Giá trị loại chỉ ra loại giao thức lớp trên sẽ tiếp nhận dữ liệu sau khi xử lý frame Ethernet hoàn tất. Chiều dài chỉ ra số byte dữ liệu kể từ sau field này trở đi. Nếu giá trị bằng 0x600 hay lớn hơn chỉ ra loại và nội dung của field dữ liệu được giải mã trên từng giao thức chỉ định.

Data và Pad field có chiều dài tuỳ ý miễn sao không làm kích thước frame vượt quá giá trị tối đa cho phép. Đơn vị truyền tối đa của Ethernet là 1500 octet. Nội dung của field không được chỉ định. Một Pad được chèn vào ngay sau số liệu người dùng khi không đủ số liệu cho frame đạt được một kích thước tối thiểu theo quy định. Ethernet yêu cầu frame không được nhỏ hơn 64 octet và không được lớn hơn 1518 octet.

Một FCS chứa bốn byte CRC được tạo ra bởi thiết bị truyền và được tính toán trở lại bởi thiết bị thu để kiểm tra sự hư hỏng của frame. Vì sự sai

sót bất cứ ở đâu từ đầu của địa chỉ nguồn cho đến kết thúc của FCS đều gây ra sự sai khác giữa hai giá trị FCS được tính ở nguồn và đích, nên khả năng của kiểm tra bao hàm luôn FCS. Không dễ dàng phân biệt giữa sai sót trong chính bản thân FCS hay trong các field trước nó trong hoạt động kiểm tra. Một vài phương pháp kiểm soát lỗi FEC có thể phân biệt được như phương pháp kiểm tra Hamming.

5.4.4. ETHERNET MAC

Khi nhiều trạm thâm nhập một đường truyền, sẽ có nguy cơ lấn át tín hiệu và phá hoại lẫn nhau. Đó là hiện tượng xung đột (*collisions*). Do vậy, LAN sử dụng một cơ cấu để giảm thiểu xung đột, tăng số khung được truyền thành công, gọi là *đa thâm nhập sử dụng sóng mang có phát hiện xung đột* CSMA/CD.

Trong phương pháp này, các trạm có dữ liệu muốn truyền làm việc trong chế độ lắng nghe trước khi truyền, xem môi trường mạng có bận hay không. Điều này thực hiện bằng cách kiểm tra điện thế, nếu 0^V là đường truyền im lặng và việc truyền có thể bắt đầu. Trong khi truyền, thiết bị cũng phải lắng nghe để đảm bảo không có trạm nào khác đang truyền. Sau khi hoàn thành, thiết bị sẽ trở về chế độ lắng nghe.

Đụng độ được nhận biết khi biên độ của tín hiệu gia tăng. Khi đó, trạm đang truyền sẽ tiếp tục truyền dữ liệu trong một thời gian ngắn để tất cả các thiết bị đều thấy có xung đột. Chúng dùng một giải thuật để quay lui trong một khoảng thời gian. Bất kỳ thiết bị nào đều cố gắng đạt được truy cập vào môi trường một lần nữa. Khi hoạt động truyền tiếp tục diễn ra, các trạm liên hệ đến đụng độ sẽ không có mức ưu tiên truyền.

Ethernet là môi trường truyền quảng bá. Nhưng chỉ trạm nào có địa chỉ MAC và IP trùng địa chỉ MAC và IP trong frame dữ liệu mới được sao chép dữ liệu. Qua bước này, trạm sẽ kiểm tra lỗi cho gói dữ liệu. Nếu phát hiện lỗi, gói dữ liệu này sẽ bị loại bỏ. Trạm đích không thông báo cho trạm nguồn bất chấp gói dữ liệu có được tiếp nhận thành công hay không. Ethernet là một kiến trúc mạng không tạo cầu nối (*connectionless*) và được thừa nhận là hệ thống phân phối cố gắng nhất (*best-effort*).

5.4.5. 10MBPS ETHERNET

1. 10BASE5

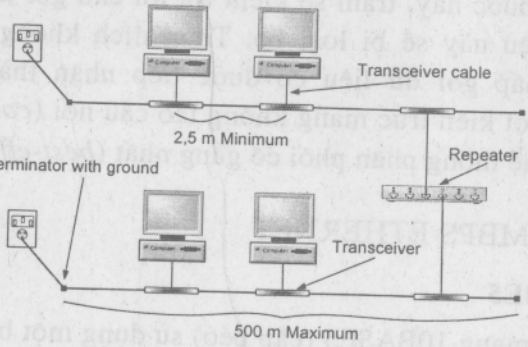
Cấu trúc mạng 10BASE5 (cáp béo) sử dụng một bộ thu phát ngoại vi để gắn kết với card adapter mạng hình 5.6. Thiết bị thu phát ngoại vi gắn chặt

vào cáp đồng trục béo. Một cáp loại AUI (Attachment Universal Interface) chạy từ transceiver đến một DIX connector ở mặt sau của card adapter mạng. Tương tự như đối với mạng Thinnet, mỗi một segment mạng đều phải có terminator ở cả hai đầu, và với một đầu sử dụng một terminator được nối đất.

Ưu điểm chủ yếu của 10BASE5 là khả năng mở rộng giới hạn về chiều dài của cable so với 10BASE2. Tuy nhiên, 10BASE5 cũng đặt ra các giới hạn của riêng nó. Các giới hạn này cần phải được xem xét đến khi cài đặt hay sửa chữa một mạng 10BASE5. Tương tự như đối với mạng 10BASE2, mạng 10BASE5 cũng có một số quy định riêng bên cạnh quy tắc 5-4-3 như sau:

- Khoảng cách tối thiểu giữa các transceiver là 2,5 meters (8 feet).
- Chiều dài tối đa của một segment mạng là 500 meters (1640 feet).
- Độ dài cable của toàn bộ mạng không thể vượt quá 2500 meters (8200 feet).
- Một terminator của segment mạng phải được nối đất.
- Cáp cho bộ thu phát có thể ngắn đến mức cần thiết nhưng không thể dài hơn 50 meters tính từ transceiver đến computer.
- Số nút mạng tối đa trên một segment mạng là 100 (bao gồm cả các repeater).

Chiều dài của các cáp cho bộ thu phát (từ transceiver đến máy tính) không được tính đến trong các phép đo chiều dài của các segment mạng và chiều dài tổng cộng của toàn bộ mạng. Các mạng Thicknet và Thinnet đôi khi được kết hợp lại với nhau trong đó một mạng xương sống (backbone) Thicknet kết hợp với các segment mạng Thinnet nhỏ hơn.

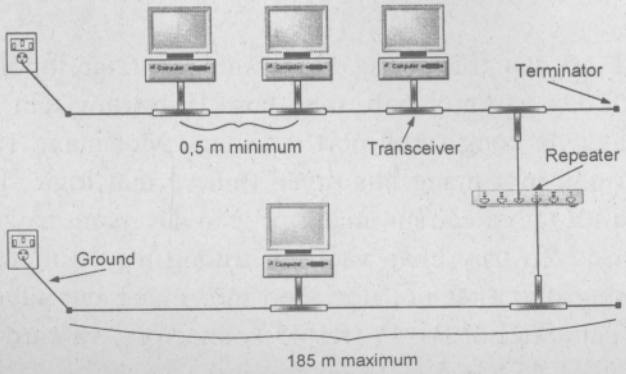


Hình 5.6. 10 Base-5

2. 10BASE2

Cấu hình mạng 10BASE2 (cáp gầy) thường sử dụng thiết bị thu phát trên bảng mạch của card giao diện mạng để truyền và thu nhận tín hiệu của mạng. Việc chạy dây cáp đồng trục gầy sử dụng các T-connector loại BNC được gắn kết trực tiếp vào adapter mạng. Mỗi một đầu cable đều phải có một terminator và bắt buộc phải dùng một terminator đã được nối đất ở một đầu cable.

Ưu điểm chủ yếu của việc sử dụng 10BASE2 là giá thành của mạng. Khi bất kỳ một đoạn cable nào trong mạng cũng không cần thiết phải dài hơn 185 meters (607 feet), thì 10BASE2 thường là giải pháp chạy cable mạng rẻ nhất.



***Hình 5.7.** 10Base-2*

Việc kết nối 10BASE2 cũng tương đối đơn giản. Mỗi một nút mạng kết nối trực tiếp vào cable mạng bằng cách sử dụng một T-connector được gắn kết vào adapter mạng. Để cài đặt thành công thì người thiết kế và cài đặt mạng cần phải tuân theo một số quy định riêng của các môi trường mạng Ethernet 10BASE2 như sau:

- Khoảng cách ngắn nhất giữa các client là 0,5 meters (1,5 feet).
- Phải sử dụng các T-connectors để kết nối với connector BNC trên adapter mạng. T-connector phải được kết nối trực tiếp với adapter mạng.
- Mỗi một segment mạng không được phép vượt quá giới hạn về độ dài là 185 meters (607 feet).
- Độ dài cable của toàn bộ mạng không thể vượt quá 925 meters (3035 feet).
- Số nút mạng tối đa trên một segment mạng là 30 (bao gồm cả các client và các repeater).
- Một terminator 50 Ω phải được sử dụng ở mỗi một đầu của bus và chỉ duy nhất một trong số các terminator đó phải được nối đất.

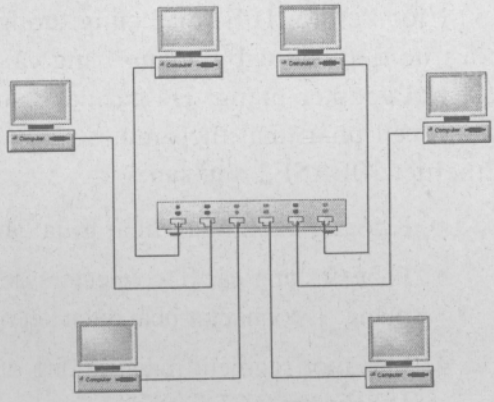
- Không được phép có nhiều hơn 5 segments trong một mạng máy. Các segment mạng này có thể được kết nối với tối đa 4 repeater, và chỉ 3 trong số 5 segments được phép có các chứa các nut mạng.
- Cần phải biết chuyển đổi chiều dài của cable từ đơn vị feet sang đơn vị meter và ngược lại. Một meter bằng 3.28 feet.

3. 10BASE-T

Xu hướng chung hiện nay là sử dụng cable loại UTP (unshielded twisted-pair) khi xây dựng các mạng Ethernet. Mạng 10BASE-T, sử dụng cable UTP, là một trong số những mạng Ethernet phổ biến nhất. 10BASE-T dựa trên chuẩn IEEE 802.3 và hỗ trợ tốc độ truyền số liệu 10 Mbps sử dụng giải tần cơ sở

10BASE-T có cấu trúc mạng kiểu hình sao (star topology). Các nút mạng được nối dây vào một hub trung tâm. Hub trung tâm này hoạt động như một repeater đa cổng (multiport repeater). Một mạng 10BASE-T hoạt động tương tự như một mạng bus tuyến tính về mặt logic. Hub trung tâm lặp lại tín hiệu tới tất cả các nút mạng, và các nút mạng này cạnh tranh với nhau để giành quyền truy nhập vào môi trường truyền một cách tương tự như thể là chúng được kết nối dọc theo một mạng bus tuyến tính. Cable UTP sử dụng các đầu nối RJ-45 (RJ-45 connectors) và card adapter mạng có các jack loại RJ-45 gắn ở mặt sau của card.

Các segment mạng 10BASE-T có thể được kết nối bằng cách sử dụng các đoạn cable xương sống loại đồng trục hoặc fiberoptic. Bên cạnh các connector loại UTP của mạng 10BASE-T, một số hub cung cấp thêm các connectors dành cho cable mạng Thinnet và Thicknet. Bằng cách gắn kết một transceiver của 10BASE-T vào cổng AUI của card adapter mạng, người ta có thể sử dụng cơ cấu bố trí máy tính của mạng Thicknet trong một mạng 10BASE-T.



Hình 5.8. 10 Base-T

Cấu trúc mạng hình sao của 10BASE-T đem lại một số ưu điểm, đặc biệt là trong các mạng rất lớn. Ưu điểm đầu tiên là mạng đáng tin cậy hơn và cũng dễ quản lý hơn, bởi vì các mạng 10BASE-T sử dụng một bộ tập

trung concentrator (một hub trung tâm). Các hub này "thông minh" ở chỗ chúng có thể phát hiện ra các đoạn cable bị hỏng và định tuyến lưu thông trong mạng tránh khỏi các đoạn cable hỏng đó. Chính khả năng này làm cho việc định vị và sửa chữa các đoạn cable hỏng trở nên dễ dàng hơn.

Mạng 10BASE-T cho phép việc thiết kế và xây dựng một mạng LAN từng phần một và có thể mở rộng và phát triển dần dần mạng nếu có nhu cầu. Điều này làm cho 10BASE-T trở nên linh động hơn hẳn so với các kiểu mạng LAN khác. 10BASE-T cũng có giá thành tương đối thấp so với các kiểu mạng LAN khả dĩ khác.

Các mạng có cấu trúc hình sao có thể sửa chữa và khắc phục sự cố một cách dễ dàng hơn rất nhiều so với các mạng bus. Với một mạng hình sao, một nút mạng có sự cố có thể được cô lập khỏi phần còn lại của mạng bằng cách ngắt đường cable và nối trực tiếp nút mạng này với hub. Nếu hub đang sử dụng là hub "thông minh" thì phần mềm quản lý của hub và bản thân hub đó có thể thực hiện việc ngắt cổng nghi là đã bị hỏng. Các quy định chung của một mạng 10BASE-T là:

- Số lượng máy tính tối đa trong một mạng LAN là 1024.
- Cable mạng phải là loại UTP Category 3, 4, hoặc 5 (cable loại STP, Shielded twisted-pair cable, có thể dùng thay cho UTP.).
- Độ dài tối đa của mỗi một đoạn cable không bọc kim (từ hub đến transceiver) là 100 meters (328 feet).
- Độ dài cable nối giữa các máy tính là 2.5 meters (8 feet).

4. 10 BASE-FL

10BASE-FL là một mạng Ethernet sử dụng cáp quang. Các đặc trưng kỹ thuật của 10BASE-FL nhằm bảo đảm tốc độ truyền số liệu 10 Mbps sử dụng băng tần cơ sở. Các ưu điểm của cáp quang (và do đó các ưu điểm của 10BASE-FL) được thảo luận kỹ ở chương 3. Các ưu điểm quan trọng nhất là độ dài đường cable (10BASE-FL cho phép sử dụng cable có chiều dài tối đa là 2000 meters) và việc loại trừ được các khó khăn phức tạp tiềm tàng về điện.

5.4.6. 100MBPS ETHERNET

100Mbps Ethernet cũng được xem là Fast Ethernet. Hai công nghệ đã trở nên quan trọng là 100BASE-TX sử dụng đường truyền cáp đồng xoắn UTP và 100 BASE-FX sử dụng đường truyền cáp quang đơn mode.

Ba đặc tính phổ biến đối với 100BASE-TX và 100BASE-FX là các thông số định thời, định dạng frame và các phần xử lý truyền. 100BASE-TX

và 100BASE-FX đều chia sẻ các thông số định thời. Lưu ý rằng một thời bit trong 100-Mbps Ethernet là 10ns.

Khuôn dạng frame 100-Mbps giống như frame 10-Mbps.

Fast Ethernet có tốc độ gấp 10 lần 10BASE-T. Bởi sự tăng tốc độ này nên phải hết sức cẩn trọng, các bit được truyền trong một khoảng thời gian hết sức ngắn với tần xuất cao. Các tín hiệu tần số cao này rất mềm yếu trước tạp âm. Đáp lại các vấn đề này, hai bước mã hoá tách biệt được dùng trong 100 - Mbps Ethernet. Bước mã hoá đầu dùng kỹ thuật được gọi là 4B/5B, bước thứ hai là sự mã hoá - đường dây thực tế được chỉ định trong cáp đồng hay cáp quang.

Bảng 5.4. Các thông số hoạt động của 100 Mbps Ethernet.

Thông số	Giá trị
Bit Time	10 nsec
Slot time	512 bit times
Interframe Spacing	96 bit
Collision Attempt Limit	16
Collision Backoff Limit	10
Collision Jam Size	32 bits
Maximum Untagged Frame Size	1518 octets
Minimum Frame Size	512 bits (64 octets)

1. 100BASE-TX

Vào năm 1995, 100 BASE-TX đã là chuẩn, dùng Cat5 UTP, trở nên thành công về mặt thương mại.

Nguồn gốc của Ethernet cáp đồng trục là truyền bán song công, chỉ một thiết bị được phép truyền vào bất cứ thời điểm nào. Tuy nhiên, vào năm 1996, Ethernet đã được mở rộng để bao gồm luôn khả năng song công hoàn toàn vào cho phép nhiều hơn một PC có thể truyền đồng thời vào một thời điểm.

Các switch thay thế nhanh chóng các hub. Các switch có khả năng song công hoàn toàn và kiểm soát nhanh các Ethernet frame.

100BASE-TX dùng mã hoá 4B/5B, được xáo trộn và được đổi thành các mức MLT-3 (multilevel transmit-3). 100BASE-TX truyền lưu lượng 100Mbps theo chế độ bán song công. Trong chế độ song công hoàn toàn, 100BASE-TX có thể truyền lưu lượng 200Mbps. Khái niệm song công hoàn toàn sẽ trở nên quan trọng khi tốc độ Ethernet tăng lên.

2. 100BASE-FX

Khi mà Fast Ethernet dựa vào cáp đồng được giới thiệu thì một phiên bản cáp sợi quang cũng đang là điều mong muốn. Một phiên bản sợi quang có thể dùng cho các ứng dụng backbone, các kết nối giữa các tầng và các building, nơi mà cáp đồng không được chuộng và cũng là mong muốn trong các môi trường có tạp âm nặng.

100BASE-FX được giới thiệu nhằm thoả mãn nhu cầu này. Tuy nhiên, 100BASE-FX chưa bao giờ được công nhận là thành công. Đó là lý do mà mới đây xuất hiện các chuẩn Gigabit Ethernet cáp đồng và cáp quang. Các chuẩn Gigabit Ethernet hiện nay đang là một công nghệ chiếm ưu thế trên các lắp đặt mạng đường trục, đấu chéo tốc độ cao và các nhu cầu về hạ tầng chung.

Định thời, định dạng frame và hoạt động truyền là tất cả những gì chung nhất cho cả hai phiên bản 100Mbps Fast Ethernet. 100BASE-FX cũng dùng mã hoá 4B/5B.

Khả năng truyền 200 Mbps là hoàn toàn có thể bởi sự tách biệt giữa đường thu và đường truyền trong 100BASE-FX optical fiber.

Bảng 5.5. Chân tín hiệu 100BASE-FX

Tín hiệu	
1	Tx (LED and laser transmitters)
2	Rx (high-speed photodiode detectors)

Bảng 5.6. Ví dụ về cấu hình kiến trúc và chiều dài cáp

Kiến trúc	100BASE-TX	100BASE-FX	100BASE-TX and FX
Station to Station Station to Switch Switch to Switch (half or full duplex)	100m	412m	N/A
One Class 1 Repeater (half duplex)	200m	272m	100m (TX) 160.8m (FX)
One Class II Repeater (half duplex)	200m	320m	100m (TX) 206m (FX)
Two Class II Repeaters (half duplex)	205m	228m	105m (TX) 211.2m (FX)

5.4.7. GIGABIT ETHERNET

1. 1000-Mbps Ethernet

Chuẩn Gigabit được sử dụng trong môi trường truyền là cáp đồng hoặc cáp quang. Chuẩn 1000BASE-X, IEEE 802.3z, cho biết một hoạt động truyền song công hoàn toàn tốc độ 1Gbps truyền qua cáp sợi quang. Chuẩn 1000BASE-TX, 1000BASE-SX và 1000BASE-LX dùng cùng các thông số định thời, như trình bày trên bảng 5.7. Gigabit Ethernet frame có cùng định dạng với 10 và 100-Mbps Ethernet. Tuỳ vào sự thực hiện, Gigabit Ethernet có thể dùng các quá trình khác nhau để biến đổi frame sang bit. Bảng 5.8 trình bày các định dạng Ethernet frame.

Bảng 5.7. Các thông số hoạt động của Gigabit Ethernet

Thông số	Giá trị
Bit Time	10 nsec
Slot time	4096 bit times
Interframe Spacing	96 bit
Collision Attempt Limit	16
Collision Backoff Limit	10
Collision Jam Size	32 bits
Maximum Untagged Frame Size	1518 octets
Minimum Frame Size	512 bits (64 octets)

Bảng 5.8. Ethernet frame

Ethernet Frame						
Preamble	SFD	Destination	Source	Length Type	Data Pad	FCS
7	1	6	6	2	46 to 1500	4

Sự khác biệt giữa các chuẩn Ethernet, Fast Ethernet và Gigabit Ethernet là ở mức vật lý. Tốc độ gia tăng trong các chuẩn mới này, khoảng thời gian bít ngắn hơn đòi hỏi phải có sự quan tâm đặc biệt. Vì các bit được đưa lên đường truyền trong một khoảng thời gian ngắn và thường xuyên nên định thời là hết sức quan trọng. Hoạt động truyền tốc độ cao yêu cầu các tần số kề cận đế các giới hạn băng thông đường truyền cáp đồng. Điều này khiến cho các bit mềm yếu hơn đối với nhiễu xảy ra trên đường truyền.

Các vấn đề này yêu cầu Gigabit Ethernet dùng hai bước mã hoá riêng biệt. Hoạt động truyền số liệu được làm cho hiệu quả hơn bằng cách dùng các mã để biểu diễn các luồng bit nhị phân. Số liệu được mã hoá cung cấp sự đồng bộ, sử dụng băng thông hiệu quả và cải thiện đặc tính SNR (Signal-to-Noise Ratio). SNR là tỷ số giữa năng lượng tín hiệu và năng lượng nhiễu trên kênh tính bằng Decibel.

2. 1000BASE-T

Khi Fast Ethernet được lắp đặt để tăng cường băng thông cho các workstation, điều này bắt đầu tạo ra các "cổ chai" trong các luồng số liệu hướng lên mạng. 1000BASE-T (IEEE 502.3ab) đã được phát triển để cung cấp thêm băng thông giúp xoá bỏ các "cổ chai" này. Fast Ethernet được thiết kế để hoạt động qua cáp UTP Cat 5 và điều này đòi hỏi cáp phải qua được phép thử Cat 5e (1000BASE-T và Cat 6). Một trong các thuộc tính quan trọng nhất của chuẩn 1000BASE-T là nó có thể liên kết hoạt động với 10BASE-T và 100BASE-TX.

Vì cáp Cat 5e có thể truyền tải một cách tin cậy đến lưu lượng 125 Mbps, nên để đạt được băng thông 1000Mbps là một thách thức đối với thiết kế. Bước đầu tiên để tạo dựng 1000BASE-T là dùng tất cả bốn đôi dây thay vì hai đôi theo truyền thống trong 10BASE-T hay 100BASE-TX. Điều này được thực hiện bằng các mạch phức tạp để cho phép hoạt động truyền song công hoàn toàn trên cùng một đôi dây. Điều này cung cấp 250Mbps trên một đôi. Với tất cả bốn đôi dây ta có 1000Mbps. Vì thông tin di chuyển một cách đồng thời xuyên qua bốn đường dẫn, nên tại máy phát mạch này phải chia các frame ra và tại máy thu sẽ tái nhập trở lại.

3. 1000BASE-SX và LX

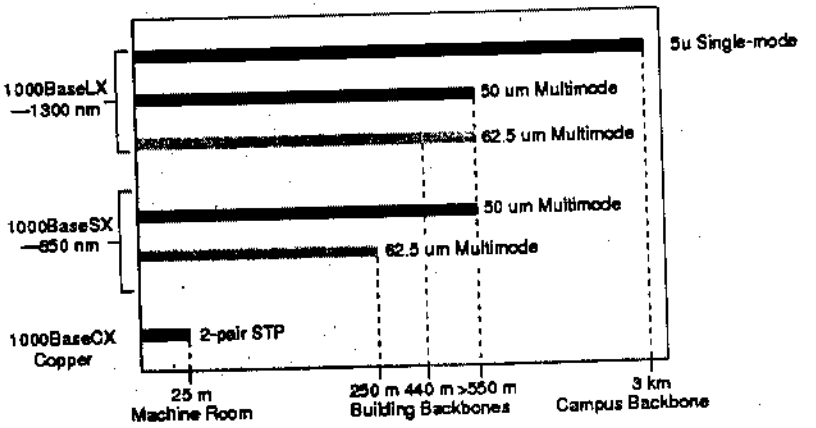
Chuẩn IEEE 802.3 cho rằng Gigabit Ethernet chạy trên cáp sợi quang là công nghệ thích hợp cho backbone. Định dạng frame và hoạt động truyền là giống nhau đối với tất cả các phiên bản của 1000 Mbps. Hai lược đồ mã hoá tín hiệu được được định nghĩa tại lớp vật lý. Lược đồ 8B/10B được dùng cho sợi quang cáp và đồng được bảo vệ và PAM 5 được dùng cho UTP.

1000BASE-X dùng 8B/10B biến đổi sang mã hoá đường dây NRZ. Mã hoá NRZ dựa vào mức tín hiệu được phát hiện trên cửa sổ định thời để xác định giá trị nhị phân cho thời bit này. Không giống như hầu hết các lược đồ mã hoá đã được mô tả, lược đồ mã hoá này điều khiển theo mức chứ không phải theo sự chuyển mức. Có nghĩa là sự xác định một bit là 0 hay 1 căn cứ vào mức điện áp nhận biết vào thời điểm lấy mẫu.

Các tín hiệu NRZ được phát dưới dạng xung vào cáp sợi quang sử dụng các nguồn phát song có bước sóng ngắn hay dài. Bước sóng ngắn dùng laser 850 nm hay LED với sợi đa mode (100BASE-SX). Nó có giá thành thấp nhưng cự ly truyền ngắn hơn. Laser 1310 nm với bước sóng dài dùng sợi đơn mode hoặc đa mode (1000 BASE-LX). Nguồn laser dùng với sợi đơn mode có thể đạt khoảng cách truyền đến 5000 mét. Laser và LED đều hoàn thành một lượt đóng mở theo các khoảng thời gian nên ánh sáng phát ra

theo dạng xung dùng công suất thấp hay cao. Giá trị 0 luận lý được biểu diễn bởi mức công suất và giá trị 1 được biểu diễn bởi công suất cao hơn.

Phương pháp điều khiển truy nhập môi trường (Media Access Control) xem liên kết như là điểm nối điểm. Vì các sợi quang tách biệt được dùng cho truyền và nhận nên liên kết nối vốn là song công hoàn toàn. Gigabit Ethernet chỉ cho phép một repeater giữa hai trạm. Hình 5.9 là một đồ thị so sánh các đường truyền cho 1000BASE Ethernet.



Hình 5.9. So sánh các đường truyền Gigabit Ethernet.

5.5. TOKEN RING

IBM phát triển mạng Token Ring đầu tiên vào những năm 1970, hiện nay là kỹ thuật LAN chủ yếu của IBM, và đứng sau Ethernet IEEE 802.3. IEEE 802.5 là chuẩn cho các kỹ thuật mạng cùng dạng hay tương thích với mạng Token Ring của IBM.

5.5.1. KHUÔN DẠNG CỦA TOKEN RING

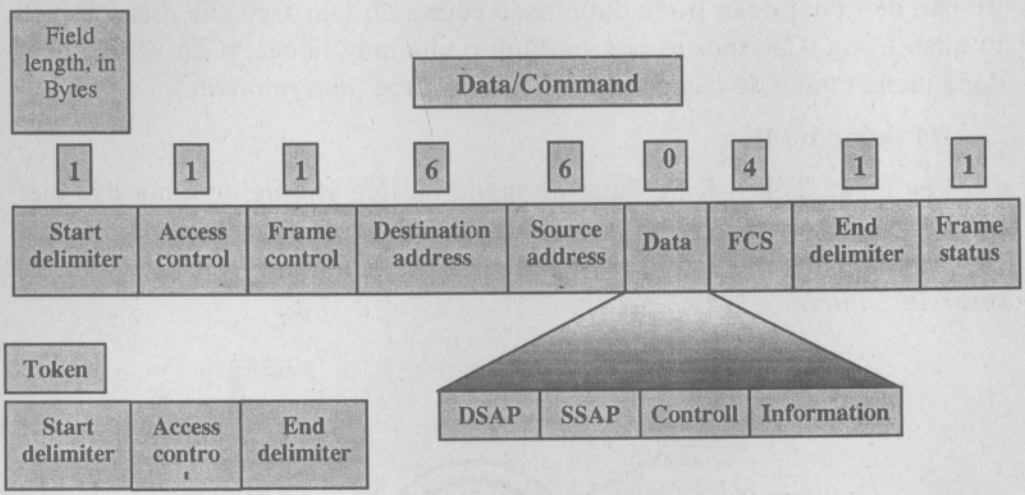
1. Các Token

Các token chiều dài 3 byte, gồm một byte xác định ranh giới đầu *start delimiter*, một byte điều khiển truy xuất *access control* và một byte xác định ranh giới cuối *end delimiter*. Start delimiter báo động cho mỗi trạm là có token đến hay có một frame đến.

2. Byte điều khiển truy xuất (*Access Control Byte*)

Byte điều khiển truy xuất chứa trường ưu tiên (*priority field*), field giữ chỗ (*reservation field*), token bit và bit giám sát (*monitor bit*). Token bit dùng để phân biệt một frame là token hay frame dữ liệu (hay frame lệnh), bit giám sát xác định một frame có tiếp tục chạy trên mạch vòng hay không.

End delimiter là dấu hiệu kết thúc một token hay một frame thường, chứa các bit mà nội dung có thể nói lên được frame bị hỏng, một frame là cuối cùng của một tuần tự logic nào đó.



***Hình 5.10**. Khuôn dạng của Token Ring.*

5.5.2. TOKEN RING MAC

Token Ring và IEEE 802.5 là các ví dụ tiêu biểu của các mạng chuyển token. Một frame nhỏ chạy xung quanh mạng được gọi là token. Sự sở hữu token đồng nghĩa với được gán quyền truyền dữ liệu. Nếu một node nào đó nhận token mà không có thông tin để truyền, nó chuyển token đến trạm cuối kế tiếp. Mỗi trạm có thể giữ token trong một khoảng thời gian tối đa tùy vào đặc tả của kỹ thuật được triển khai.

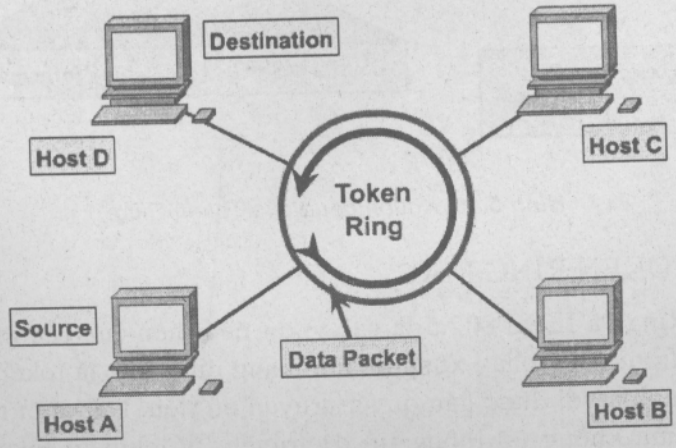
Khi token được chuyển tới host có thông tin cần truyền, host bắt lấy token và thay đổi token bit của nó. Lúc này, token trở thành một tuần tự đánh dấu đầu frame. Kế tiếp host gắn tiếp các thông tin muốn truyền vào token và truyền frame mới này đến trạm kế trên vòng. Không có token trên vòng trong khi frame dữ liệu chạy vòng trên ring, trừ khi ring có hỗ trợ giải phóng token sớm. Các trạm khác trên mạch vòng không thể truyền dữ liệu tại thời điểm này mà phải đợi token trở nên sẵn sàng. Các mạng Token Ring không xảy ra đụng độ.

Frame thông tin chạy vòng trên mạch vòng cho đến khi đạt đến trạm đích mà nó hướng tới, trạm đích sẽ chép thông tin để xử lý. Frame thông tin sẽ tiếp tục chạy về trạm nguồn, tại đây nó sẽ bị loại bỏ. Trạm nguồn hoàn toàn có thể xác định được frame đã được tiếp nhận và được chép bởi trạm đích hay chưa.

Không giống như các mạng CSMA/CD hay Ethernet, các mạng chuyển token là đoán trước được. Điều này có nghĩa là có thể tính toán được thời gian tối đa sẽ chuyển trước khi một trạm bất kỳ nào có thể truyền, nên mạng Token Ring lý tưởng cho các ứng dụng mà yêu cầu bất kỳ thời gian trễ nào đều phải đoán trước được hoặc cường độ làm việc của mạng là yếu tố quan trọng. Các môi trường tự động ở nhà máy là các ví dụ về các hoạt động mạng cường độ cao có thể đoán trước được (*deterministic*).

Hệ thống ưu tiên

Các mạng Token Ring dùng hệ thống ưu tiêu cho người dùng đặc biệt nào đó, các trạm có ưu tiên cao sẽ dùng mạng thường xuyên hơn. Các frame của Token Ring có hai field để điều khiển ưu tiên: *priority field* và *reservation field*.



Hình 5.11. Token Ring.

Chỉ các trạm có mức ưu tiên ngang bằng hay lớn hơn giá trị ưu tiên chứa trong token mới có thể bắt token. Khi token đã được bắt lấy và thay đổi để trở thành một frame thông tin, chỉ các trạm với giá trị ưu tiên cao hơn giá trị ưu tiên của trạm đang truyền mới có thể đăng ký giữ chỗ cho lần chuyển kế. Token kế tiếp được phát ra bao gồm giá trị ưu tiên mức cao của trạm đăng ký. Các trạm gia tăng mức ưu tiên của token phải phục hồi mức ưu tiên ban đầu khi hoạt động truyền của chúng hoàn tất.

5.5.3. TRUYỀN TÍN HIỆU TRÊN TOKEN RING

Mã hoá tín hiệu là một phương pháp tổ hợp cả thông tin của đồng hồ và dữ liệu vào trong một luồng tín hiệu truyền qua môi trường. Các mạng Token Ring 4/16Mbps dùng mã hóa Manchester vi phân.

- Không có cực tính tại đầu của thời bit: 1

- Thay đổi cực tính tại đầu của thời bit: 0

5.6. FDDI

FDDI (Fiber Distributed Data Interface - Giao diện dữ liệu phân tán sợi quang) là công nghệ mạng tốc độ cao do uỷ ban X3T9.5 của ANSI (American National Standards Institute) phát triển vào giữa những năm 1980. Ban đầu được thiết kế cho cáp quang (FDDI) nhưng ngày nay nó cũng hỗ cáp đồng với khoảng cách ngắn hơn (CDDI). Chuẩn này được phổ biến trong mạng LAN. FDDI có tốc độ dữ liệu 100Mbps và dùng đồ hình vòng kép dự phòng, hỗ trợ 500 trạm với khoảng cách cực đại 100km. Với khoảng cách này FDDI cũng được dùng cho mạng MAN.

FDDI được dùng rộng rãi cho đồ hình đường trục. Các phân đoạn LAN nối vào đường trục này, cùng với các máy mini, mainframe và các hệ thống khác. Các mạng nhỏ với ít thành phần LAN có thể dùng đường trục Ethernet để tiết kiệm chi phí. Các mạng lớn nhiều thành phần LAN và có lượng lưu thông lớn thì nên sử dụng FDDI. Để ý rằng Ethernet tốc độ cao như Fast Ethernet và 100VG-AnyLAN có thể cung cấp cùng chức năng như FDDI, nhưng do giới hạn về khoảng cách nên chúng không thích hợp với các đường trục dùng trong phạm vi lãnh thổ rộng lớn.

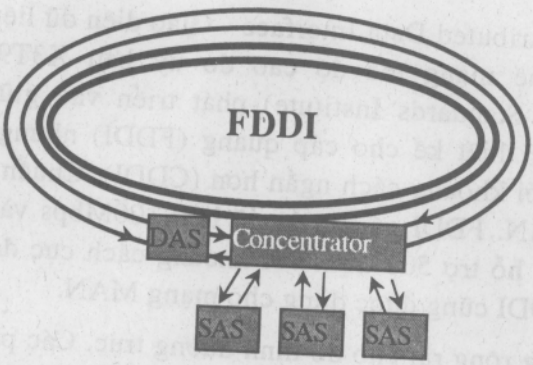
5.6.1. ĐỊNH CẤU HÌNH FDDI

Chiều dài lớn nhất của ring là 100km. Khoảng cách lớn nhất giữa các trạm kề nhau là 2km. Về mặt vật lý là một ring nhiều cây, nhưng về mặt logic, toàn bộ mạng tạo nên một vòng của các kết nối điểm - điểm giữa các trạm kề nhau. Hai ring FDDI có tên là ring sơ cấp và ring thứ cấp. Có thể dùng cả hai ring để truyền dẫn hoặc chỉ dùng một còn một dự phòng trong trường hợp vòng sơ cấp có sự cố.

Trong cấu hình ring đôi (*dual-ring configuration*), tải trên mỗi ring di chuyển theo hai chiều ngược nhau. Có ba loại thiết bị có thể kết nối vào ring:

- Class A, hay DAS (*dual-attachment station*): gắn vào cả hai ring, chẳng hạn máy chủ giải quyết trường hợp khẩn cấp và các thiết bị đi kèm.
- DAC (*dual-attachment concentrator*): nối vào cả hai ring và cung cấp điểm kết nối cho các máy trạm.
- Class B, hay SAS (*single-attachment station*): nối vào ring sơ cấp thông qua bộ tập trung concentrator.

Bộ tập trung đảm bảo rằng một lỗi, hay sự tắt nguồn của bất kỳ một SAS nào không ngắt được ring. Điều này đặc biệt hữu dụng khi các PC, hay các thiết bị tương tự gắn vào ring mà đóng ngắt nguồn thường xuyên.



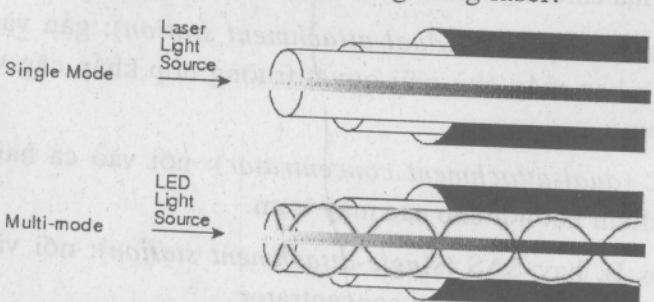
Hình 5.12. Các node FDDI: DAS, SAS, Concentrator.

5.6.2. MÔI TRƯỜNG FDDI

Đặc trưng riêng của FDDI là truyền bằng sợi quang, so với dây đồng có ưu điểm:

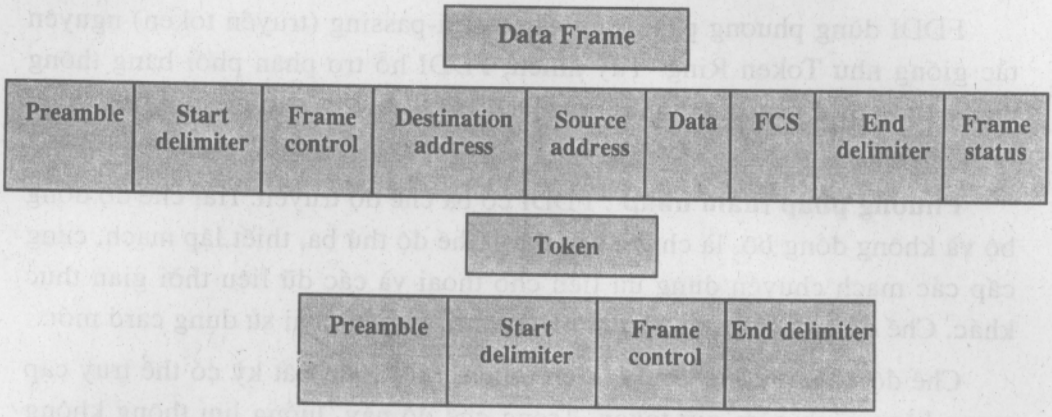
- Bảo mật: không phát các tín hiệu điện nên không thể mắc rẽ một cách đơn giản.
- Tin cậy: loại bỏ được các xuyên nhiễu điện.
- Tốc độ: thông lượng cao hơn.

Sợi quang truyền đơn mode và đa mode. Các mode truyền xem như các chùm tia sáng đi vào sợi theo các góc tới khác nhau, đường đi khác nhau làm cho chúng đến đích tại các thời điểm khác nhau gây ra hiện tượng tán sắc mode. Sợi đơn mode băng thông cao hơn, cự ly chạy cable xa hơn sợi đa mode nên thường dùng kết nối giữa các tòa nhà (*inter-building*). Sợi đa mode dùng trong một toà nhà (*intra-building*). Sợi đa mode dùng các LED làm thiết bị phát quang, sợi đơn mode thường dùng laser.



Hình 5.13. Các nguồn sáng khác nhau đối với cáp quang đơn và đa mode.

5.6.3. KHUÔN DẠNG CỦA FDDI FRAME



Hình 5.14. Khuôn dạng của FDDI.

- **Preamble:** chuẩn bị frame truyền đi tại mỗi trạm.
- **Start delimiter:** chỉ ra vị trí bắt đầu của frame, và bao gồm các mẫu dấu hiệu phân biệt nó với phần còn lại của frame.
- **Frame control:** chỉ ra kích thước của trường địa chỉ, frame chứa dữ liệu đồng bộ hay bất đồng bộ và các thông tin điều khiển khác.
- **Destination address:** chứa địa chỉ đơn, nhóm hay quảng bá, 6 byte (giống Ethernet và Token Ring).
- **Source address:** chỉ ra trạm truyền frame, 6 byte (giống Ethernet, Token Ring).
- **Data:** thông tin điều khiển hay thông tin dành riêng cho một giao thức mức cao.
- **Frame check sequence:** được làm đầy bởi trạm nguồn bằng cách tính toán CRC, giá trị phụ thuộc vào nội dung frame. Trạm đích tính toán trở lại giá trị này căn cứ vào thông tin trên frame nhận được và so sánh với giá trị cũ để xác định xem frame có bị hỏng trong khi chuyển hay không, nếu hỏng frame sẽ bị hủy bỏ.
- **End delimiter:** chỉ ra vị trí kết thúc frame.
- **Frame status:** cho phép trạm nguồn xác định xem có lỗi xảy ra hay không và frame có được chấp nhận và sao chép bởi một trạm đích hay không.

5.6.4. FDDI MAC

FDDI dùng phương pháp truy cập token-passing (truyền token) nguyên tắc giống như Token Ring. Tuy nhiên, FDDI hỗ trợ phân phối băng thông mạng theo thời gian thực, nhờ đó FDDI rất lý tưởng cho một số ứng dụng khác nhau.

Phương pháp thâm nhập : FDDI có ba chế độ truyền. Hai chế độ đồng bộ và không đồng bộ, là chuẩn ban đầu. Chế độ thứ ba, thiết lập mạch, cung cấp các mạch chuyên dụng ưu tiên cho thoại và các dữ liệu thời gian thực khác. Chế độ này có trong chuẩn FDDI mới, và cần phải sử dụng card mới.

Chế độ không đồng bộ dựa trên token. Một trạm bất kỳ có thể truy cập mạng bằng cách nắm giữ token. Trong chế độ này, luồng lưu thông không có độ ưu tiên. Thông tin thuộc loại không nhạy về thời gian, gọi là các khung A (*asynchronous*).

Chế độ chuyển token đồng bộ cho phép ưu tiên. Các card FDDI với khả năng đồng bộ cho phép dành riêng một phần băng thông cho các luồng thông tin nhạy bén về thời gian (âm thanh và ảnh động). Các trạm không đồng bộ sẽ chia nhau phần còn lại. Khả năng đồng bộ được bổ sung bằng cách nâng cấp phần mềm.

5.6.5. TRUYỀN TÍN HIỆU TRÊN FDDI

Dùng cơ cấu mã 4B/5B. Mỗi đoạn dữ liệu 4 bit được thay thế bằng mã 5 bit trước khi mã NRZ-I. Sở dĩ phải thêm một bit vì trong mã NRZ-I nếu chuỗi liên tiếp các "0" kéo dài có thể bị mất đồng bộ, 4B/5B cho thấy trong một đoạn không có quá 2 bit "0" liên tiếp.

5.6.6. FDDI-II

FDDI-II được thiết kế cho các mạng cần chuyển tải dữ liệu thời gian thực. Đây là một cải tiến của FDDI nhằm hỗ trợ dữ liệu đồng bộ như thoại và lưu thông ISDN. FDDI- II đòi hỏi tất cả các nút mạng phải sử dụng FDDI-II; nếu không mạng sẽ chuyển đổi về FDDI. Các trạm FDDI sẵn có cần được tách ra thành mạng riêng.

FDDI-II dùng kỹ thuật đa hợp (*multiplexing*) để chia băng thông thành 16 mạch chuyên dụng giúp chuyển tải đúng giờ đối với các luồng lưu thông được ưu tiên. Các mạch này có tốc độ từ 6.144Mbps đến 99.072Mbps. Lý do khác biệt là băng thông được cấp phát cho bất kỳ

trạm nào có độ ưu tiên cao nhất. Mỗi kênh có thể chia nhỏ để tạo nên tổng cộng 96 mạch 64Kbps.

Các kênh này có thể hỗ trợ luồng không đồng bộ hoặc đẳng thời. Các khe thời gian được cấp phát để truyền dữ liệu. Các trạm có ưu tiên sử dụng một số khe này để chuyển tải dữ liệu đúng giờ. Nếu có các khe không sử dụng, chúng được cấp phát tức thời cho các trạm khác.

FDDI-II chưa trở thành công nghệ được sử dụng rộng rãi vì nó không tương thích thiết kế FDDI hiện hành. Một lý do khác là Ethernet 100Mbps và ATM cung cấp giải pháp tốt hơn trong đa số các trường hợp.

Chương 6

INTERNET

6.1. INTERNET VỚI MÔ HÌNH THAM CHIẾU TCP/IP

6.1.1. GIỚI THIỆU INTERNET

Internet là một hệ thống gồm các mạng máy tính được liên kết với nhau trên phạm vi toàn thế giới, tạo điều kiện thuận lợi cho các dịch vụ truyền thông dữ liệu, như đăng nhập từ xa, truyền tệp tin, thư tín điện tử và các nhóm thông tin. Internet là một phương pháp ghép nối các máy tính, phát triển rộng rãi tầm hoạt động của từng hệ thống thành viên.

Nguồn gốc Internet là hệ thống máy tính của Bộ Quốc phòng Mỹ, mạng ARPAnet, một mạng thí nghiệm được thiết kế từ năm 1969 để tạo điều kiện thuận lợi cho việc hợp tác hóa khoa học các công trình nghiên cứu quốc phòng. ARPAnet đã nêu cao triết lý truyền thông bình đẳng (*peer-to-peer*), trong đó mỗi máy tính của hệ thống đều có khả năng nói chuyện với bất kỳ máy tính thành viên nào khác.

Mặc dù mô hình OSI được chấp nhận rộng rãi khắp nơi, nhưng chuẩn mở về kỹ thuật mạng mang tính lịch sử của Internet lại là TCP/IP (*Transmission Control Protocol / Internet Protocol*). Mô hình và các giao thức TCP/IP tạo khả năng truyền dữ liệu giữa hai máy tính bất cứ nơi nào trên thế giới, tốc độ gần bằng tốc độ ánh sáng.

Mạng Internet kết nối các máy tính không phân biệt đẳng cấp và không có hệ điều hành trung tâm của mạng. Internet tạo ra một cộng đồng bình đẳng của những người sử dụng. Mọi người tham gia vào Internet đều có thể gửi đi, nhận lại và tìm kiếm tất cả những gì họ muốn. Internet hoạt động liên tục suốt ngày đêm, nhưng không một ai thực sự "chạy" Internet, cũng chẳng có ai chịu trách nhiệm và không có một cơ quan, tổ chức nào quản lý và trả chi phí cho Internet.

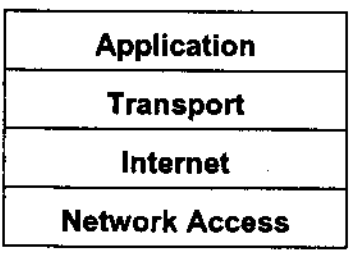
Tổ chức có vai trò điều phối tối cao các hoạt động của Internet là Hiệp hội Internet ISOC. Đây là tổ chức phi lợi nhuận, tập hợp các cá nhân và tổ chức tự nguyện tham gia, hoạt động nhằm khuyến khích và phát triển sử dụng Internet trên toàn thế giới. Cơ quan lãnh đạo cao nhất của ISOC là Ban kiến trúc Internet (Internet architecturre board-IAB). IAB xem xét các

chuẩn liên quan và các quy định cấp phát tài nguyên. Tiểu ban đặc nhiệm kỹ thuật Internet (Internet engineering task force-IETF) của IAB giải quyết các vấn đề hệ trọng về kỹ thuật.

Từ năm 1992, do nhu cầu tăng nhanh của Internet, việc cấp phát địa chỉ cho máy tính của người sử dụng (host) được phân cấp cho các trung tâm thông tin mạng (Network information center-NIC) của các khu vực đảm nhận. Ở hai khu vực châu Á- Thái Bình Dương, hiện mới có hai NIC quốc gia của Nhật Bản và Hàn Quốc. Hiện tại APNIC vẫn chịu trách nhiệm điều hành và phân phối địa chỉ cho các host ở Việt Nam.

6.1.2. CÁC LỚP CỦA MÔ HÌNH TCP/IP VÀ SƠ ĐỒ GIAO THỨC TCP/IP

Cấu trúc một mạng Internet (mô hình TCP/IP) gồm bốn lớp (hình 6.1) và sơ đồ giao thức TCP/IP (hình 6.2).



Hình 6.1. Mô hình TCP/IP

1. Lớp ứng dụng: Các vấn đề liên quan đến ứng dụng vào một lớp, như kiểm soát các giao thức mức cao, các vấn đề của lớp trình bày, mã hóa và điều khiển hội thoại. Lớp này đảm bảo dữ liệu được đóng gói thích hợp cho lớp kế tiếp.

Một số ứng dụng phổ biến của tầng ứng dụng:

Trong TCP/IP, ở trên tầng giao vận là tầng ứng dụng và tầng này chứa một số lớn các ứng dụng, cụ thể là:

- X: đây là một hệ thống cửa sổ có thể thực hiện trong môi trường multivendor

- TELNET: cung cấp dịch vụ truy nhập từ xa

- FTP (File transfer protocol- giao thức truyền tệp): cung cấp khả năng truyền tệp giữa các hệ thống

- SMTP (Simple mail transfer protocol- giao thức truyền thư điện tử đơn giản): cung cấp dịch vụ thư tín điện tử (e-mail) cho người sử dụng.

- DNS (Domain name service): dịch vụ tên miền được thiết kế để giải quyết vấn đề địa chỉ đến trong mạng TCP/IP. Đây là một phương pháp đã được tự động hoá để nhằm cung cấp địa chỉ của mạng mà không cần phải cập nhật các bảng host một cách thủ công.

- TFTP (Trivial file transfer protocol): ứng dụng của giao thức UDP này được sử dụng hiệu quả nhất trong quá trình khởi động các thiết bị mạng. TFTP chỉ là một giao thức truyền tệp tin đơn giản sử dụng UDP nên nó rất thích hợp cho việc tải xuống các phần mềm vào các thiết bị mạng trong quá trình khởi động.

- SNMP (Simple network management protocol- giao thức quản lý mạng đơn giản): phần lớn các mạng TCP/IP được quản lý theo kiểu SNMP. SNMP được sắp đặt dựa trên cơ sở "nhân viên và quản trị". Cụ thể là "nhân viên" thu thập thông tin về các host (mỗi thiết bị chạy một chương trình con thu thập thông tin) sau đó cung cấp các thông tin này cho bộ phận quản lý. Bộ phận quản lý sẽ bảo quản và lưu giữ các thông tin thu được về các host tham gia vào mạng.

- NFS (Network file server- hệ thống tập tin mạng): đây là hệ thống dịch vụ phân phối và cung cấp các tập tin dùng chung cho môi trường mạng. Nhờ NFS mà các thư mục chung không thực sự tồn tại trên máy trạm thành viên của mạng, sẽ xuất hiện như là một phần của hệ thống thư mục của máy trạm này.

- RPC (Remote procedure call- gọi thủ tục từ xa): giao thức này cho phép gọi và chạy các chương trình trên một server.

- Custom applications (các ứng dụng của người sử dụng): người sử dụng có thể viết, lập trình các ứng dụng của riêng mình sử dụng giao thức UDP tương tự như một giao thức tầng giao vận. Nếu được thực hiện, các đối thoại đồng đẳng ngang hàng giữa các ứng dụng sẽ có thể đạt được.

2. Lớp vận chuyển: Các vấn đề chất lượng dịch vụ như độ tin cậy, điều khiển luồng và sửa lỗi. Một trong các giao thức là TCP, cung cấp các phương thức linh hoạt và hiệu quả để thực hiện việc truyền dữ liệu tin cậy, hiệu suất cao và ít lỗi. TCP là giao thức có tạo cầu nối (*connection-oriented*). Nó tiến hành hội thoại giữa nguồn và đích trong khi bọc thông tin lớp ứng dụng thành các đơn vị gọi là các segment. Tạo cầu nối không có nghĩa là tồn tại một mạch thực sự giữa hai máy tính, mà là các segment của lớp 4 di chuyển tới và lui giữa hai host để công nhận kết nối tồn tại một cách logic trong một khoảng thời gian nào đó, coi như là chuyển mạch gói (*packet switching*).

Giao thức UDP cũng được sử dụng ở lớp này nhưng có độ tin cậy không cao, không thể tái truyền phát thông tin như TCP/IP.

3. Lớp Internet: Mục tiêu là truyền các gói bất nguồn từ bất kỳ mạng nào trên liên mạng đến đích trong điều kiện độc lập với đường dẫn và các mạng mà chúng trải qua. Giao thức đặc trưng là IP. Công việc xác định đường dẫn tốt nhất và hoạt động chuyển mạch gói diễn ra tại lớp này.

Lớp mạng của TCP/IP gồm có các thành phần sau:

- Internet Protocol (IP): IP có một cơ cấu đánh địa chỉ được dùng để xác định host và network. IP tham gia vào chức năng định tuyến.

- Internet Control message protocol (ICMP): ICMP là một thành phần cần thiết trong TCP/IP. Nó chịu trách nhiệm gửi đi các thông điệp (message) qua mạng nhờ IP header

- Address resolution protocol (ARP-giao thức giải pháp địa chỉ). ARP dịch địa chỉ IP sang địa chỉ vật lý (card ghép nối phần cứng)

- Reserve address resolution protocol (RARP- giao thức giải pháp địa chỉ đảo): RARP cho phép máy tính nhận được địa chỉ IP của nó bằng cách thông báo địa chỉ vật lý của chính mình. Thông thường một server RARP được lựa chọn và đáp ứng yêu cầu địa chỉ IP này.

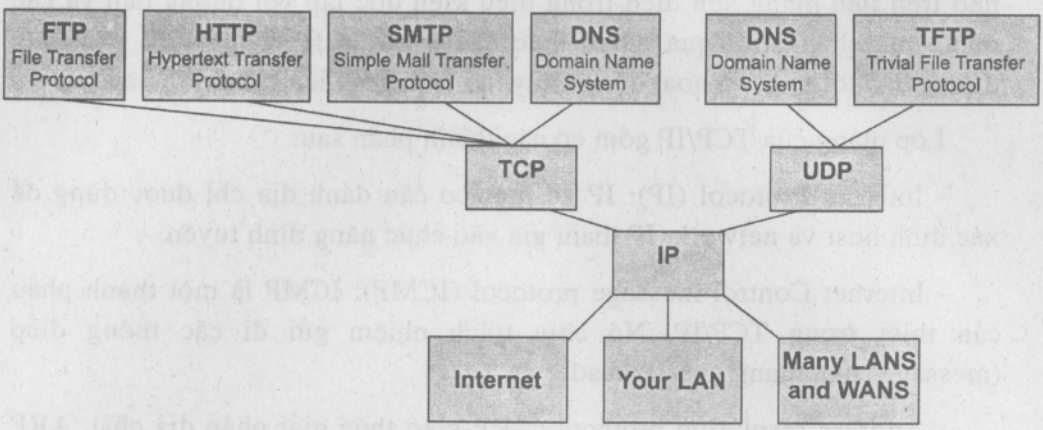
- Routing information protocol (RIP- giao thức thông tin định tuyến): RIP là một giao thức định tuyến được sử dụng ở tầng mạng. Nó thực hiện việc định tuyến các gói tin.

- Open shortest path first (OSPF): OSPF cũng là một giao thức định tuyến được tiến hành ở tầng mạng như RIP. Tuy nhiên giao thức này sử dụng hiểu biết về cấu trúc mạng Internet để định tuyến các thông điệp theo tuyến nhanh nhất.

4. Lớp truy xuất mạng: Liên quan đến các vấn đề mà một gói IP yêu cầu để tạo một liên kết vật lý thực sự. Nó bao gồm các chi tiết kỹ thuật LAN và WAN, và tất cả các chi tiết trong lớp liên kết dữ liệu cũng như lớp vật lý của mô hình OSI.

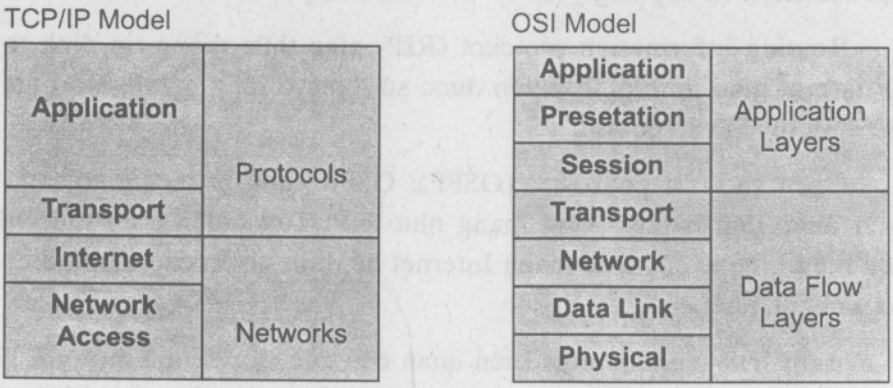
Mô hình TCP/IP hướng đến tối đa độ linh hoạt tại lớp ứng dụng cho người phát triển phần mềm. Lớp vận chuyển liên quan đến hai giao thức TCP và UDP (*user datagram ptotocol*). Lớp cuối cùng, lớp truy xuất mạng liên quan đến các kỹ thuật LAN hay WAN đang được dùng. Trong mô hình TCP/IP không cần quan tâm đến ứng dụng nào yêu cầu các dịch vụ mạng,

và không cần quan tâm đến giao thức vận chuyển nào đang được dùng, chỉ có một giao thức mạng IP phục vụ như một giao thức đa năng cho phép bất kỳ máy tính nào, ở bất cứ đâu, truyền dữ liệu vào bất cứ thời điểm nào.



***Hình 6.2**. Sơ đồ giao thức TCP/IP*

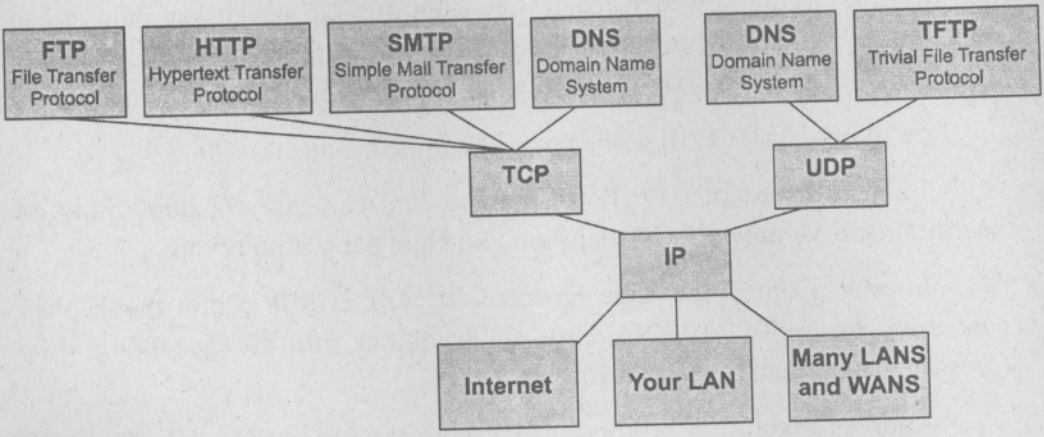
6.1.3. SO SÁNH MÔ HÌNH OSI VÀ MÔ HÌNH TCP/IP



***Hình 6.3.** So sánh TCP/IP với OSI*

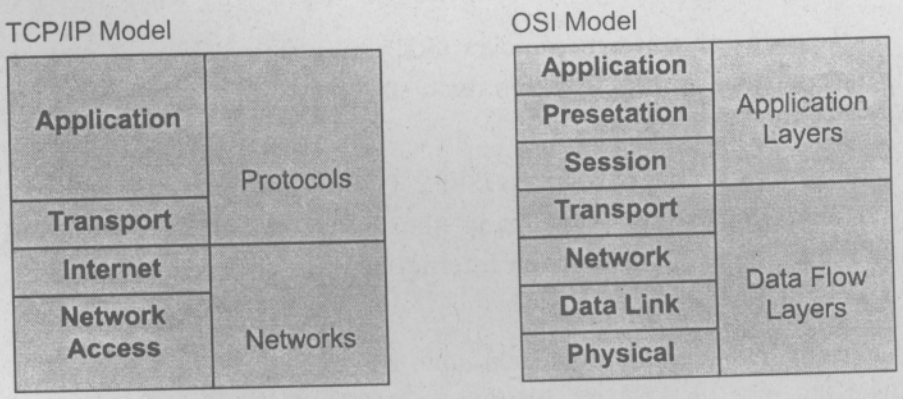
Các mạng thông thường không được xây dựng dựa trên giao thức OSI, ngay cả khi OSI được dùng như một hướng dẫn. Nói cách khác, nó là một văn phạm nghèo và có thiếu sót. Nhiều chuyên viên lập mạng có các quan điểm khác nhau nên sử dụng mô hình nào. Nói chung, nên dùng OSI như một kính hiển vi trong khi phân tích mạng, nhưng các giao thức lại là TCP/IP.

và không cần quan tâm đến giao thức vận chuyển nào đang được dùng, chỉ có một giao thức mạng IP phục vụ như một giao thức đa năng cho phép bất kỳ máy tính nào, ở bất cứ đâu, truyền dữ liệu vào bất cứ thời điểm nào.



Hình 6.2. *Sơ đồ giao thức TCP/IP*

6.1.3. SO SÁNH MÔ HÌNH OSI VÀ MÔ HÌNH TCP/IP



Hình 6.3. *So sánh TCP/IP với OSI*

Các mạng thông thường không được xây dựng dựa trên giao thức OSI, ngay cả khi OSI được dùng như một hướng dẫn. Nói cách khác, nó là một văn phạm nghèo và có thiếu sót. Nhiều chuyên viên lập mạng có các quan điểm khác nhau nên sử dụng mô hình nào. Nói chung, nên dùng OSI như một kính hiển vi trong khi phân tích mạng, nhưng các giao thức lại là TCP/IP.

OSI Model

7	Application	FTP, TFTP, HTTP, SMTP, DNS, TELNET
6	Presetation	Very little focus
5	Session	
4	Transport	TCP (the Internet)
3	Network	IP (the Internet)
2	Data Link	Ethernet
1	Physical	

Hình 6.4. Tương quan mô hình OSI và giao thức TCP/IP

Để quản lý mạng, Internet thường dùng một số địa chỉ sau:

- IP hAddress: gồm bốn byte, cách nhau bằng dấu chấm. Thông thường, số hiệu mạng và số hiệu máy được dùng để đơn giản việc chọn đường. Khi một byte không đủ để phân biệt các số hiệu mạng, người ta dùng phân lớp địa chỉ.

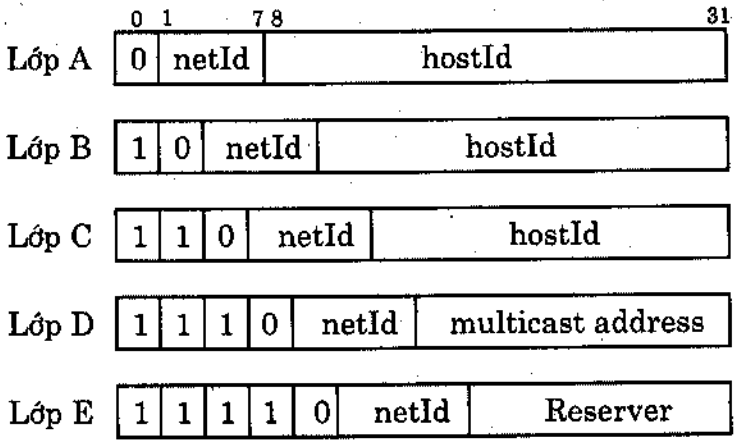
- Name Address: để quản lý tên cần dùng hệ thống quản lý tên vùng NDS (*Domain Name System*), là cơ sở dữ liệu được duy trì bởi nhiều tổ chức, mỗi tổ chức chỉ quản lý một phần theo cấu trúc phân cấp hay cấu trúc cây.

- Email Address: là địa chỉ theo hộp thư điện tử, trong đó phải có ký hiệu @.

IP address

IP là một giao thức kiểu "không liên kết" (connectionless), có nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu. Đơn vị dữ liệu dùng trong IP được gọi là Datagram.

Sơ đồ địa chỉ hóa để định danh các host trong liên mạng. Mỗi địa chỉ IP có độ dài 32 bít được tách thành 4 vùng (mỗi vùng 1 byte), có thể biểu hiện dưới dạng thập phân, thập lục phân, nhị phân. Cách viết phổ biến nhất là dùng 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 host 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, E với cấu trúc chỉ định ra trên hình 6.5.



netId : Network Identifier
hostId: Host Identifier

***Hình 6.5.** Các lớp của mô hình IP*

Các bít đầu tiên được dùng để định danh lớp địa chỉ:

0 - lớp A
10 - lớp B
110 - lớp C
1110 - lớp D
11110 - lớp E

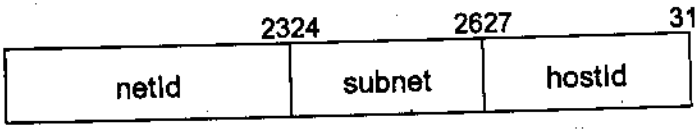
- Lớp A: cho phép định danh 126 mạng với tối đa 16 triệu host / mạng
- Lớp A được dùng cho các mạng có số trạm cực lớn
- Lớp B: định danh 16384 mạng với tối đa 65534 host / mạng
- Lớp C: định danh 2 triệu mạng với tối đa 254 trạm / mạng

được dùng cho mạng ít trạm

- Lớp D: dùng để gửi IP datagram tới một nhóm các host trên một mạng
- Lớp E: dự phòng cho tương lai

Một địa chỉ host = 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 gồm toàn số "1" thì nó hướng tới tất cả các host trong liên mạng.

Trong nhiều trường hợp một mạng có thể chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnet được lấy từ vùng hostid, cụ thể với:



Hình 6.6. Mô hình có subnet

6.1.4. ROUTER PROTOCOL

Mục này tập trung trình bày hai giao thức router thông dụng là giao thức thông tin định tuyến (RIP) và giao thức OSPF. Các giao thức này được sử dụng bởi các thiết bị mạng như router, host và các thiết bị khác thông thường được cài đặt TCP/IP software. Tuy nhiên, các giao thức này cũng hoàn toàn có thể cài đặt và thực hiện bởi firmware.

*Router Information Protocol (RIP)

RIP có nguồn gốc từ tập các giao thức hệ thống mạng của Xerox. Nó cũng đã từng nằm trong phần mềm của TCP/IP phân phối cùng với UCB UNI. Giao thức RIP là một ví dụ điển hình của loại giao thức không chính thức. Nó đã được sử dụng trước khi một RFC tiêu chuẩn ra đời. Giao thức này là một phần của TCP/IP và có tất cả các điều kiện cần thiết để trở thành một sản phẩm thông dụng: nó hoạt động và thực sự được cần đến. RFC 1058 đã làm cho RIP trở thành một chuẩn chính thức.

+ Phân tích header của RIP

Xét ví dụ về dạng của thông điệp RIP, các phần của thông điệp này sẽ được mô tả ngắn gọn dưới đây:

Command: Xác định xem hành động là một yêu cầu hay là một đáp ứng

Version: Xác định phiên bản của giao thức.

Zero: Là một vùng bỏ trống.

Address family identifier: Được dùng để nhận dạng họ giao thức.

Zero: Vùng bỏ trống.

IP address: Thông thường luôn có một router mặc định gắn liền với địa chỉ IP này.

Zero: Bỏ trống.

Zero: Bỏ trống.

Distance to net: Cho biết khoảng cách đến mạng đích.

Các thông điệp RIP hoặc là yêu cầu hoặc là thông báo các thông tin về định tuyến. RIP dựa trên công nghệ quảng bá. Một Router (hay một thiết bị được chọn trước) sẽ truyền phát toàn bộ bảng định tuyến RIP trên mạng một cách định kỳ. Chỉ riêng phương diện này thôi đã là một vấn đề đối với một số môi trường vì lý do kém hiệu quả.

Bên cạnh việc thông báo và cập nhật thông tin định tuyến, RIP cũng đồng thời cập nhật về những thay đổi của cấu hình mạng. Những cập nhật loại này được xếp vào loại "đáp ứng" (Response)

Một đặc trưng khác nữa của RIP là giao thức này dựa vào các thiết bị khác (các nút mạng kế tiếp) để định tuyến thông tin cho các máy đích ở xa hơn một "hop" (bước truyền). Một bước nhảy được tính trong đơn vị (mét). Số bước nhảy tối đa mà RIP có thể thực hiện được dọc theo một đường dẫn truyền là 15.

RIP duy trì các bảng với các mục khác nhau. Bảng này chính là bảng đã được nhắc đến ở trên, nó được quảng bá trên toàn mạng. Thông tin chứa trong mỗi mục trong bảng này gồm có:

- Địa chỉ IP của đích đến.
- Số bước nhảy (hop) cần thiết đi đến đích.
- Địa chỉ IP của router tiếp theo dọc theo đường truyền.
- Thông tin về việc tuyến có bị thay đổi hay không.
- Các bộ ghi thời gian dọc theo tuyến.

RIP hiện vẫn được sử dụng. Nhiều hãng cung cấp vẫn tiếp tục hỗ trợ RIP. Trong một số môi trường mạng RIP có thể vẫn là một giao thức tốt để sử dụng. Tuy nhiên, một số lớn các nhà cung cấp ngày nay hỗ trợ OSPF.

* Open shortest path first (OSPF- tìm đường dẫn ngắn nhất trước hết):

Triết lý của OSPF khác với của RIP. Một trong các nguyên lý của OSPF là:

- Cung cấp một loại định tuyến dịch vụ.
- Các mạng ảo (virtual network) có thể được xác định.
- Cung cấp phân bố tuyến.
- Quảng bá được tối thiểu hoá.
- Hỗ trợ một phương thức cho các router tin cậy.

Bên cạnh đó, nhiều dịch vụ khác cũng được hỗ trợ và thực hiện tuỳ thuộc vào nhà cung cấp.

* OSPF advertisments (quảng cáo OSPF): OSPF sử dụng phương thức hoạt động được gọi là "quảng cáo". Các quảng cáo này cho phép các router thông tin cho các router khác về các đường truyền. Có bốn loại quảng cáo khác nhau lần lượt là:

Autonomous: Có thông tin của các router trong các hệ thống tự trị khác.

Network: Chứa một danh sách các router được kết nối trong mạng.

Router: Chứa các thông tin về các bộ ghép nối router trong một phạm vi nhất định.

Summary: Lưu giữ thông tin về tuyến bên ngoài phạm vi đó.

Các quảng cáo này cung cấp một phương thức tiếp cận tập trung hơn để lan truyền thông tin trên toàn mạng. Bên cạnh các quảng cáo này, OSPF còn sử dụng một số các thông điệp để đối thoại. Một số thông điệp được liệt kê dưới đây:

- HELLO.
- Data base description: mô tả cơ sở dữ liệu.
- Yêu cầu trạng thái kết nối.
- Update trạng thái kết nối.
- Chấp nhận trạng thái kết nối.

Hai trong số các thông điệp trên sẽ được trình bày và giải thích tỷ mỉ dưới đây để hiểu rõ về hoạt động của OSPF.

* Phân tích header của OSPF: Các vùng của header được giới thiệu và giải thích một cách ngắn gọn dưới đây.

Version: phiên bản giao thức.

Type: cho biết thông điệp thuộc loại nào trong số 5 loại thông điệp nói trên.

Message length: cho biết độ dài của thông điệp bao gồm cả header.

Source gateway IP address: cung cấp địa chỉ IP của máy nguồn.

Area ID: xác định khu vực mà từ đó các gói tin đã được truyền đi.

Checksum: Checksum được thực hiện trên toàn bộ gói tin.

Authentication type: cho biết loại thẩm định sẽ được sử dụng, Authentication type bao gồm một giá trị từ loại thẩm định.

Gói tin HELLO bao gồm các thông điệp được gửi đi định kỳ để xác minh xem một đích đến nào đó có thể đến được không.

Dưới đây là danh sách các vùng trong một gói HELLO:

OSPF header: bắt buộc phải có

Network mask: chứa mặt nạ mạng cho mạng mà từ đó thông điệp này được gửi đi.

Deadtimer: giá trị đo bằng giây (s) cho biết rằng một lân cận đã ngừng hoạt động và không đáp ứng (không phản ứng).

HELLO interval: vùng này có một giá trị đo bằng giây (s) phản ánh thời gian tổng cộng giữa hai lần gửi gói tin HELLO của một router.

Router priority: vùng này được sử dụng nếu một router đã được chọn để sử dụng vào mục đích sao lưu dự phòng

Designated or backup router: xác định danh tính của router thực hiện nhiệm vụ sao lưu dự phòng (backup)

Neighbour router ID: vùng này và các vùng tiếp theo cho biết ID của các router vừa mới gửi đi các gói tin HELLO trong phạm vi mạng.

Thông điệp của gói tin mô tả cơ sở dữ liệu bao gồm một header của OSPF và các vùng chứa thông tin cần thiết. Các vùng này chứa thông tin về các thông điệp đã nhận được. Chúng có thể được chia nhỏ thành các đơn vị nhỏ hơn nữa. Việc mất mát hay thiếu hụt thông tin sẽ được phát hiện và thông báo đầy đủ. Gói tin mô tả cơ sở dữ liệu còn chứa cả các thông tin về loại và ID của kết nối (link). Chức năng Checksum cũng được cung cấp để bảo đảm không có những sai lệch, sai sót.

Header của gói tin về trạng thái kết nối (link state packet) bao gồm một OSPF header và các vùng nhằm cung cấp thông tin về router, mạng và loại trạm kết nối (link station type).

Điều cốt yếu của OSPF là ở chỗ nó làm giảm lưu lượng truyền thông trong mạng bởi vì OSPF chỉ thực hiện các cập nhật thông tin đơn lẻ chứ không quảng bá tràn lan trong toàn mạng. OSPF còn cung cấp khả năng kiểm duyệt quyền truy xuất. Một điểm mạnh khác nữa của OSPF là nó có khả năng trao đổi các mặt nạ (mask) và địa chỉ của các mạng con (subnet work).

6.1.5. INTERNET VÀ INTRANET

Intranet khác với LAN. LAN là mạng cục bộ chú trọng đến tính giới hạn về kích thước vật lý của mạng. Mạng Intranet là mạng nội bộ chú trọng đến tính giới hạn của cộng đồng người có quyền truy cập vào mạng.

Intranet vận hành theo giao thức TCP/IP và các giao thức khác có liên quan đến Internet, bao gồm Web server để xuất bản thông tin và cung cấp khả năng truy cập đến hệ thống back-end, có hỗ trợ trình duyệt web như một giao diện client thông dụng, và có hỗ trợ thư tín Internet như một hệ thống thư tín diện rộng.

Intranet có một số đặc trưng sau:

- Mạng Intranet là mạng máy tính được thiết lập trong phạm vi một cơ quan, tổ chức nhằm phục vụ cho việc chia sẻ tài nguyên thông tin, xây dựng môi trường làm việc chung thông qua sử dụng công nghệ Internet.

- Intranet có thể cô lập hoàn toàn khỏi Internet hoặc có thể bị ngăn cách bởi firewall.

Một số ví dụ về các ứng dụng dễ phát triển trên nền intranet bao gồm:

- Thư mục dành cho nhân viên (số điện thoại, lợi tức cá nhân...) hay các trang web cá nhân dành cho nhân viên

- Các ứng dụng cộng tác như các công cụ lập lịch/thời gian biểu, phần mềm nhóm và luồng công tác.

- Các công cụ trao đổi thông tin điện tử như chatroom, hội thảo điện tử dạng thoại và video, và các ứng dụng bảng thông báo.

- Thư viện điện tử dành cho tiếp thị, kỹ thuật và các loại thông tin khác.

Cũng có các bộ sản phẩm cung cấp các dịch vụ intranet từ server. Ví dụ như SuiteSpot của Netscape, bao gồm một Web server tiêu chuẩn, mail server, news server, catalog server, directory server, certificate server và một proxy server.

Phân phối multimedia thời gian thực trên mạng intranet đang trở nên phổ biến nhờ băng thông của mạng ngày càng tăng. Ngoài ra, các công nghệ nén mới giúp giảm đi nhu cầu băng thông, làm cho việc phân phối thời gian thực cho đàm thoại trực tiếp và hội nghị điện tử trở nên thực tế hơn.

Xu hướng nổi bật trong môi trường Internet/Intranet là dùng các công nghệ thành phần. Các ứng dụng được chia thành các thành phần nhỏ hơn để có thể dễ dàng phân phối và cập nhật khi cần. Các hệ thống theo dõi giao

dịch giữ cho các thay đổi trên đối tượng và dữ liệu tại nhiều vị trí được an toàn và chính xác.

Extranet

Extranet về cơ bản là một intranet được kết nối với một số intranet của các tổ chức khác. Việc kết nối có thể qua mạng internet hay sử dụng các kết nối mạng riêng. Trong cả hai trường hợp, hai tổ chức đều quyết định cùng chia sẻ thông tin và cho phép người dùng trong các tổ chức trao đổi thông tin qua lại. Các đối tác thương mại thường thực hiện điều này với EDI (Electronic Data Interchange) truyền thống. Với EDI, các định dạng và cấu trúc của các tài liệu điện tử như hóa đơn, đơn đặt hàng đều theo tiêu chuẩn đã định. Vì vậy, các dòng tài liệu có thể chuyển giao giữa nhiều tổ chức. EDI cũng được mở rộng thành công nghệ Web, theo cách như EDI truyền thống hoặc thành công nghệ business-to-business hoàn toàn mới.

6.1.6. BỨC TƯỜNG LỬA (FIREWALL)

Firewall chỉ đơn giản là một server đứng chắn giữa Intranet và thế giới bên ngoài, theo dõi các thông tin vào/ra Intranet. Firewall làm màn chắn điều khiển luồng lưu thông giữa các mạng, thường là giữa mạng và Internet, giữa các mạng con trong công ty.

Khi thảo luận về việc bảo vệ mạng, người ta thường tập trung mối đe dọa từ Internet, nhưng người dùng nội bộ cũng là mối đe dọa. Thật vậy, người ta thấy rằng đa số các hoạt động không được phép là do người dùng nội bộ gây ra. Ngoài ra, các công ty nối với các bạn hàng qua mạng dùng riêng rất dễ bị tấn công. Người dùng trên mạng của bạn hàng có thể khai thác các kết nối để ăn cắp thông tin có giá trị.

Chiến lược phòng vệ

Firewall thường được mô tả như là một hệ phòng thủ bao quanh, với các "chốt" để kiểm soát tất cả các luồng lưu thông nhập và xuất. Các mạng dùng riêng nối với Internet thường bị đe dọa bởi những kẻ tấn công. Firewall được dùng để bảo vệ dữ liệu bên trong và phải có một cách nào đó để cho phép người dùng hợp lệ đi qua và chặn lại những người dùng bất hợp lệ. Các máy chủ Web và FTP sẽ là nơi được kết nối vào Internet cho phép truy cập công cộng. Đằng sau hệ thống này là mạng dùng riêng của bạn, cần được bảo vệ bằng bức tường lửa.

Mọi giao dịch trước khi thực hiện phải được kiểm soát. Người đại diện làm dịch vụ ủy thác là Proxy server.

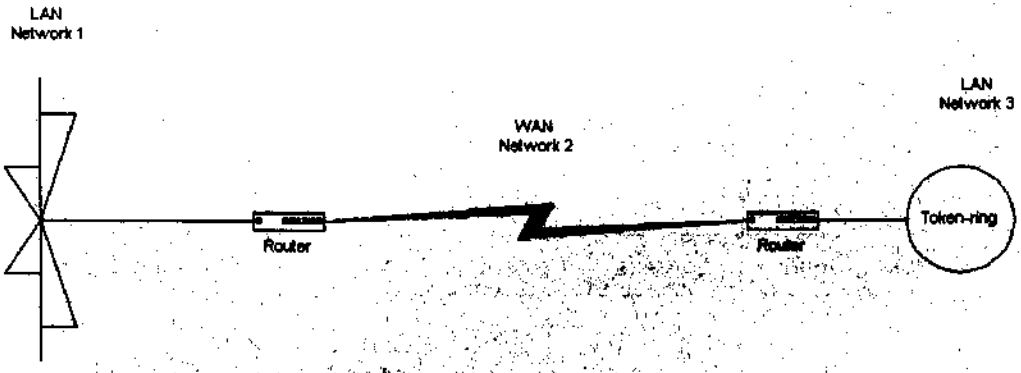
Firewall được thiết kế theo hai tiếp cận này. Firewall lọc gói (packet-filtering) dùng phương pháp khám xét tận đáy (strip search). Các gói dữ liệu trước hết được kiểm tra, sau đó được trả lại hoặc cho phép đi vào theo một số điều kiện nhất định. Dịch vụ ủy thác proxy server hoạt động như là một người đại diện cho những người dùng cần truy cập hệ thống ở phía bên kia bức tường lửa. Còn một phương pháp thứ ba gọi là giám sát trạng thái (stateful inspection). Phương pháp này tương tự như người giữ cổng, nhớ các đặc trưng của bất cứ người sử dụng nào rời khỏi trình duyệt web và chỉ cho phép quay trở lại theo những đặc trưng này.

Phân loại bức tường lửa

Có 3 loại sử dụng các chiến lược khác nhau để bảo vệ tài nguyên trên mạng. Thiết bị cơ bản nhất được xây dựng trên các bộ định tuyến và làm việc ở các tầng thấp hơn trong giao thức mạng. Chúng lọc các gói dữ liệu và thường được gọi là bộ định tuyến kiểm tra (screening router). Các cổng proxy server ở đầu cuối trên vận hành ở mức cao hơn trong giao thức. Firewall loại 3 dùng kỹ thuật giám sát trạng thái. Các bộ định tuyến được dùng cùng với các gateway để tạo nên hệ thống phòng thủ nhiều tầng.

6.2. CÁC DỊCH VỤ WAN

Mạng WAN nối liền các mạng LAN, qua đó tạo điều kiện cho việc truy xuất các máy tính, các file server tại các vị trí khác nhau. Không có các trạm làm việc nối trực tiếp vào liên kết này.



Hình 6.7. Hai mạng LAN nối với nhau bởi một liên kết WAN

Mục đích của kết nối WAN là làm sao để truyền dữ liệu một cách hiệu quả nhất. Tuy nhiên, các mạng LAN ở cự ly cách xa nhau nên kết nối chỉ được thực hiện qua các giao tiếp tốc độ thấp, làm cho tốc độ mạng WAN

chậm hơn nhiều so với của mạng LAN (tốc độ mạng T1 là 1.544Mbps so với Ethernet 10BASE-T là 10Mbps).

Vì được kết nối với nhau nên các máy tính, máy in, và các thiết bị khác trên một mạng WAN có thể liên lạc được với nhau để chia sẻ tài nguyên và thông tin, cũng như truy cập Internet.

6.2.1. POINT-TO-POINT PROTOCOL (PPP) - GIAO THỨC LIÊN KẾT ĐIỂM-ĐIỂM

Có hai phương pháp được cộng đồng Internet chấp nhận khi đóng gói và truyền tải gói dữ liệu IP qua một chuỗi các liên kết điểm-điểm. SLIP (*Serial Line Internet Protocol*) và PPP. Trong khi SLIP là giao thức nguyên thủy, PPP chiếm ưu thế hơn vì nó hoạt động chung với các giao thức khác như IPX (*Internetwork Packet Exchange*)...

PPP tạo các nối kết từ bộ định tuyến này đến bộ định tuyến kia, từ host đến bộ định tuyến, và từ host đến host. PPP sử dụng phổ biến cho các liên kết Internet trên các đường dây quay số. Ví dụ, người dùng tại nhà quay số đến ISP (*Internet service providers*) tại địa phương của họ. Sau khi modem đã tạo ra một nối kết, một phiên PPP được thiết lập giữa hệ thống người dùng và nhà cung cấp dịch vụ. Giai đoạn thiết lập bao gồm sự xác thực quyền truy cập của người dùng và việc khai báo địa chỉ IP. Về cơ bản, máy tính người sử dụng bây giờ được xem là thiết bị nối thêm vào mạng IP của nhà cung cấp dịch vụ Internet và cổng nối tiếp cùng với modem của người dùng có chức năng như một card giao diện mạng nối vào hệ thống mạng ISP.

PPP sử dụng phương pháp chia khung dữ liệu để đóng gói các gói tin ở giao thức cấp cao rồi truyền tải chúng qua các liên kết. Định dạng frame được mô tả:

			Data Frame		
Delimiter	**Control**	**Address**	**Protocol**	**Data**	**Frame check sequence**

Hình 6.8. Khuôn dạng của PPP

Delimiters: các khoảng giới hạn, đánh dấu điểm bắt đầu và kết thúc một frame.

Address: địa chỉ đích đến.

Control: số thứ tự để đảm bảo cho các điều khiển thích hợp.

Protocol: xác định giao thức trong frame (*IP, IPX, AppleTalk...*).

Data: dữ liệu, có thể có các chiều dài khác nhau.

Frame check sequency: tính tổng kiểm tra, dùng cho việc phát hiện lỗi.

Là thế hệ kế tiếp SLIP, PPP làm việc cả với lớp vật lý và lớp liên kết dữ liệu. Lớp vật lý hỗ trợ sự chuyển giao trên các đường dây bất đồng bộ và đồng bộ nhờ giao thức truyền nối tiếp như EIA-232-E, EIA-422, EIA-423, và CCITT V.34 và V.35.

PPP có ba thành phần chức năng chính. Tầng liên kết dữ liệu dựa trên cơ sở cấu trúc frame của điều khiển HDLC (*High-level data link control - điều khiển liên kết dữ liệu cấp cao*). Giao thức LCP (*Link control protocol - giao thức điều khiển liên kết*) thiết lập và quản lý các liên kết giữa hai trạm được nối với nhau. Nó thành lập các phương pháp đóng gói và kích thước gói, phương pháp nén dữ liệu, và các giao thức xác thực quyền (thông qua ID và mật mã người dùng). Hệ thống đang tiếp nhận phúc đáp lại bằng các gói tin LCP khác để thừa nhận và thẩm tra hay từ chối các lựa chọn cấu hình. Một khi nối kết đã được tạo ra, một giao thức điều khiển mạng được sử dụng để dàn xếp cấu hình của các loại giao thức, để hai host có thể bắt đầu trao đổi dữ liệu. Giao thức NCP (*Network control protocol - giao thức điều khiển mạng*) giúp cho việc định cấu hình của các giao thức lớp mạng khác nhau như IP, IPX, AppleTalk.

6.2.2. FRAME RELAY - DỊCH VỤ LIÊN VẬN KHUNG

Frame Relay là giao thức WAN chuyển đổi gói tin (*packet-switched protocol*), chuẩn hóa bởi ITU-T. Nó có khả năng nối kết vào nhiều mạng WAN khác nhau mà chỉ thông qua một liên kết đơn, làm cho Frame Relay chi phí rẻ hơn so với PPP trong giao tiếp với các mạng WAN lớn. Các mạch PPP sẽ nối khách hàng vào chuyển mạch Frame Relay gần nhất tại các điểm tải (*carrier*). Từ đó, các Frame Relay làm việc như các router, chuyển tiếp các gói tin thông qua mạng chuyển tải liên vận (*carrier's network*) nhờ vào phần địa chỉ đích trong header của gói tin.

Virtual circuit - Mạch ảo

Mạch ảo là đường liên lạc điểm-điểm giữa hai DTE trong mạng chuyển mạch gói hoặc frame relay, cung cấp liên kết hướng kết nối tạm thời hoặc chuyên dụng thông qua một mạng dùng bộ định tuyến (*router*) hoặc chuyển mạch. Các thiết bị đi cùng mạch này được lập trình bằng số hiệu của mạch để khi gói dữ liệu đến, bộ chuyển mạch biết được chính xác làm thế nào để

gói đi mà không cần xem chi tiết tiêu đề của gói. Điều này cải tiến vận hành và giảm kích thước tiêu đề các khung và gói dữ liệu. Về kỹ thuật, đường dẫn vật lý thông qua mạng chuyển mạch gói có thể thay đổi để tránh tắc nghẽn đường truyền, nhưng hai trạm đầu cuối phải bảo trì kết nối và cập nhật đặc tả đường dẫn nếu cần thiết. Mạch ảo có thể là cố định hoặc chuyển mạch.

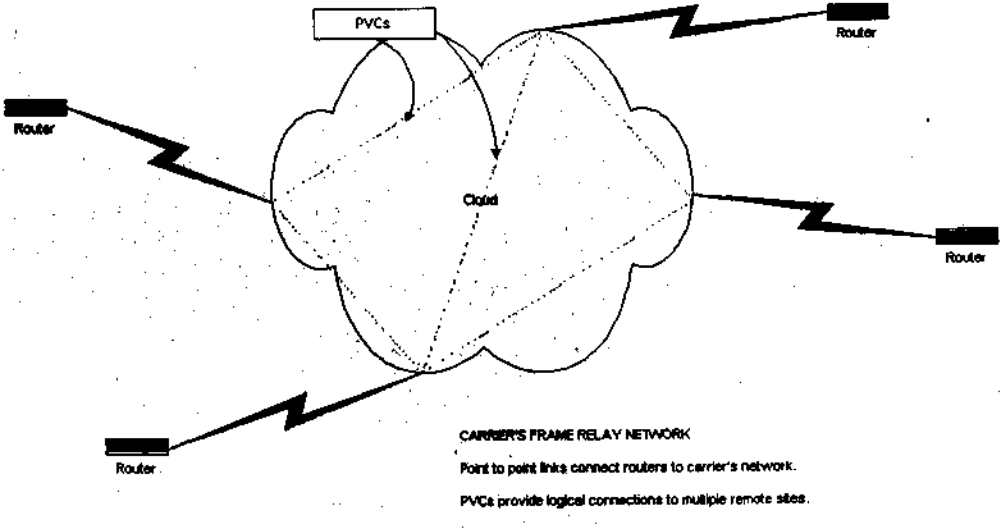
PVC (permanent virtual circuit - mạch ảo cố định)

Kết nối các trạm được định nghĩa trước, thường bằng băng thông tiền định và được bảo đảm. Trong các dịch vụ chuyển mạch công cộng như ATM hoặc frame relay, khách hàng có thể thỏa thuận trước các DTE của PVC với nhà cung cấp. Đối với mạng nội bộ, người quản lý tạo trước các PVC để định hướng đường truyền thông qua các phần riêng biệt của mạng hoặc để dành băng thông cho các ứng dụng đặc biệt.

SVC (switched virtual circuit - mạch ảo chuyển mạch)

Một kết nối tạm thời theo yêu cầu giữa các DTE, kéo dài chừng nào cần thiết và được tắt khi hoàn tất. Nhà cung cấp có thể để khách hàng xác định SVC hoặt thiết đặt một số SVC tiền định mà khách hàng thường yêu cầu nhất. Ví dụ, SVC trên mạng Frame Relay có thể dùng để gọi điện thoại trên mạng.

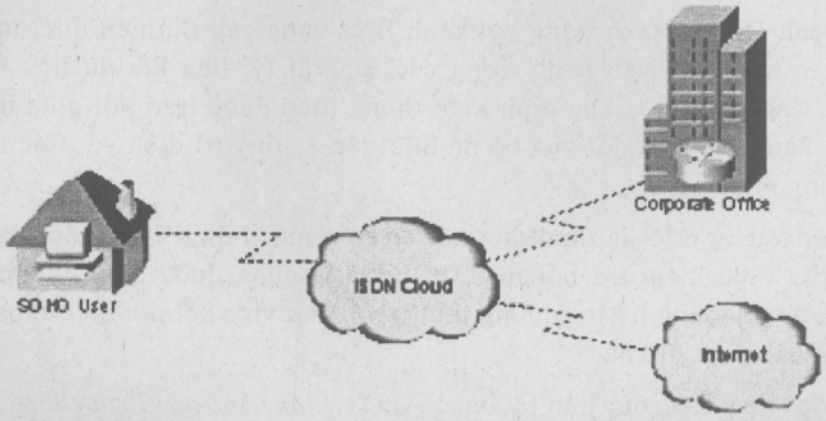
PVC là tốt nhất khi lượng thông tin lớn truyền qua lại giữa hai vị trí. SVC thích hợp hơn đối với những kết nối tạm thời. Các nhà cung cấp cảm thấy thoải mái với các PVC vì chúng cho phép họ quản lý băng thông và dễ dàng thanh toán cước phí với khách hàng. Có thể tính cước phí cho PVC theo từng tháng hay từng gói dữ liệu.



Hình 6.9. Mạng Frame Relay dùng PVC

6.2.3. INTEGRATED SERVICES DIGITAL NETWORK (ISDN) - MẠNG SỐ TÍCH HỢP CÁC DỊCH VỤ

ISDN là một hệ thống điện thoại chuyển mạch số, thiết kết thay thế cho hệ thống điện thoại tương tự PSTN (*Public Switched Telephone Network*), được chuẩn hóa bởi ITU-T. Một hệ thống có nhiều thuận lợi, bao gồm sự tin cậy, tính khả mở và thích hợp cho việc truyền dữ liệu số. ISDN thực hiện kết nối Internet và các WAN khác thông qua modem và mạng điện thoại số.



***Hình 6.10**. Hai mạng LAN liên kết bởi WAN*

Ba loại ISDN

BRI (Basic Rate ISDN), version đáng quan tâm nhất đối với người tiêu dùng vì nó vận hành trên dây đồng sẵn có, cung cấp các kênh thoại số và dữ liệu. BRI chia thành hai kênh, một kênh 64Kbps (*kênh B*) và một kênh 16Kbps (*kênh D*). Kênh B có thể được dùng cho thoại hoặc dữ liệu và được kết hợp tạo thành kênh dữ liệu 128kbps.

PRI (Primary Rate ISDN), tốc độ dữ liệu cao hơn. Về cơ bản, nó cung cấp các kênh bổ sung theo yêu cầu, lên đến tổng số 23 kênh B và một kênh D 64Kbps cho toàn bộ băng thông, tương đương một đường T1 (1.544Mbps).

Bảng 6.1. Cấu hình BRI và PRI

Giao diện	Số kênh B	Số kênh D	Tốc độ	Giải thông
BRI	2 (64Kbps)	1 (16Kbps)	144 Kbps	128 Kbps
PRI (T1)	23 (64Kbps)	1 (64Kbps)	1.544 Mbps	1.47 Mbps
PRI (T2)	30 (64Kbps)	1 (64Kbps)	2.048 Mbps	1.920 Mbps

B-ISDN (Broadband ISDN), CCITT phát triển với tốc độ 155Mbps do dự đoán các dịch vụ video và thông tin đa phương tiện. B-ISDN sử dụng

ATM (*Asynchronuous Transfer Network*) ở lớp liên kết dữ liệu và SONET (*Synchronuous Optical Network*) ở lớp vật lý.

Mạch ISDN hỗ trợ nhiều thiết bị ở cùng một thời điểm bằng bộ dồn kênh phân chia theo thời gian. Dòng dữ liệu được chia thành các khung, mỗi khung mang dữ liệu từ một thiết bị khác. Các bit được chuyển theo dòng đi qua mạch và được tách ra trên bộ truyền tải cuối rồi phân phối về thiết bị đích.

Giao diện kênh tín hiệu

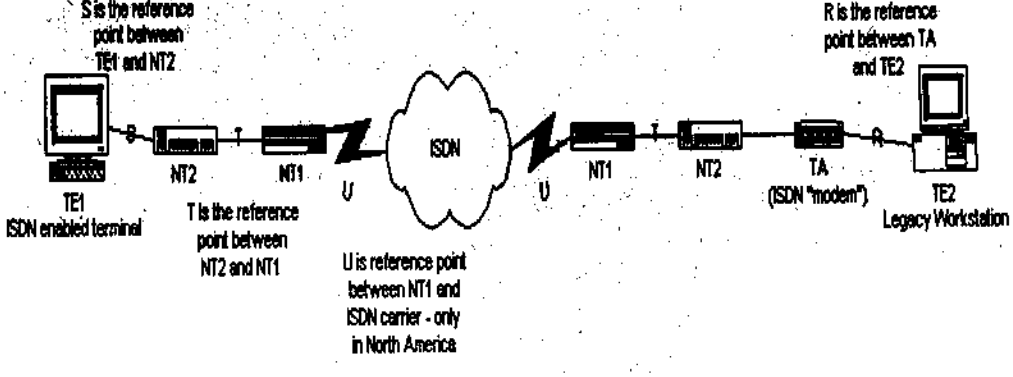
Kênh D được tách riêng với kênh B và cung cấp tín hiệu thiết lập cuộc gọi. Tín hiệu này vận hành trong các lớp vật lý, liên kết dữ liệu và tầng mạng. Các giao thức xác định kiểu thông điệp được trao đổi giữa thiết bị-khách hành, và trao đổi cục bộ để thiết lập và duy trì dịch vụ. Các dịch vụ mỗi tầng như sau:

Lớp vật lý thiết lập một kết nối chuyển mạch điện cung cấp truyền tải 64Kbps. Việc kiểm tra hồi tiếp và theo dõi cũng được quản lý trong lớp này. Lớp này cũng hỗ trợ đường multidrop cho việc kết nối điện thoại, máy tính và các thiết bị khác.

Lớp liên kết dữ liệu dùng LAPD (*Link Access Procedure for D Channel*), cũng là một HDLC. LAPD làm việc trên kênh D cung cấp thông tin điều khiển và tín hiệu. Nó cung cấp các dịch vụ liên vận (frame relay) và chuyển mạch khung (frame-switching). Lớp này chuyển tiếp các khung bằng cách đọc thông tin địa chỉ và gửi tiếp các khung theo đường dẫn ảo tương ứng đến đích.

Lớp mạng cung cấp các dịch vụ chuyển mạch gói. Các thông điệp trong lớp này được truyền đi bằng các giao thức lớp liên kết dữ liệu.

Một vài thành phần của ISDN được mô tả như ví dụ dưới đây:



***Hình 6.11** - Kết nối thiết bị ISDN*

Thiết bị đầu cuối loại 1 (*TE1*); thiết bị đầu cuối loại 2 (*TE2*), loại Pre-ISDN; đầu cuối mạng loại 1 (*NT1*), thiết bị nối đường thuê bao 4 dây vào vòng lặp cục bộ 2 dây; đầu cuối mạng loại 2 (*NT2*), thiết bị thi hành chức năng giao thức của lớp liên kết dữ liệu và lớp mạng; adapter đầu cuối (*TA*), dùng với pre-ISDN để nối nó với ISDN.

6.3. WORLD WIDE WEB (HOẶC WWW HOẶC W3)

World Wide Web là phương thức giao tiếp hữu hiệu và sinh động, giúp cho người sử dụng Internet có thể trao đổi thông tin và tìm kiếm thông tin một cách nhanh chóng và dễ dàng. Một tổ chức hay một đối tượng bất kỳ đều có thể tạo ra các trang Web cho riêng mình.

Có hai lí do khiến cho các trang Web ngày càng được phát triển phổ biến. Thứ nhất là khả năng dễ dàng sử dụng. Bạn có thể tìm được con đường để đến đích thông tin nhờ một động tác đơn giản là kích chuột vào những biểu tượng sinh động trên màn hình máy tính mà không phải tìm hiểu các câu lệnh bí ẩn của Unix hay những địa chỉ phức tạp. Thứ hai, bạn có thể dễ dàng thực hiện những công việc như truy cập vào những site FTP, login vào các máy tính khác sử dụng Telnet, hay đọc các nhóm tin của Usenet.

Nhưng cái thực sự làm cho Webpage trở nên độc lập và có sức mạnh chính là dựa trên nền tảng những Siêu liên kết (Hyperlinks). Để hiểu được siêu liên kết, bạn hình dung đến một cuốn từ điển bách khoa (encyclopaedia). Khi bạn tra từ đến Africa, bạn sẽ thấy hình ảnh một chú voi... Vậy thì, cách thức làm việc của một trang Web cũng hoàn toàn như vậy, với những siêu liên kết, có thể nhanh chóng và dễ dàng đưa bạn đến nơi bạn muốn tìm kiếm thông tin. Một trang web khi được mở ra sẽ hiện ra các biểu tượng dạng ký tự (text), hình ảnh tĩnh (static images), hoặc hình ảnh động (animations)... tương ứng chứa đựng các liên kết. Khi bạn di chuyển chuột hay bàn phím đến một biểu tượng, kích vào đó, bạn sẽ mở ra được một trang mới, trang được liên kết với trang chủ bằng siêu liên kết.

Tim Berners - Lee là người đầu tiên xây dựng trang chủ (homepage), là một trung tâm thông tin rất sáng sủa rõ ràng, chứa đựng những biểu tượng thông tin ảo (virtual information), thông qua việc gắn kết bằng những hyperlink, sẽ chỉ đến những không gian vật lý (physical space) là nơi chứa đựng những thông tin thật.

Ngôn ngữ sử dụng dựa trên sự nâng cấp của ngôn ngữ liên kết SGML, được gọi là ngôn ngữ liên kết siêu văn bản HTML (Hypertext Markup Language). HTML là một loại văn bản bao gồm những mã ASCII đơn giản,

xen kẽ là các lệnh đặc biệt (tags) tạo nên những hiệu ứng và điển hình là các siêu liên kết nói trên.

Như vậy, W3 dựa trên nền tảng HTML và cho phép HTML chạy trên Internet, thông qua giao thức chuyển giao siêu văn bản HTTP (Hypertext Transfer Protocol). Một lưu ý quan trọng là W3 sử dụng cấu trúc khách/chủ (client/server). Nếu bạn là tác giả, bạn chuẩn bị một trang web với đầy đủ thông tin, lưu trữ trong máy tính của bạn (server). Người sử dụng sẽ thông qua trang web của bạn, sẽ giao tiếp trực tiếp với server theo tư cách của một client. Họ sẽ sử dụng các chương trình khác nhau để có thể xem được nội dung của trang Web của bạn nhờ các chương trình trình duyệt (browsers) như Internet Explore, Nescape, Linux...

HTTP

Hypertext Transfer Protocol là một giao thức truyền tải dữ liệu tầng ứng dụng (application-level protocol of data transfering) liên kết các nguồn cung cấp tài nguyên W3 toàn cầu (W3 global information system) với người sử dụng, thông qua việc sử dụng ngôn ngữ siêu văn bản hypertext, như là tên của server, các hệ thống quản lý tài nguyên, thông qua sự mở rộng của yêu cầu (request), mã lỗi (error code) và tiêu đề (header). Đặc điểm của HTTP là các biểu trưng đại diện và sự thương lượng của dữ liệu thông tin, cho phép hệ thống được xây dựng hoàn toàn độc lập với dữ liệu sẽ được truyền đi.

Được bắt đầu sử dụng với W3 từ năm 1990, phiên bản đầu tiên của HTTP là HTTP/0.9, là giao thức đơn giản để truyền số liệu qua Internet. HTTP/1.0, định nghĩa dựa theo RFC (Request for Comments), cải thiện giao thức bằng cách cho phép các thông báo (messages), các thông tin về dữ liệu truyền nằm trong định dạng của MIME-like messages (Multipurpose Internet Mail Extension), những thay đổi trong nội dung của yêu cầu/đáp ứng (request/response). Dù sao, HTTP/1.0 không đủ khả năng đáp ứng cho những yêu cầu cao và phức tạp hơn, như việc dùng cấu trúc Proxy phân nhánh (hierarchical proxies), caching, yêu cầu của cuộc nối trong thời gian lâu (persistant connections), hoặc việc sử dụng các host ảo (virtual hosts)... Phiên bản hiện nay, HTTP/1.1 có đầy đủ sức mạnh để đáp ứng các yêu cầu trên.

Các hệ thống thông tin trên thực tế, đòi hỏi cao hơn như là tìm kiếm (search), nâng cấp đầu cuối (front-ended update)... HTTP đưa ra một cách sắp đặt cho đầu cuối mở (open-ended) và các tiêu đề (header) để chỉ ra mục đích của yêu cầu. Nó hoạt động dựa trên nguyên tắc tham chiếu, cung cấp bởi URI (Uniform Request Identifier), như là URL (Uniform Request

Location) hoặc URN (Uniform Request Name). Các thông báo (messages) sẽ được truyền đi theo định dạng giống như Internet Mail, dựa vào định dạng MIME-like message nói trên.

Nguyên tắc hoạt động của HTTP:

Giao thức HTTP là giao thức Yêu cầu / Đáp ứng. Khách hàng client gửi đến server:

- Yêu cầu theo phương thức định dạng URI
- Phiên bản protocol (protocol version)
- MIME-like message đã sửa đổi có chứa nội dung yêu cầu
- Thông tin khách hàng (client information)
- Và một vài nội dung nào đó tới server (body contents)...

Server đáp ứng yêu cầu trên đường trạng thái (status line):

- Phiên bản giao thức của thông báo (message's protocol version)
- Thành công hoặc mã lỗi
- MIME-like message chứa thông tin của server...

Hầu hết các giao tiếp HTTP đều bắt đầu thông qua trạm quản lý người sử dụng (user agent), yêu cầu được gửi đến nguồn cung cấp của một số server cơ sở (origin server). Trong trường hợp một giao tiếp phức tạp, cần phải có môi trường trung gian (intermediary) trên đường truyền Request Chain/ Response Chain. Có 3 loại trung gian điển hình: proxy, gateway, tunnel.

- Proxy là chương trình chuyển tiếp (program, forwarding agent), hoạt động như cả server lẫn client. Nhận yêu cầu, thực hiện trong nội tại proxy. hoặc viết lại tất cả hay một phần của thông báo yêu cầu và chuyển tới server được xác định trong yêu cầu nói trên. Transparent proxy, không sửa lại nội dung của yêu cầu. Non-Transparent proxy, sẽ sửa đổi lại nội dung của yêu cầu để thêm vào một số dịch vụ cho trạm quản lý người sử dụng, như là dịch vụ chú giải nhóm (group annotation services), hình thức biến đổi thông tin media (media type transformation), thu nhỏ giao thức (protocol reduction)... Trừ những ngoại lệ, HTTP proxy sử dụng đồng thời cả hai loại trên.

- Gateway là trạm nhận (server, receiving agent), như một server lớp trên (above server) của một số server, trong các trường hợp cần thiết sẽ phiên dịch Yêu cầu dưới dạng giao thức của server, hoạt động như một origin server. Client có thể không biết rằng nó đang làm việc với gateway.

- Tunnel là chương trình, hoạt động như một điểm trì hoãn (delay point) giữa hai mối liên lạc (connection) và không có một thay đổi nào nội dung của thông báo. Tunnel được sử dụng khi truyền thông tin cần vượt qua những trung gian (firewall), thậm chí khi các đối tượng trung gian không hiểu được nội dung của yêu cầu.

Giao thức truyền tập tin FTP

FTP (File Transfer Protocol) là một dịch vụ truyền tập tin trên hệ thống mạng Internet và trên các hệ thống mạng TCP/IP. Về cơ bản, FTP là giao thức client/server, trong đó một hệ thống đang sử dụng trình FTP server chấp nhận các yêu cầu từ một hệ thống đang chạy FTP client. Dịch vụ này cho phép người dùng gửi đến máy chủ các yêu cầu tải lên hoặc chép về các tập tin.

FTP làm việc thông qua nhiều hệ thống tập tin khác nhau, như vậy, các người dùng phải lưu ý rằng các kiểu tập tin trên FTP server có thể không tương thích với hệ thống của họ. Nói chung, tập tin văn bản có thể xem được bởi tất cả mọi loại hệ thống, còn các loại tập tin phổ biến mới hơn như PDF (Portable Document Format) của Adobe có ít khả năng này hơn.

Trên thực tế, FTP client điều hành quản lý phần lớn tiến trình đưa ra yêu cầu. Trước hết, nó thông dịch các câu lệnh của người dùng rồi mới gửi yêu cầu đó đến FTP server đang sử dụng giao thức FTP. Các câu lệnh và dữ liệu được gửi đi băng qua hai kết nối khác nhau. Khi bạn khởi động FTP và nối vào một FTP server, một liên kết được mở ra cho máy chủ đó để giữ nguyên tình trạng mở cho đến khi bạn gõ lệnh Close. Khi bạn đưa ra một yêu cầu truyền tập tin, dữ liệu của tập tin đó được truyền thông qua một kết nối khác, và kết nối này sẽ kết thúc khi quá trình truyền tập tin hoàn thành. Như vậy, một phiên truyền FTP điển hình có thể có vài liên kết được mở cùng một lúc nếu có nhiều tập tin đang được truyền đi. Sử dụng phương pháp này để chia sẻ điều khiển và dữ liệu, có nghĩa là liên kết đó có thể được sử dụng trong khi dữ liệu đã được truyền đi.

6.4. AN TOÀN THÔNG TIN TRÊN MẠNG

Cùng sự phát triển không ngừng của Internet, bảo mật hệ thống mạng trở thành vấn đề cấp thiết. Ngày nay, người dùng có nhiều công cụ và thông tin để truy nhập bất hợp pháp vào mạng, vì vậy cần có các công cụ ngăn chặn những truy cập này và theo dõi dữ liệu chuyển trong mạng.

6.4.1. CÁC CÁCH LẤY DỮ LIỆU BẤT HỢP PHÁP TRÊN MẠNG

a. Network Packet Sniffers (Bộ thu các gói tin mạng)

Packet Sniffes là những ứng dụng dùng card giao tiếp tiếp xúc với mạng truyền gói tin, cho phép lấy các packet đang truyền trên mạng. Packet Sniffers cung cấp những thông tin quan trọng như tên người dùng, từ khóa, thông tin về công nghệ mạng... khiến người tấn công có thể truy cập bất hợp pháp vào nhiều chương trình lấy thông tin và tài nguyên, vào tầng người sử dụng để tạo tài khoản mới, thay đổi những thông số hệ thống, liệt kê dịch vụ và quyền trên file server, truy cập vào những máy tính khác nữa trong mạng để lấy thông tin.

b. IP Spoofing (Giả mạo địa chỉ IP)

Người tấn công có thể dùng địa chỉ IP nằm trong dải IP đáng tin cậy của mạng để giả làm máy tính tin cậy, truy nhập bất hợp pháp vào mạng.

c. Password Attacks (Tấn công mật khẩu)

Hiện nay có nhiều cách để tấn công từ khóa như: IP Spoofing, Packet Sniffers, Trojan... Trong đó hai phương pháp thường dùng là IP Spoofing và Packet Sniffers.

d. Sự phân phối thông tin nhạy cảm

Dù đã có một chính sách bảo mật với những quyền truy nhập hợp pháp, vẫn có thể có sự vi phạm bảo mật khi phân bố thông tin nhạy cảm cho những người không tin cậy. Những thành viên này có thể dùng từ khóa và IP Spooping tấn công, sao chép và chia xẻ thông tin bảo mật.

e. Man-in-the- Midle attacks (Tấn công với người nội gián)

Người tấn công ở đây là người có khả năng truy cập vào các gói thông tin mạng, có khả năng theo dõi các gói tin truyền từ mạng này tới mạng khác.

6.4.2. CÁC CHIẾN LƯỢC AN TOÀN HỆ THỐNG

Trước khi đưa các giải pháp an toàn hệ thống cần một chiến lược nhìn chung tổng thể cả hệ. Có một số mặt cần lưu ý trong chiến lược an toàn hệ thống là:

a. Quyền hạn tối thiểu (Last Privilege)

Theo chiến lược này bất kỳ đối tượng nào cũng chỉ có những quyền hạn nhất định đối với thông tin và tài nguyên mạng. Đây là chiến lược nền tảng nhất.

b. Bảo vệ theo chiều sâu (Defence In Depth)

Theo nguyên tắc này, cần tạo nhiều cơ chế an toàn để hỗ trợ lẫn nhau, không chỉ dựa vào một chế độ an toàn cho dù nó rất mạnh.

c. Nút thắt (Choke Point)

Nguyên tắc này tạo một nút thắt, ở đó chỉ cho phép thông tin đi vào hệ thống bằng đường duy nhất, xây dựng một cơ chế kiểm soát và điều khiển các luồng thông tin qua nút thắt này.

d. Điểm nối yếu nhất (Weakest Link)

Người phá hoại thường tìm những điểm yếu nhất của hệ thống để tấn công, do vậy cần tìm và bảo vệ điểm yếu này. Thông thường, an toàn về mặt vật lý được coi là điểm yếu nhất.

e. Tính toàn cục

Cần có tính toàn cục cho các hệ thống cục bộ trong hệ thống an toàn. Nếu có thể phá vỡ một cơ chế an toàn thì cũng có thể tấn công thành công một hệ thống tự do, sau đó phá hoại hệ thống từ bên trong.

f. Tính đa dạng của việc bảo vệ

Khi truy nhập bất hợp pháp vào một hệ thống bất kỳ, người tấn công có thể truy nhập vào các hệ thống khác nữa. Do vậy, một hệ thống an toàn phải sử dụng nhiều biện pháp bảo vệ khác nhau cho những hệ thống khác nhau.

6.4.3. CÁC MỨC BẢO VỆ AN TOÀN

Các mức bảo vệ an toàn bao gồm: quyền truy nhập, đăng ký tên và mật khẩu, mã hóa dữ liệu, lớp bảo vệ vật lý, Fire wall. Để ngăn chặn các truy nhập mạng bất hợp pháp, người ta thường dùng đồng thời nhiều mức bảo vệ khác nhau cho mạng.

Chương 7

MẠNG KHÔNG DÂY 802.11

7.1. GIỚI THIỆU MẠNG KHÔNG DÂY

Nhu cầu về sử dụng hệ thống mạng di động ngày càng tăng. Các cách thức truyền dữ liệu trên hệ thống mạng truyền thống trên thế giới không còn đáp ứng được sự thách thức đề ra của đời sống xã hội. Nếu người sử dụng nối vào Internet thông qua hệ thống cáp vật lý, việc di chuyển của họ sẽ bị hạn chế, gò bó trong một vùng diện tích nhỏ hẹp. Kết nối không dây cho phép di chuyển nhiều hơn. Công nghệ không dây đang dần dần xâm lấn hệ thống mạng có dây (hoặc cố định) truyền thống.

Chúng ta đang ở trong thời kỳ thay đổi sâu sắc về hệ thống mạng và truyền thông máy tính. Công nghệ điện thoại không dây đã phát triển thành công bởi nó cho phép con người kết nối với nhau không cần ở những địa điểm cố định nào cả. Những công nghệ mới tập trung vào mạng máy tính thực hiện những điều tương tự khi kết nối vào mạng Internet. Một trong những công nghệ mạng không dây thành công đó là chuẩn 802.11

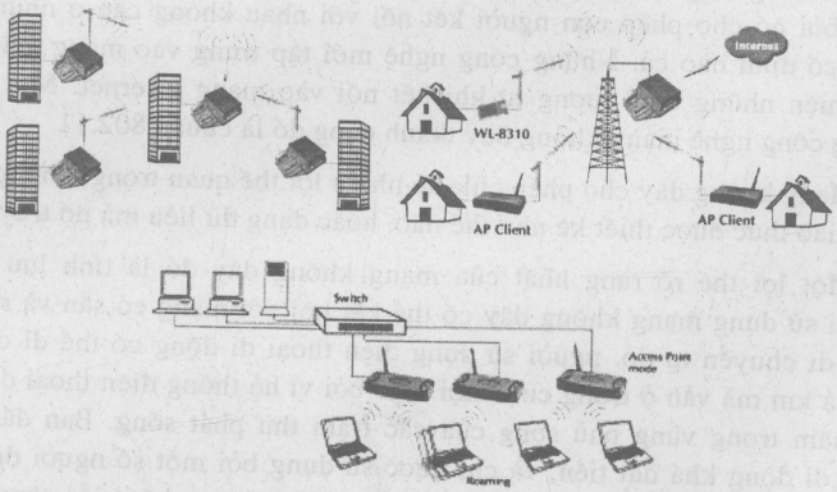
Mạng không dây cho phép chia sẻ nhiều lợi thế quan trọng, không quan tâm giao thức được thiết kế như thế nào, hoặc dạng dữ liệu mà nó truyền.

Một lợi thế rõ ràng nhất của mạng không dây đó là tính lưu động. Người sử dụng mạng không dây có thể kết nối với mạng có sẵn và rồi cho phép di chuyển tự do. người sử dụng điện thoại di động có thể di chuyển đến cả km mà vẫn ở trong cuộc hội đàm bởi vì hệ thống điện thoại di động vẫn nằm trong vùng phủ sóng của các trạm thu phát sóng. Ban đầu điện thoại di động khá đắt tiền, và chỉ được sử dụng bởi một số người dùng có nhu cầu cấp thiết về địa điểm và thời gian. Chiến lược phát triển rộng khắp, không biên giới của các nhà cung cấp dịch vụ điện thoại di động, đồng thời cùng với sự phát triển công nghệ điện thoại di động, sự phát triển của các hãng sản suất điện thoại di động và giá thành hết sức hợp lý, giúp cho điện thoại di động phát triển hết sức rộng lớn.

Mạng dữ liệu không dây giúp cho người sử dụng loại bỏ những giới hạn về tính di động của hệ thống cáp mạng cố định. Người sử dụng có thể ở trong thư viện, ở trong phòng hội thảo, hoặc là những phút giải lao nhâm nhi ly cafe tại quán cafe bên đường, miễn là trong vùng phủ sóng của trạm

đều có thể sử dụng mạng máy tính như những máy tính dùng cáp cố định. Cùng với sự phát triển không ngừng về thiết bị và công nghệ, tại thời điểm này, người sử dụng có thể di chuyển trong các khu vực bán kính vài trăm mét cách xa trạm thu phát. Bạn cũng có thể mở rộng khoảng cách trên bằng cách sử dụng các trạm thu phát nối nhau liên tục.

Đặc thù của mạng không dây là tính mềm dẻo cao, có thể triển khai lắp đặt nhanh. Mạng không dây sử dụng nhiều trạm thu phát cơ sở để kết nối người sử dụng với mạng máy tính có sẵn. Cơ sở hạ tầng của mạng không dây là giống nhau đối với việc bạn kết nối 1 người dùng hay hàng triệu người dùng. Để tạo ra vùng phủ sóng cho nơi sử dụng mạng không dây, phải sử dụng trạm thu phát sóng cơ bản và hệ thống ăng ten. Khi hệ thống cơ sở hạ tầng mạng không dây được xây dựng, vấn đề thêm người dùng chỉ còn là việc xác nhận quyền sử dụng. Với một hệ thống cơ sở hạ tầng đã xây dựng có thể thiết lập cấu hình để nhận dạng và cung cấp dịch vụ cho người dùng mới, nhưng việc xác nhận không yêu cầu thêm các thành phần, người dùng mới truy cập mạng không cần phải kéo thêm dây, hàn đầu nối, xác lập đầu cuối.



Hình 7.1. Một số sơ đồ ứng dụng giải pháp mạng không dây

Khả năng mềm dẻo là thuộc tính quan trọng của các nhà cung cấp dịch vụ. Nhiều nhà sản xuất sản phẩm theo chuẩn 802.11 đã theo đuổi thị trường kết nối được gọi là "điểm nóng". Sân bay, nhà ga đều có khách hàng quan tâm đến việc truy cập Internet trong lúc chờ đợi. Có nhiều lý do để không chọn việc sử dụng đường truyền cáp, việc chạy cáp mạng đắt tiền, lại tốn thời gian phục vụ khách và đôi khi lại phải thay đổi cấu trúc toà nhà, mất tính thẩm mỹ. Với mạng không dây, không cần sửa chữa xây

dựng gì, không cần phải dự đoán nhu cầu số lượng người cần sử dụng mạng. Chỉ cần một kết nối đơn giản vào Internet, rồi mạng không dây làm những việc còn lại cho người sử dụng. Tuy vậy, mạng không dây có giới hạn về băng thông, càng nhiều người sử dụng một trạm thu phát, sẽ làm giảm băng thông cho từng máy.

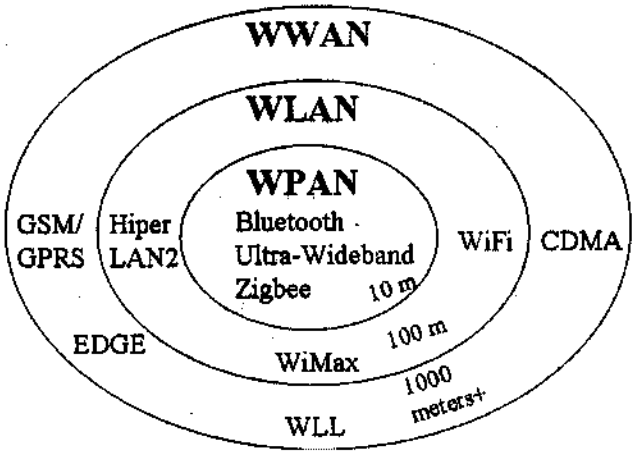
Đối với các toà nhà kiến trúc cổ, việc thay đổi kiến trúc để đấu nối hệ thống cáp mạng sẽ làm ảnh hưởng đến tính lịch sử của ngôi nhà, với giải pháp mạng không dây, điều đó sẽ không còn là vấn đề. Có thể triển khai nhanh một hệ thống mạng không dây phủ sóng toàn bộ toà nhà, và chỉ có một ít hệ thống cáp cần phải cài đặt trong toà nhà, điều này sẽ làm hài lòng các nhà lịch sử học.

Mạng không dây đã làm thay đổi sự phát triển của mạng truyền thông công cộng, nơi rất khó có thể xây dựng được hệ thống cáp mạng cố định. Với sự giảm giá nhanh chóng của các thiết bị chuẩn 802.11, những nhóm người tình nguyện có thể thiết lập chia sẻ mạng không dây cho mọi người. Những mạng cộng đồng sẽ mở rộng giải truy cập Internet thông qua đường kết nối DSL tốc độ cao, thông qua mạng không dây người dùng có thể dễ dàng sử dụng các kết nối này truy nhập vào mạng Internet.

Giống mọi hệ thống mạng khác, mạng không dây truyền dữ liệu trên môi trường truyền mạng. Môi trường truyền là một dạng của sóng điện từ. Để đáp ứng tốt nhất cho việc sử dụng mạng di động, môi trường truyền chắc chắn phải được phủ trên một diện tích rộng để những người sử dụng có thể di chuyển trong khoảng cánh rộng mà vẫn sử dụng được dịch vụ. Có hai môi trường truyền hay được sử dụng cho những ứng dụng cục bộ là ánh sáng hồng ngoại và sóng radio. Hầu hết các máy tính xách tay hiện nay đều có cổng hồng ngoại có thể nhanh chóng kết nối với các thiết bị ngoại vi có cổng hồng ngoại. Tuy nhiên sử dụng ánh sáng hồng ngoại sẽ bị giới hạn về khoảng cách, dễ dàng bị chặn lại bởi các bức tường, các thiết bị nội thất và văn phòng khác. Sóng radio có thể đi xuyên qua hầu hết các vật cản và cho phép mở rộng khoảng cách sử dụng. Điều này giải thích tại sao hiện nay các thiết bị chuẩn 802.11 đều sử dụng sóng radio.

7.1.1. LỊCH SỬ PHÁT TRIỂN MẠNG KHÔNG DÂY

Wireless network là giao thức mạng kết nối không dây sử dụng sóng radio để kết nối các thiết bị như máy tính xách tay vào mạng.



Hình 7.2. Các mô hình Wireless Network

Năm 1997, the Institute of Electrical and Electronic Engineers (IEEE) phác thảo chuẩn 802.11 cho WLANs (Wireless Local Area Networking).

WLAN là mạng cục bộ không dây cho phép kết nối không dây ethernet hoạt động theo đặc tả 802.11 của IEEE (Hiệp hội điện và điện tử Hoa Kỳ).

Năm 1999, chuẩn 802.11b được phác thảo và được công nhận bởi mạng lưới công nghiệp, và những sản phẩm từ mạng không dây trên khắp tần số 2.4GHz bắt đầu tồn tại.

WLAN hoạt động trong phổ tần số mà ủy ban truyền thông của Mỹ (FCC) cho phép tự do sử dụng không phải đăng ký. Bất kỳ ai cũng có thể vận hành nhiều loại thiết bị khác nhau trong những băng tần này mà không cần phải xin cấp bản quyền.

Hình 7.2 mô tả các mô hình mạng không dây, trong đó với khoảng cách ngắn dưới 10 m ta có thể sử dụng công nghệ ko dây WPAN như Bluetooth, Ultra-wideband... Khoảng cách từ dưới 100m sử dụng công nghệ WLAN như WiFi, WiMax....(Phần này là phần trọng điểm của tài liệu này).Khoảng cách từ 100m trở lên sử dụng công nghệ WWAN như CDMA, GSM/GPRS.

7.1.2. DẢI TẦN SỐ KHÔNG DÂY

Thiết bị không dây bắt buộc phải hoạt động tại dải tần nào đó, mỗi một dải có một băng thông (là khoảng rộng tần số trong dải). Băng thông hiểu theo nghĩa rộng là số đo của dung lượng dữ liệu kết nối. Đối với mạng điện thoại Analog sử dụng độ rộng dải là 20kHz, tín hiệu TV sử dụng độ rộng băng thông lên đến 6 MHz. Việc sử dụng phổ radio được nhà nước quản lý,

và khi muốn sử dụng sóng radio bạn phải đăng ký với đơn vị quản lý tần số tại nước ta.

Giữa những năm 80 của thế kỷ XX, Uỷ ban truyền thông liên bang (FCC) thay đổi phần 15 về quy định phổ radio, không chế các thiết bị không bản quyền. Sự thay đổi xác nhận các sản phẩm mạng không dây sử dụng điều chế phổ trải rộng hoạt động tại dải tần công nghiệp, khoa học và y tế (ISM). Dạng điều chế này trước đây được quy định chỉ dùng cho các mục đích quân sự. Tần số ISM có ba băng khác nhau tại các dải tần số 900 MHz, 2.4 GHz, 5 GHz (xem chi tiết ở phần trên). Trong giáo trình này ta chỉ quan tâm đến hai dải tần số 2.4 và 5 GHz.

Một điển hình của những dải tần ISM là cho phép người sử dụng các sản phẩm mạng không dây mà không cần xác nhận bản quyền sử dụng tần số, tuy nhiên ở một vài quốc gia, trong đó có Việt Nam, khi sử dụng dải tần số này phải xin giấy phép sử dụng tần số. Sau đây là một số dải tần số sử dụng trong công nghệ mạng không dây.

7.1.2.1. Dải tần 900MHz

Dải tần số thấp 900 MHz thường được sử dụng là dải trong công nghiệp, nghiên cứu và y học (ISM). Tổng độ rộng băng là 26 MHz, tín hiệu trong dải này có bước sóng xấp xỉ bằng 30cm. Những tín hiệu này có khả năng xuyên qua khá nhiều chướng ngại vật, ví dụ như những cây nhỏ, đồi thấp và đủ mạch để thu phát trong khoảng cách vài km. Bảng dưới đây cho biết chi tiết mức công suất của dải tần 900MHz

Bảng 7.1. Chi tiết mức công suất tại giải tần 900 MHz.

Dải	Công xuất truyền cực đại	Khuếch đại ăngten lớn nhất	EIRP (Công xuất phát xạ đẳng hướng đương lượng)
902 đến 928 MHz	+30dBm (1 Watt)	+6 dBi	+36 dBi (4 watt, liên quan đến hướng ăng ten)

7.1.2.2. Dải tần 2.4 GHz

Dải tần 2.4 GHz là dải giữa ISM, tổng độ rộng của dải là 83 MHz. Tín hiệu trong giải này có bước sóng xấp xỉ 12 cm. Tín hiệu này có khả năng xuyên qua các trướng ngại vật, nhưng không mạnh, xuyên qua một bức tường có thể gây ra độ suy hao 10 tới 12 dB. Độ suy hao khi đi qua cây phụ thuộc vào vóc dáng của tán lá cây và cây ướt hay khô, trung bình cứ đi qua 1 mét cây sẽ suy hao khoảng 0.5 dB, với đường kính cây 10 m sẽ có độ suy

hao lên đến 5 dB, độ suy hao 6dB sẽ giảm chiều dài kết nối đi 1/2 so với độ dài không bị suy hao. Khi đi qua một vài cây, khoảng cách có thể giảm đi hàng chục mét. Bảng dưới đây cho ta thấy chi tiết các mức công xuất tại dải tần 2.4 GHz.

Bảng 7.2. Chi tiết mức công suất tại giải tần 2.4 GHz

Dải	Công xuất truyền cực đại	Khuếch đại ăngten lớn nhất	EIRP (Công xuất phát xạ đẳng hướng đương lượng)
2403 đến 2483MHz (điểm đến nhiều điểm)	+30 dBm (1 Watt)	+6 dBi	+36 dBi (4 watt)
2403 đến 2483 MHz (điểm đến điểm)	+30 dBm (1 Watt)	(quy luật 3 đến 1) với mỗi độ khuếch đại ăngten 3 dBi giảm công suất máy phát là 1 dB. (Ví dụ với ăngten +9dBi, giảm công suất máy phát đến +29dBm)	Phụ thuộc vào kích cỡ ăng ten, với ăngten +24 dBi và ccông suất bộ phát là +24 dBm, kết nối điểm tới điểm là +38 dBi (64 Watt)
2403 tới 2483 MHz Phổ tần số dải rộng trải rộng sử dụng từ 15 đến 74 tần số	+21 dBm (125 mW)	+6 dBi	+27 dBi (500mW)

7.1.2.3. Dải tần 3.5 GHz

Giải tần này ít được sử dụng, tuy nhiên một vài dải con giữa 3.3 và 4.0 GHz được sử dụng tại một số nước. Dải này được đề cập ở đây là do thiết bị ở dải này trong một số trường hợp khá giống với thiết bị ở giải 2.4 GHz. Tín hiệu trong giải này có bước sóng khoảng 9 cm. Đặc trưng truyền trong một số trường hợp giống với dải tần 2.4 GHz, độ suy hao khi xuyên qua vật cản là lớn hơn

7.1.2.4. Dải tần số 5 GHz

Có 4 dải tần con tại 5 GHz (ở một vài nước trên thế giới đây là dải tần số tự do), qua hai băng tần gối lên nhau cho mỗi loại. Có một dải ISM từ 5725 đến 5850 MHz và có 3 băng tần (U-NII) 5150 đến 5250 MHz, 5250 đến 5350 MHz, 5725 đến 5825 MHz, mỗi băng tần ISM có độ rộng 125 MHz và mỗi một băng tần thuộc dạng U-NII là 100 MHz. Tín hiệu ở dải tần số 5 GHz có bước sóng khoảng 5 cm. Mỗi một băng tần con 5 GHz có độ rộng lớn hơn băng tần 2.4 GHz. Các thiết bị ở dải tần 5 GHz sẽ có nhiều băng thông hơn. Độ suy hao khi qua 1 mét cây sẽ là 1.2 dB. Với đường kính

cây là 10m ta sẽ có độ suy hao về chiều dài kết nối không dây lên đến 75%. Bảng dưới cho biết các mức công suất.

Bảng 7.3. Chi tiết mức công suất tại giải tần 5 GHz

Dải	Công xuất truyền cực đại	Khuếch đại ăngten lớn nhất	EIRP (Công xuất phát xạ đẳng hướng đương lượng)
ISM 5725 đến 5850 MHz	+30dBm (1 Watt)	+6 dBi	+36 dBi (4 watt) Chú ý rằng, với những hệ thống điểm tới điểm có thể sử dụng ăngten có độ khuếch đại lớn hơn +6dBi không gây giảm công suất bộ phát
U-NII 5150 đến 5250 MHz	+17dBm (50 mW)	+6dBi	+23 dBi (500 mW)
U-NII 5250 đến 5350 MHz	+24 dBm (250 mW)	+6dBi	+30 dBi (1 W)
U-NII 5725 đến 5825 MHz	+30dBm (1 W)	+6dBi	+35 dBi (4 W)

7.1.2.5. Dải tần 60 GHz

Băng ISM từ 59 tới 64 GHz được sử dụng tại Mỹ vào năm 1999, tổng độ rộng băng lên đến 5 GHz. Tín hiệu của băng này có bước sóng khoảng 1/2 cm. Tín hiệu trong tần số này bị suy hao bởi sự có mặt của Oxy trong không khí. Khoảng cách nối xa nhất trong dải tần này đạt 800m. Tín hiệu bị ngăn chặn hoàn toàn khi đi xuyên qua chướng ngại vật. Đặc điểm bổi bật của dải tần này là các thiết bị cung cấp tốc độ truyền dữ liệu kiểu điểm - điểm đạt 622 MBPS.

7.1.3. ƯU VÀ NHƯỢC ĐIỂM HỆ THỐNG MẠNG KHÔNG DÂY

7.1.3.1. Ưu điểm hệ thống mạng không dây

Chúng ta biết rằng mạng LAN có dây truyền thống có các ưu điểm như tính bảo mật cao, tốc độ nhanh (đặc biệt nếu dùng cáp quang)...,nhưng tại những nơi không thể triển khai được và yêu cầu tính linh động thì LAN có dây không đáp ứng được. Mặt khác với sự cải tiến công nghệ và sự hoàn thiện của các chuẩn, Wireless LAN ngày càng có nhiều ưu điểm:

Tiết kiệm được chi phí thiết lập các đường mạng trong tòa nhà và chi phí bảo dưỡng.

Tiết kiệm được thời gian.

Khả năng mở rộng và quản lý cao: do đặc tính dễ bổ sung các điểm truy cập trên mạng mà không mất thêm chi phí đi dây hay đi lại dây thông thường. Mạng không dây đặc biệt thuận tiện đối với những địa điểm khó đi dây. Với kết nối không dây luôn luôn sẵn sàng, các tổ chức, doanh nghiệp sẽ không gặp phải trường hợp bị mất, đứt hay hỏng dây dịch vụ của mình.

Tính linh động: Những người dùng máy laptop đã có thể di chuyển khắp nơi trong khu làm việc, dễ dàng kết nối với tài nguyên của hệ thống hữu tuyến. Các nhân viên có thể truy cập vào mạng LAN của công ty từ sân bay hoặc khách sạn khi đi công tác...

Tích hợp tốt với các mạng máy tính đã có sẵn, chia sẻ tài nguyên.

7.1.3.2. Nhược điểm hệ thống mạng không dây

Hệ thống mạng không dây hiện nay vẫn chưa thể thay thế cho mạng có dây. Với các hệ thống máy chủ, việc kết nối mạng không dây cho máy chủ là không thích hợp bởi chẳng ai lại di chuyển máy chủ khi đang hoạt động.

Tốc độ của mạng không dây bị hạn chế bởi băng thông có sẵn. Theo lý thuyết thông tin có thể giảm giới hạn trên của tốc độ mạng, càng nhiều thiết bị truy cập không dây thì tốc độ càng giảm. Ví dụ khi có bộ thu phát 11 MBPS ta có 11 trạm sử dụng thì mỗi trạm sẽ có tốc độ truyền là 1 MBPS, đối với mỗi bộ thu phát mạng không dây chỉ nên dùng tối đa 25 trạm sử dụng để nâng cao tốc độ mạng. Tốc độ mạng không dây bị giới hạn bởi dải tần số và cách điều chế, trong tương lai gần tốc độ mạng cũng chưa thể cải thiện ngay được, trong khi hiện nay tốc độ mạng dây đã lên đến 10 GBPS và sẽ còn tiếp tục tăng.

Sự ổn định đường truyền phụ thuộc quá nhiều vào các thiết bị phát sóng khác, khi gặp chướng ngại vật, gặp các bộ thu phát sóng khác ở gần giải tần số, độ suy hao sẽ tăng lên dẫn đến giảm tốc độ và khoảng cách đường truyền.

Tính bảo mật của hệ thống chưa cao, bởi chỉ cần bạn ở trong vùng phủ sóng của hệ thống mạng không dây là bạn đã có thể tiếp cận với dữ liệu truyền trên mạng.

Tần số càng cao thì tốc độ càng cao nhưng độ suy hao cũng tăng theo làm giảm khoảng cách

7.1.4. NHU CẦU VÀ SỰ CẦN THIẾT CỦA MẠNG KHÔNG DÂY

Trong hai thập kỷ qua, người dùng vẫn kết nối các máy tính cá nhân bằng cáp, việc kết nối qua không gian không cần đến các loại cáp vẫn còn tương đối mới với người sử dụng.

Hiện nay, ở những nơi mà chi phí địa ốc đắt đỏ, các tổ chức, doanh nghiệp có xu hướng chuyển đổi sang trạng thái di động. Cùng với các thiết bị không dây (điện thoại di động, máy tính xách tay, PDA...), xu hướng này không chỉ làm tăng năng suất và hiệu quả làm việc của nhân viên mà còn giảm diện tích văn phòng cho họ.

Văn phòng di động mang tới cho nhân viên độ linh hoạt và khả năng quản lý thời gian tốt hơn, tăng năng suất làm việc và tiết kiệm được chi phí đáng kể trong các hoạt động.

Với mạng LAN không dây, nhân viên làm việc có thể truy cập vào cơ sở dữ liệu của cơ quan mình tại văn phòng hay bên ngoài và có thể liên tục sử dụng những thiết bị nối mạng để kết nối vào Internet. Ứng dụng không dây đặc biệt thích hợp đối với những nhóm người làm việc thường phải di chuyển. Ví dụ như gửi thư điện tử trong khi đang đợi chuyến bay tiếp theo hay gửi thông tin đi ngay khi máy bay hạ cánh xuống sân bay. Các bà mẹ có thể cùng con gái tham gia lớp học bơi đồng thời vẫn có thể đọc và trả lời thư điện tử của mình.

Sử dụng công nghệ mạng không dây, các tổ chức, doanh nghiệp tiết kiệm được chi phí thiết lập các đường mạng trong tòa nhà và chi phí bảo dưỡng. Mạng LAN không dây còn có khả năng mở rộng và quản lý cao do đặc tính dễ bổ sung các điểm truy cập trên mạng mà không mất thêm chi phí đi dây hay đi lại dây thông thường. Mạng không dây đặc biệt thuận tiện đối với những địa điểm khó đi dây. Kết nối không dây luôn luôn sẵn sàng, các tổ chức, doanh nghiệp sẽ không gặp phải trường hợp bị mất, đứt hay hỏng dây dịch vụ của mình.

Tốc độ là điều cốt yếu. Mạng không dây sẽ tiết kiệm được thời gian lắp đặt chạy dây khắp cả văn phòng và tiếp tới là tiết kiệm công sức nhân lực vì không cần phải lắp đặt các điểm truy cập mạng LAN thông thường. Kết nối người sử dụng không dây được tự động hóa giữa các mạng, cài đặt và phần cứng khác nhau, giúp việc triển khai cũng như bố trí lại đơn giản và linh hoạt. Đến nay, người sử dụng không còn phải lo lắng về chuyện tốc độ nữa, vì mạng LAN không dây hiện nay nhanh gấp đã đạt đến tốc độ 108 Mbps

và có thể còn tiếp tục tăng trong tương lai gần - chỉ chậm hơn không đáng kể so với mạng Ethernet thông thường.

Trên lý thuyết, mạng không dây có thể truyền dữ liệu với tốc độ 11Mbps, trong khi mạng LAN nối dây tương đương có thể truyền dữ liệu với tốc độ 9Mbps. Công nghệ mạng không dây chắc chắn sẽ còn nhanh hơn nữa.

Chi phí cho mạng LAN không dây mới ngày càng hợp lý hơn. Thời điểm viết giáo trình này, chi phí đầu tư cho mỗi một máy tính hoà mạng không dây chỉ khoảng 100 USD, chi phí này sẽ còn tiếp tục giảm trong tương lai.

Nếu xét mạng LAN có dây tính luôn chi phí lắp đặt thì giá thành của mạng LAN có dây và không dây tương đương nhau. Hơn nữa, WLAN lại tiện dụng hơn, chỉ cần bổ sung một ĐTC trong một khu vực cho nhiều người sử dụng chỉ trong vài giờ.

An toàn thông tin là vấn đề cực kỳ quan trọng trong thế giới nối mạng. Các vấn đề về an toàn thông tin như gửi dữ liệu bị giải mã trên những tần số không an toàn là vấn đề đã được đề cập tới nhiều trong các mạng không dây. Các công ty cần bảo vệ thông tin nhạy cảm, phần cứng và các giao dịch của mình.

An toàn thông tin phụ thuộc vào khả năng thiết lập hoạt động truyền dữ liệu được xác thực, bảo mật và bảo đảm nguyên vẹn. Nhưng nếu một khu vực công cộng như quán cà phê đặt gần một công ty cũng có mạng không dây, thì về cơ bản, thông tin sẽ di chuyển không được bảo vệ trong không gian trên những mạng này và một hacker có thể can thiệp được.

Trong phạm vi an toàn thông tin không dây, những băn khoăn chính tập trung xung quanh mật khẩu mã hóa tĩnh hay động, quản lý tập trung hay phân tán. Một vài lựa chọn về an toàn thông tin mạng không dây gồm có: Mạng riêng ảo (Virtual Private Network - VPN) và giao thức 802.1x (chuẩn công nghiệp), đều kết hợp mật khẩu và mã hóa cũng như quản lý tập trung. Chỉ khá hơn mạng liên lạc thông tin tế bào analog, 802.11b là giao thức thông tin dễ bị tấn công nhất. Sử dụng chuẩn công nghiệp và công nghệ, máy xách tay IBM ThinkPad đã kết hợp hệ thống bảo mật với công nghệ VPN cung cấp phương thức đảm bảo an toàn cho liên lạc qua giao thức.

Hiện nay, nhiều công ty cung cấp dịch vụ bảo mật đã đưa ra nhiều giải pháp ứng phó với những vụ xâm nhập bất hợp pháp. Phương pháp "mã hóa" là phân tán thông tin theo một mã được gửi theo một tần số. Dữ liệu được mã hóa này sau đó được tập hợp lại khi tới điểm nhận.

Những người sử dụng thường được nhắc nhở chỉ gửi thông tin đã được mã hóa để đảm bảo không có sự rò rỉ thông tin quan trọng. Phương pháp sử dụng máy dò Sniffers có thể dò được địa điểm của mạng 802.11b và biết được khi nào mạng đang truyền dữ liệu. Ngoài ra, " mạng riêng ảo VPNs" (Virtual Private Networks) là những hệ thống trung gian điện tử không thể dò tìm được đặt giữa các mạng trao đổi dữ liệu cũng đã được nhiều nơi sử dụng hiệu quả trong việc đảm bảo an toàn cho mạng.

Một công ty hay tổ chức sử dụng công nghệ không dây để có thể hoạt động năng suất cao hơn nhưng họ cũng cần xem xét kỹ lưỡng nhu cầu cũng như yêu cầu hoạt động của mình để có thể tận dụng được hết các lợi ích của mạng không dây.

Điều đầu tiên, họ cần phải chọn cho đúng nhà cung cấp giải pháp tin cậy, có thể phát triển được phần mềm, phần cứng và công nghệ mạnh nhất, nhằm thực hiện được tất cả những công việc của họ một cách hoàn hảo nhất.

Cho tới nay Viện Kỹ thuật Điện và Điện tử (Institute of Electrical and Electronic Engineers - IEEE) đã phát triển ba chỉ tiêu kỹ thuật cho mạng LAN không dây: 802.11a, 802.11b và 802.11g. Cả ba chỉ tiêu kỹ thuật này sử dụng công nghệ đa truy nhập nhạy cảm sóng có phát hiện va chạm (Carrier Sense Multiple Access - Collision Detection CDMA/CD) như một giao thức chia sẻ đường dẫn. CDMA/CD là một phương pháp truyền dữ liệu được ưa thích vì độ tin cậy của nó thông qua khả năng chống mất dữ liệu. Các ứng dụng mạng LAN, các hệ điều hành hoặc giao thức mạng, bao gồm cả giao thức Internet TCP/IP sẽ chạy trên các mạng WLAN tương thích chuẩn 802.11 dễ dàng như chạy trên Ethernet nhưng không cần phải chạy cáp qua tường hay trần nhà.

Trong vài năm qua chuẩn 802.11b đã thực sự mở ra nhiều cơ hội hấp dẫn. Các hệ thống khách sạn và công ty cho thuê xe hơi đã triển khai các sản phẩm dựa trên chuẩn 802.11b để hỗ trợ các hoạt động nhận phòng, trả phòng, nhận xe trả xe di động. Các chuyên gia y tế không chỉ đọc bệnh án mà còn có thể nhận được theo thời gian thực các tín hiệu sinh tử và dữ liệu đối chiếu khác từ giường bệnh mà không còn phải phụ thuộc vào hàng đống đồ thị và giấy tờ luân chuyển qua các bộ phận. Các công nhân trong xưởng sản xuất có thể truy cập vào thông số kỹ thuật mà không phải kết nối dây phức tạp. Hiện nay, các công ty sản suất thiết bị mạng không dây dần chuyển tất cả các thiết bị không dây sang hoạt động tại chuẩn 802.11g, các thiết bị này thường hỗ trợ cùng một lúc hai chuẩn 802.11b và 802.11g, cho phép cùng lúc các thiết bị không dây hoạt động tại hai chuẩn 802.11b,

802.11g hoạt động trên cùng một mạng. Hiện nay chuẩn 802.11g đã hỗ trợ tốc độ đạt 108 MBPS (chi tiết xem phần chuẩn 802.11).

Các hệ thống WLAN hiện tại trên thị trường đang hỗ trợ chuẩn 802.11b chỉ có tốc độ giới hạn ở 11Mbps, tuy nhiên tốc độ này vẫn nhanh hơn tốc độ modem 56Kps 200 lần và thậm chí vẫn nhanh hơn modem cáp đồng trục và DSL. Chỉ tiêu kỹ thuật mới của IEE đại diện cho một thế hệ WLAN mới. 802.11a là chuẩn riêng không phụ thuộc, nó hứa hẹn có nhiều tính năng mới xuất sắc.

Intel đã công bố sẽ hỗ trợ chỉ tiêu kỹ thuật 802.11a bằng cách tung ra Bộ truy cập không dây Intel Pro/Wireless 5000 LAN Access Point và các bộ chuyển đổi CardBus và PCI. Intel cũng công bố bộ công cụ mở rộng dual-mode cho phép các điểm truy cập phục vụ được cả chuẩn 802.11b hiện hành và chuẩn 802.11a mới, giúp các tổ chức doanh nghiệp chuyển lên các hệ thống tốc độ cao hơn.

Mặc dù các sản phẩm 802.11a và 802.11b có dải giống nhau nhưng 802.11a tạo tốc độ cao hơn trên toàn diện tích nó phủ sóng. Với tốc độ truyền dữ liệu 54Mbps, nó nhanh hơn bất cứ giải pháp WLAN nào khác. Thế hệ sản phẩm WLAN tốc độ 54Mpbs đầu tiên sẽ hấp dẫn các ứng dụng đòi hỏi nhiều băng thông như thiết kế CAD, truyền video nhưng nó sẽ chỉ thực sự phổ biến khi các ứng dụng phát triển cao hơn chuẩn 802.11b.

Dải tần 5GHz, nơi 802.11a hoạt động, không "đông đúc" lắm nên sẽ ít bị nhiễu hoặc tranh chấp tín hiệu. 802.11a là phương tiện hợp lý và hiệu quả nhất có thể tải hết các ứng dụng băng thông cao cho một số lượng lớn người dùng - đồng thời 8 kênh không trùng nhau cho phép khả năng mở rộng cao hơn, lắp đặt linh hoạt hơn. Do đó, có thể nhóm 8 điểm truy cập (Access Points) để tạo ra tốc độ 432Mbps chia sẻ được giữa nhiều người dùng trong cùng một khu vực. Điều này tạo ra giá trị tốt nhất cho lựa chọn mạng tốc độ cao cho những người không triển khai mạng LAN không dây hoặc người dùng muốn gia tăng tốc độ cho mạng LAN không dây có sẵn của mình. Tuy nhiên vẫn còn một số câu hỏi: Mạng WLAN có mức bảo mật bằng hoặc cao hơn mạng cáp thông thường không?

Về khía cạnh kinh tế + tốc độ, không ai nói đó là ưu điểm của hệ thống Wireless cả.: Một Access Point có công suất là 11 Mbps, nhưng đó là share giữa các Wireless client với nhau, tưởng tượng một AP cover 20 user, tương ứng với 11m/20, mỗi user chưa tới 1m. Đối với 802.11b, tốc độ 11Mbps chỉ đạt được ở mức 50 mét đổ xuống, mà đâu phải lúc nào user cũng chỉ trong bán kính 50m.

Sau này, khi ra chuẩn 802.11a, một vài thiết bị như Cisco 1200 AP, có module hỗ trợ chuẩn này, thì tốc độ lên được 52 Mbps, cũng có cải thiện về băng thông.

Cùng nằm trong hệ thống MxU của Cisco (hệ thống Broadband service) với wireless là Cable và LongReachEthernet, cả 3 đều là những giải pháp khá lý tưởng cho người dùng đầu cuối không chuyên, hoặc cân bằng giải quyết được bài toán "băng thông - độ dài - giá tiền" khá phức tạp.

Ở các nước tiên tiến, đặc biệt là Hàn Quốc, mô hình MxU được áp dụng khá rộng rãi, gần như là tuyệt đối.Trên thị trường Việt Nam có 4 đến 6 hãng cung cấp thiết bị mạng không dây nổi tiếng như Cisco, Planet, SMC và Rebotec (Đài Loan), Skywave (Mỹ), Linksys, Dlink. Trong đó chỉ một vài hãng cung cấp thiết bị không dây ngoài trời với khoảng cách phủ sóng tối đa là 40km. Một trong những hãng được chọn để sử dụng nhiều nhất là Skywave do tốc độ truyền dữ liệu và vùng phủ sóng cao.

Hỗ trợ giải pháp WDS (Wireless Distribution System) kết hợp với một hay nhiều AP Router khác làm chức năng nối sóng, cho phép mở rộng vùng phủ sóng lên nhiều lần so với loại thông thường. Đồng thời tích hợp khả năng bảo mật mới WPA (WiFi Protect Access), mã hóa 128bit, cho phép nhận diện thiết bị mạng thông qua địa chỉ MAC. Chỉ có thiết bị ngoài trời có công suất mạnh từ 350mW đến 2watt với vùng phát sóng từ 1 đến 40km, kết hợp nhiều loại anten như Ommi, Patch Panel, Yagi, Parabolic Grid để tạo ra vùng phủ sóng và tỏa xa khác nhau.

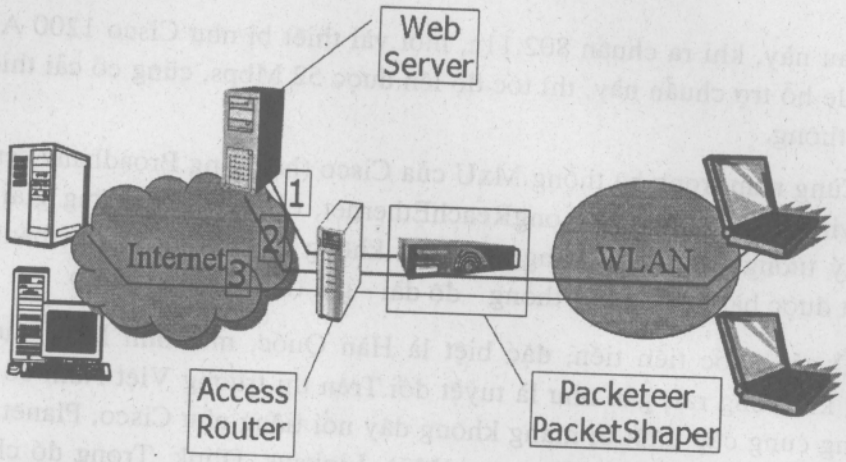
Các tính năng thiết bị ngoài trời là chịu được môi trường lực từ, ẩm ướt, nhà xưởng nhiều bụi than, gió... phù hợp với điều kiện nhiệt độ Việt Nam.

Các giải pháp trên ứng dụng để nối mạng Ethernet trong văn phòng, nhà xưởng cho tất cả các thiết bị vi tính văn phòng; dùng làm điểm truy cập Internet với hệ thống IP động và hệ thống ngăn chặn những cuộc truy cập từ xa không được phép tại các nơi công cộng như sân bay, bệnh viện, nhà ga..

Hệ thống mạng không dây cũng hỗ trợ thêm nhiều ứng dụng khác nhau như IP phone, camera, PDA, wireless mini printer.

Đối với giải pháp ngoài trời dùng để nối mạng giữa các tòa nhà cao tầng, giữa trung tâm và chi nhánh, giữa văn phòng chính và nhà xưởng.

Hiện nay không còn tồn tại mạng cáp truyền thống, chứng minh cho xu thế mạng không dây đang phát triển.



Hình 7.3. Wireless LAN và môi trường khác

Những ai cần sử dụng mạng không dây:

Đó là các tổ chức, công ty có địa điểm rất khó triển khai mạng LAN có dây như những tòa nhà cũ, khu di tích lịch sử, những công ty phải thuê cơ sở hạ tầng, những công ty có ngân sách hạn hẹp...

Các tổ chức, công ty có nhiều trụ sở, nhiều tòa nhà, họ cần phải nối các mạng với nhau mà không muốn thuê đường truyền, hoặc không muốn đi dây cáp dưới đất, dưới đường, việc này rất tốn kém và phiền phức.

Những người sử dụng hay phải di chuyển, hay phải đi công tác...

Cho các ứng dụng "điểm nóng" như các quán cafe, nơi công cộng cần truy cập Internet.

Cho các địa điểm cho thuê ngắn hạn cần triển khai kết nối mạng trong các khoản thời gian ngắn và gọn.

7.2. PHỔ TRẢI RỘNG

Công nghệ *Phổ trải rộng* (spread spectrum) được dùng lần đầu trong thế chiến II để điều khiển ngư lôi. Spread spectrum truyền một tín hiệu trên một dải tần số rộng. Máy nhận thu thập các tín hiệu này dựa trên thông tin đã được sắp xếp trước với máy gửi. Các tín hiệu spread spectrum rất khó phát hiện và nếu phát hiện được thì cũng rất khó biên điệu. Điều này bảo

đảm an toàn. Ngoài ra, các tín hiệu spread spectrum ít gây giao thoa với các tín hiệu khác. Tín hiệu rộng đòi hỏi năng lượng truyền ít hơn. Trong thực tế, các tín hiệu spread spectrum có thể chiếm cùng băng thông như các tín hiệu sử dụng băng thông hẹp.

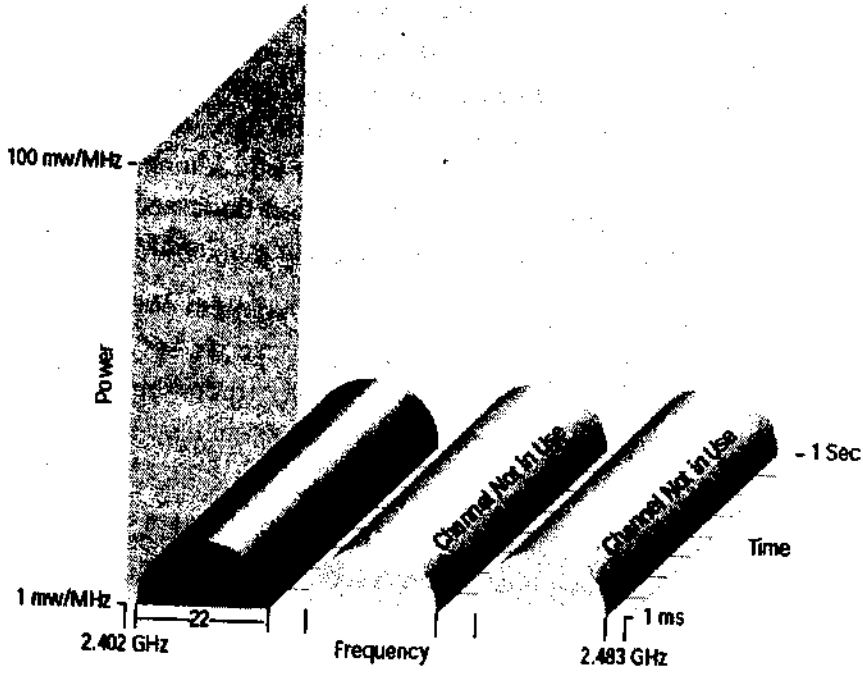
Đặc trưng chính của spread spectrum là tín hiệu ban đầu được trải ra trên băng thông rất lớn, thường trên 200 lần so với băng thông của tín hiệu ban đầu. Với ngành công nghệ thông tin, công nghệ phổ trải rộng là phương pháp thường dùng để điều biến thông tin vào thành dạng những bits có quản lý được gửi qua hệ thống không dây phát sóng trên không. Phổ trải rộng được phát minh bởi Heddy Lamar, nhà phát minh được xác nhận và nhận được nhiều phần thưởng của các chính phủ bởi công nghệ này.

Về cơ bản, công nghệ phổ trải rộng đưa ra khái niệm chia thông tin qua chuỗi các kênh radio hoặc tần số. Nói chung, số các tần số vào khoảng 70, và hầu hết các thông tin sẽ gửi trên các kênh này trước khi được giải điều chế. Có nhiều kỹ thuật spread spectrum, nhưng có hai kỹ thuật phổ dụng nhất đó là

Phổ trải rộng tuần tự trực tiếp (DIRECT SEQUENCE SPREAD SPECTRUM - DSSS): Trong phương pháp này, dữ liệu truyền được thay đổi bởi một dòng bit do bên gởi tạo ra. Dòng bit này biểu diễn mỗi bit trong dữ liệu ban đầu bằng nhiều bit trong dữ liệu tạo ra, như vậy làm mở rộng tín hiệu trên băng thông rộng hơn. Nếu có 100 bit được dùng để biểu diễn mỗi bit dữ liệu, thì dòng tín hiệu được mở rộng 100 lần so với băng thông ban đầu. Nguồn tạo ra dòng bit giả ngẫu nhiên để điều biến dữ liệu nguồn, và đích tạo ra cùng dòng bit để giải điều biên những gì nó nhận. Spread spectrum sẽ báo thẳng vào các băng thông bị nhiều nhiễu, nhưng không vượt quá âm lượng nhiễu. Các tín hiệu âm của phổ trải rộng quá yếu không thể giao thoa với các tính hiệu âm thường và ít bị vi phạm những điều cấm kỵ do uỷ ban truyền thông liên bang FCC quy định. Để dễ hiểu hơn, ta có thể hình dung spread spectrum là chuỗi các đoàn tàu nối tiếp đang khởi hành cùng một thời điểm, tải trọng chia đều cho từng tàu và tất cả đều đến cùng thời điểm, khi đến tất cả tải trọng sẽ được lấy ra khỏi mỗi tàu và được đối chiếu so với nguyên bản. Sự nhân đôi tải trọng là bình thường với spread spectrum khi dữ liệu truyền đến bị lỗi.

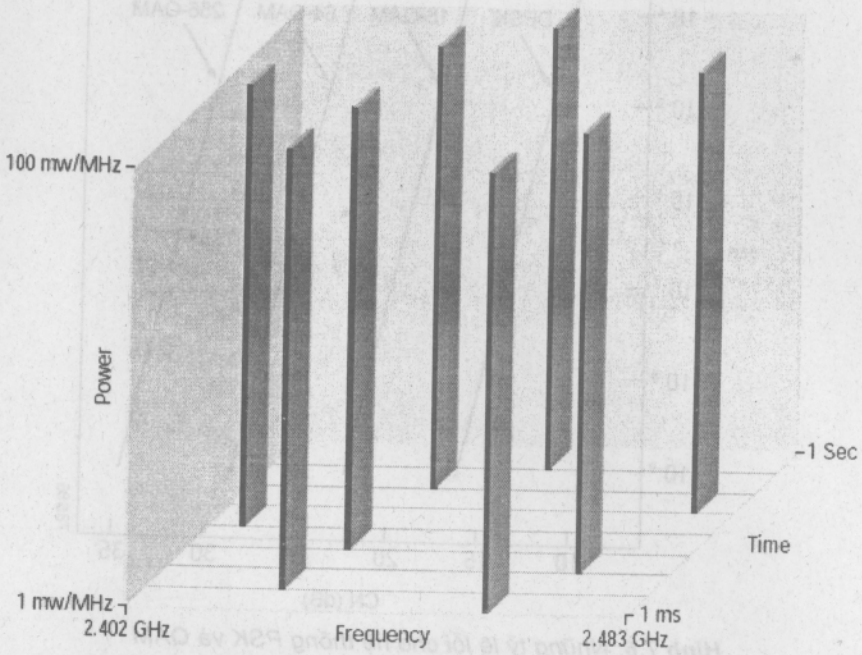
DSSS cung cấp 11 kênh chồng lên nhau trong dải tần số 83 MHz tại phổ 2.4 GHz, trong 11 kênh này sẽ có 3 kênh không chồng lên nhau độ rộng

22 MHz xem hình trên. Độ rộng băng thông cùng với phương pháp điều biến tiên tiến dựa trên khoá mã gốc bù (CCK) của DSSS hỗ trợ tốc độ truyền dữ liệu lơn hơn điều biến FHSS.



Hình 7.4. Direct Sequencing

Phổ trải rộng nhảy tần (FREQUENCY HOPPING SPREAD SPECTRUM - FHSS) Trong kỹ thuật này, dữ liệu ban đầu không được mở rộng, những dữ liệu được truyền qua dải rộng các tần số thay đổi trong các khoảng thời gian chia theo giây. Cả đầu phát lẫn đầu nhận đồng bộ thay đổi tần số trong quá trình truyền để gây khó khăn cho đối tượng làm nhiễu tín hiệu trên đường truyền trong việc dò tìm tần số chính xác mà tín hiệu đó đang được truyền đi. Các tần số thay đổi được rút ra từ một bản mã máy phát lẫn nhận điều biến.

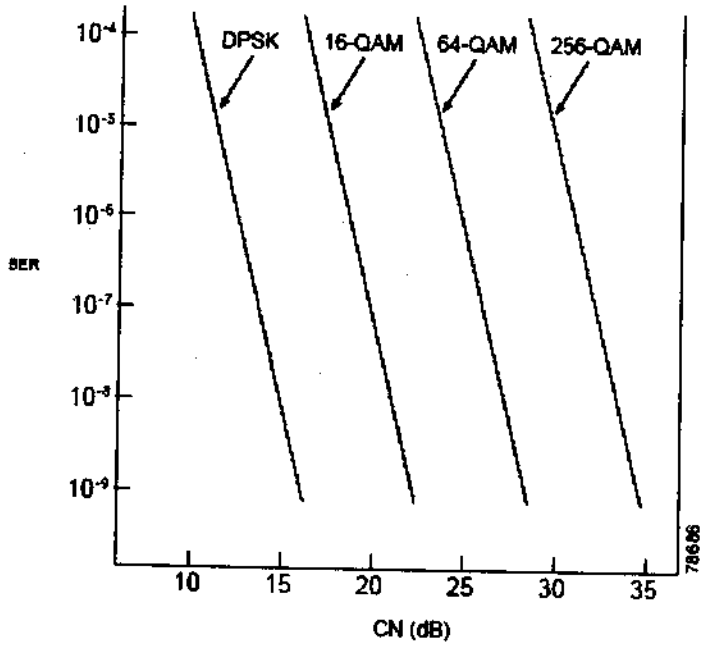


***Hình 7.5**. Nhảy tần*

Băng ISM 2.4 Ghz cho một phổ tần số 83 MHz. Cấu trúc nhảy tần số tạo ra các thang tần số sẵn sàng bằng việc tạo thành các kiểu dạng nhảy tần lên đến 79 dải tần số với độ rộng dải tần là 1 MHz (hình 7.5).

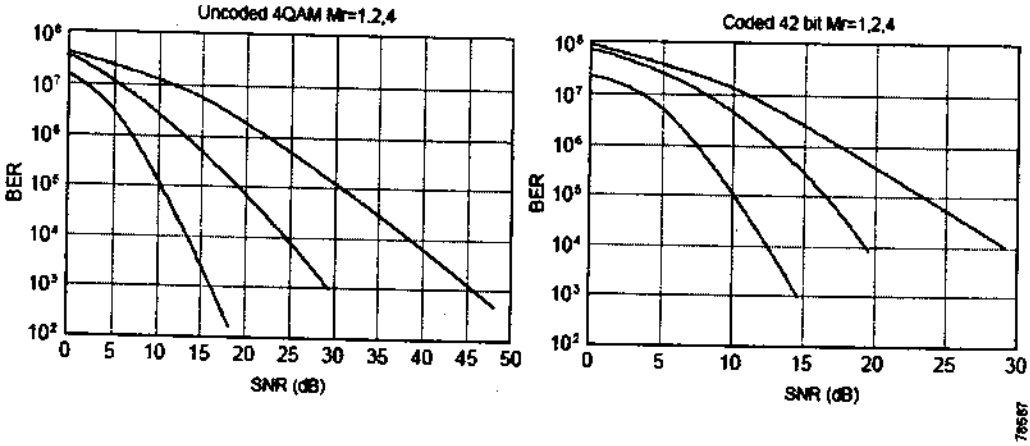
Rất nhiều hệ thống truyền thông sóng cực ngắn (vi ba) xác định hiện đại dựa trên phương pháp điều biến biên độ cầu phương (QAM). Những hệ thống này có nhiều mức độ phức tạp.

Những hệ thống đơn giản như khoá dịch pha (PSK) là khá đơn giản và dễ thực hiện bởi chúng có tốc độ dữ liệu thấp. Trong điều biến PSK, hình dạng của sóng được thay đổi không theo biên độ mà cũng chẳng ở tần số mà ở pha, những pha này được coi là dịch chuyển thời gian, ở trong khoá dịch pha nhị phân (BPSK), những pha của sóng hình sin bắt đầu từ 0 hoặc 1/4. Trong điều biến BPSK, chỉ một bit được truyền trên 1 vòng (gọi là ký hiệu). Trong những phối hợp điều biên phức tạp hơn, hơn 1 bit được truyền trên 1 ký hiệu. Kết hợp điều biến QPSK là tương tự với BPSK. Mặc dù vậy, thay vì chỉ hai trạng thái pha riêng biệt thì QPSK sử dụng 4 (0, 1/2, 1, 3/2), mang hai bit trên một ký hiệu. Khi bốn mức biên độ kết hợp với bốn mức pha ta có 16-QAM, trong 16-QAM, 2 bit được mã hoá trên sự đổi pha, và 2 bits được mã hoá trên đổi biên độ, và dễ dàng tính được tổng là 4 bits trên ký hiệu.



Hình 7.6. Những tỷ lệ lỗi cho hệ thống PSK và QAM

Trong hình 7.6 mỗi một pha duy nhất được đặt cách nhau ở hai góc I và Q. Góc quay cho biết pha và khoảng cách từ tâm điểm cho ra biên độ. Sự gần đúng điều biến này có thể mở rộng ra tới 64-QAM và 256 –QAM hoặc cao hơn. Thông qua 64-QAM là hai sản phẩm băng thông rộng dây và không dây, 256-QAM cũng đã được kiểm tra. Mật độ trong QAM cao hơn, tỷ lệ nhiễu tín hiệu cao hơn phải được bảo đảm để đáp ứng tỷ lệ lỗi bit (BER) như yêu cầu.



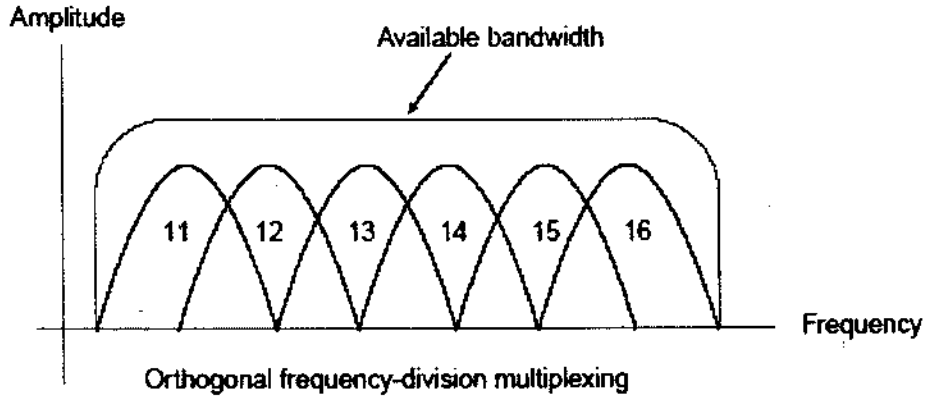
Hình 7.7. BER Dòng dữ liệu mã hoá và không mã hoá chống lại nhiễu tín hiệu BER

Code division multiple access (CDMA) được sử dụng để cho cùng xuất hiện đồng thời nhiều đường truyền. Mỗi dòng dữ liệu được nhân lên với mã nhiễu giả ngẫu nhiên (PN code). Mọi người sử dụng hệ thống CDMA sử dụng chung một dải tần số, mỗi tín hiệu được trải rộng ra, và sắp xết theo tầng và nó trải rộng bằng việc sử dụng mã trải rộng trong cùng một khe thời gian. Tín hiệu truyền được phục hồi bằng việc sử dụng mã PN.

FHHS: với cấu trúc FHHS, tàu sẽ rời trong các yêu cầu khác nhau, có nghĩa rằng không có sự tuần tự từ tàu 1 đến tàu N. Trong hệ thống FHHS tốt nhất, những đoàn tàu hoạt động trong nhiều không được gửi ra lần nữa cho đến khi nhiễu bị triệt tiêu. Trong hệ thống FHHS, những tần số xác định (kênh) được ngăn lại cho đến khi nhiễu bị triệt tiêu.

Nhiễu thường gây ảnh hưởng không chỉ 1 kênh tại 1 thời diểm, bởi vậy hệ thống DSSS gây ra mất nhiều dữ liệu hơn. Hệ thống FHSS tạo bước nhảy giữa những kênh trong chuỗi không tuần tự. Hệ thống FHSS tốt nhất điều chỉnh sự lựa chọn kênh sao cho những kênh nhiễu cao được chặn lại khi xác nhận vượt qua ngưỡng tỷ lệ lỗi bit.

FDM: Trong hệ thống dồn theo tần số (Frequency – division multiplexing – FDM), băng thông có sẵn được chia vào trong các sóng mang đa dữ liệu. Dữ liệu được truyền và rồi chia nằm trong các sóng mang con này. Bởi vì mỗi một sóng mang được coi như độc lập với nhau, nên dải tần số guard được đặt quanh nó. Trong một vài hệ thống FDM, hơn 50% băng thông có sẵn là không sử dụng. Trong hầu hết hệ thống FDM, khi các sóng mang con để không, băng thông của chúng không chia sẻ cho các sóng mang con khác.

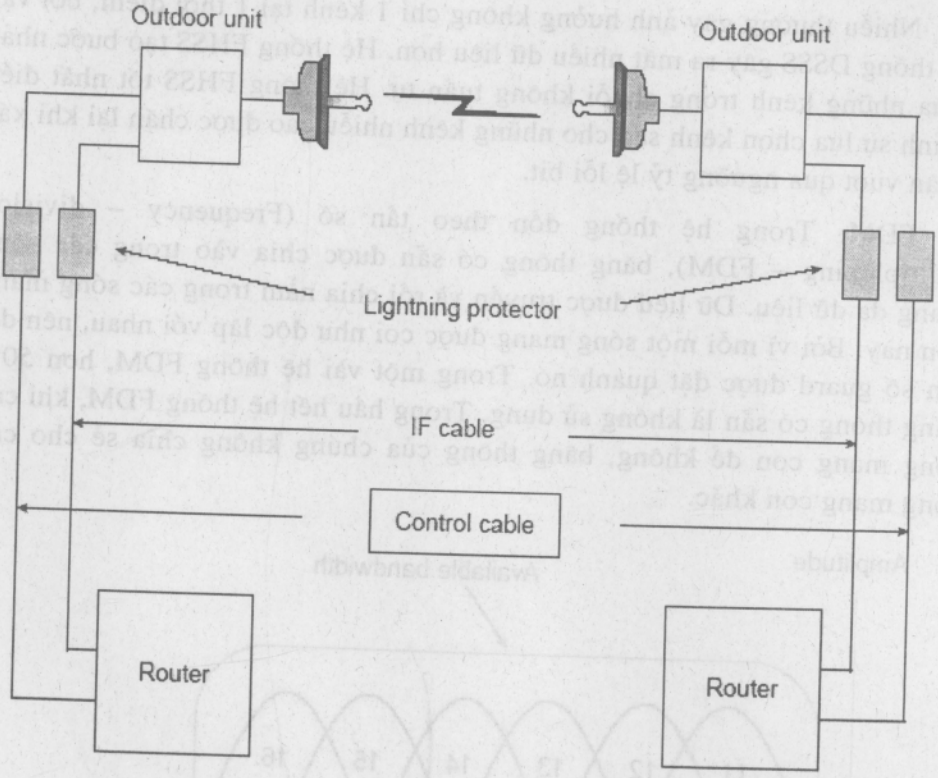


Hình 7.8. Một ví dụ về OFDM tone

OFDM (hình 7.8): nhiều sóng mang (hoặc tone) được chia dữ liệu kéo dài từ bên này sang bên kia của phổ, gần giống với FDM, trong hệ thống

OFDM, mỗi tone được coi như là giao thoa với những tone ngay kề bên, không cần yêu cầu băng gard. Bởi OFDM được lắp ghép bởi nhiều các tone băng hẹp, nhiễu băng hẹp sẽ chỉ làm giảm một phần nhỏ của tín hiệu và không ảnh hưởng hoặc ảnh hưởng ít đến thành phần của tần số.

Hệ thống OFDM sử dụng truyền loạt của dữ liệu để giảm mức tối thiểu ISI gây ra bởi sự chậm trải rộng. Dữ liệu được truyền theo dạng truyền loạt, với mỗi truyền loạt gồm có một tiền tố tuần hoàn của ký hiệu dữ liệu. Ví dụ tín hiệu OFDM chiếm dải tần số 6 MHz tạo ra được 512 sóng mang độc lập, mỗi một sóng mang sẽ mang ký hiệu QA trên một truyền loạt. Cho mỗi ký hiệu tuần hoàn, tổng 576 ký hiệu được truyền chỉ bởi 512 ký hiệu QAM trên 1 truyền loạt.



Hình 7.9. Công nghệ phổ

7.3. CHUẨN 802.11

7.3.1. CHUẨN CƠ SỞ 802.11

Chuẩn Ethernet không dây đầu tiên, IEEE 802.11, đã được chấp nhận vào năm 1997. Chuẩn này cung cấp 3 lớp vật chất (PHY) đạc điểm kỹ thuật

bao gồm tia hồng ngoại, 1-2 Mbps tần số quang phổ trải rộng và 1-2 Mbps trình tự điều khiển phổ trải rộng nhảy tần (frequency hopping spread spectrum FHSS) and 1-2 Mbps direct sequence spread spectrum (DSSS)) trong 2.3 GHz ISM band.

7.3.2. CHUẨN 802.11A

Chuẩn 802.11a hoạt động trong phạm vi 5GHz và cho phép tốc độ đạt đến 54Mbps. Dải tần số 5GHz ngày càng được sử dụng nhiều mục đích, nên ngày càng hẹp và băng thông ở đây sử dụng rộng hơn so với băng thông ở dải tần 2.4 GHz. Tuy nhiên, 802.11a không được chấp nhận như là một chuẩn WiFi, 802.11a sử dụng một lược đồ điều biến nhận biết như dồn theo tần số trực giao (orthogonal frequency-division multiplexing (OFDM)) chống lại FHSS và DSSS. Phần lớn sản phẩm 802.11a không tương thích với sản phẩm 802.11b hoặc 802.11g.

7.3.3. CHUẨN 802.11B

Chuẩn 802.11b hoạt động trong phạm vi dải tần là 2.4GHz và tốc độ truyền dữ liệu là 11Mbps, 802.11b là chuẩn thực tế cho công nghệ Wifi bởi vì nó rất hữu ích và giá thành hợp lý. Mặc dù chậm hơn 802.11a, nhưng 802.11b đã đạt được tốc độ dịch vụ 10BaseT Ethernet. 802.11b sử dụng DSSS và bổ sung mã khóa mã bù (complementary code keying - CCK). 802.11b được chứng nhận bởi IEEE vào năm 1999, cho phép các thiết bị đạt được tốc độ truyền dữ liệu lên đến 11 Mbps hoặc 33 Mbps khi 3 kênh không chồng nhau đồng thời cùng hoạt động.

7.3.4. CHUẨN 802.11G

Chuẩn IEEE 802.11g xây dựng cho mạng LAN không dây hoạt động tại tần số 2.4 GHz với tốc độ truyền dữ liệu lên đến 54 Mbps được chính thức phê duyệt vào ngày 11 tháng 7 năm 2003. Với tốc độ đạt 54 Mbps giúp chuẩn 802.11g có thể so sánh được với chuẩn 802.11a hoạt động ở băng tần 5 GHz, chuẩn 802.11g thiết kế có khả năng tương thích lùi về chuẩn 802.11b. Điều này giúp các thiết bị hoạt động theo chuẩn 802.11b sẽ hoạt động được đồng thời với các thiết bị chuẩn 802.11g giống như trong chuyển mạch sử dụng công nghệ autosensing per port chuyển tốc độ tự động giữa 10Base-T và 100Base-TX.

7.3.4.1. Sơ lược về chuẩn 802.11g

Chuẩn WLAN IEEE 802.11g có thể được xem như là sự giao nhau giữa hai chuẩn 802.11a và 802.11b. Giống như chuẩn 802.11b, 802.11g hoạt động ở băng phổ tần số radio 2.4 GHz. Một yêu cầu bắt buộc quan trọng của chuẩn 802.11g là khả năng tương thích lùi về chuẩn 802.11b, điều này

đảm bảo cho việc những thiết bị đã xây dựng trên chuẩn 802.11b hoạt động được trên hệ thống chuẩn mới 802.11g, giúp chúng ta không cần phải thay thế toàn bộ thiết bị khi đã có sẵn một mạng không dây chuẩn 802.11b và nâng cấp lên chuẩn 802.11g. Giống chuẩn 802.11a, 802.11g sử dụng dồn theo tần số trực giao (Orthogonal Frequency Division Multiplexing - OFDM) cho việc truyền dữ liệu. OFDM có hiệu quả truyền hơn là truyền DSSS, được sử dụng bởi chuẩn 802.11b. Với cả hai dạng điều chế khác nhau trên, chuẩn 802.11g (như 802.11a) hỗ trợ tốc độ truyền tốt hơn chuẩn 802.11b. Theo bảng 7.4 dưới đây, chuẩn 802.11g sử dụng kết hợp hai truyền OFDM và DSSS hỗ trợ tốc độ truyền lơn hơn nhiều.

Bảng 7.4. Bảng tốc độ dữ liệu dạng truyền và lược đồ điều chế

Tốc độ truyền dữ liệu (Mbps)	Dạng truyền	Lược đồ điều chế
54	OFDM	64 QAM
48	OFDM	64 QAM
36	OFDM	16 QAM
24	OFDM	16 QAM
18	OFDM	QPSK1
12	OFDM	QPSK
11	DSSS	CCK2
9	OFDM	BPSK3
6	DSSS	CCK
5.5	DSSS	QPSK
2	DSSS	QPSK
1	DSSS	BPSK

7.3.4.2. Hiệu suất và công suất của chuẩn 802.11g

Với công nghệ WLAN, công suất mạng của sản phẩm tăng mạnh mẽ thông lượng lên nhiều lần nhờ vào số các kênh có sẵn. Như đã nói ở phần trên, giống như 802.11b, các thiết bị chuẩn 802.11g giới hạn không quá 3 kênh không lặp lại. Thông lượng của mạng 802.11g phụ thuộc vào số các môi trường truyền và hệ số ứng dụng, và quan trọng là mạng 802.11g hỗ trợ các thiết bị chuẩn 802.11b. Mạng 802.11 sử dụng đa truy nhập cảm nhận sóng mang với sự tránh xung đột (CSMA/CA), phương pháp truy nhập môi trường truyền giống như chia sẻ Ethernet. Thiết bị mạng 802.11b, chia sẻ cùng băng thông 2.4GHz giống như chuẩn 802.11b, không thể tự nhận dạng truyền OFDM. Mặc dù thiết bị 802.11b có thể cảm nhận nhiễu tại băng 2.4 GHz thông qua khả năng đánh giá kênh sạch (CCA), chúng không thể giải mã bất cứ dữ liệu, quản lý hoặc gói điều khiển được gửi thông qua OFDM. Để thực hiện việc này, chuẩn 802.11g bao gồm cấu trúc bảo vệ cung cấp khả năng cùng tồn tại và lùi.

Bảng 7.5. Bảng so sánh thông lượng giữa các chuẩn 802.11a, 802.11b, 802.11g

Chuẩn	Tốc độ dữ liệu Mbps	Thông lượng gần đúng (Mbps)	Tỷ lệ phần trăm so với thông lượng của 802.11b
802.11b	11	6	100%
802.11g (có mặt của thiết bị chuẩn 802.11b)	54	8	133%
802.11g (không có mặt của thiết bị chuẩn 802.11b)	54	22	367%
802.11a	54	25	417%

Khi các ứng dụng khác 802.11b kết hợp với điểm truy cập theo chuẩn 802.11g, điểm truy cập sẽ thay đổi cơ cấu bảo vệ gọi yêu cầu gửi và xoá gửi (RTS/CTS). Cơ cấu ban đầu của địa chỉ "vấn đề điểm ẩn" (điều kiện ở đó 2 trạm khách không thấy nhau do khoảng cách có thể bảo đảm kết nối tới điểm truy cập). Khi RTS/CTS được hiện lên, các trạm khách phải yêu cầu truy cập đầu tiên tới môi trường truyền từ điểm truy cập với một thông báo CTS. Trạm khách sẽ kiểm chế truy cập vào môi trường truyền và truyền dữ liệu của chúng cho đến khi điểm truy cập trả lời bằng một thông báo CTS. Khi nhận được tín hiệu RTS ban đầu từ nhiều trạm khách, lệnh CTS được hiểu là "lệnh không gửi", bắt chúng phải kiểm chế truy cập vào môi trường truyền.

Khi mạng 802.11g hoạt động không có trạm khách chuẩn 802.11b. thông lượng của mạng sẽ đạt gần như 802.11a, còn khi có trạm khách chuẩn 802.11b thông tượng của mạng sẽ giảm đi đáng kể, bảng dưới đây cho thấy so sách thông lượng giữa chuẩn 802.11a, 802.11b, 802.11g.

Do chuẩn 802.11g hoạt động trên cùng dải tần 2.4 Ghz với chuẩn 802.11b nên có thể sử dụng chung một hệ thống ăngten ở dải tần 2.4 Ghz. còn chuẩn 802.11a thì hoạt động ở giải tần 5 Ghz nên sẽ sử dụng loại ăngten khác.

Bảng 7.5 so sánh phạm vi hoạt động trong các môi trường văn phòng qua các tường dạng khối.

7.3.4.3. Những lý do sử dụng chuẩn 802.11g

Chuẩn 802.11g quan tâm đến hoạt động của 802.11b, với những khả năng như tương thích lùi cộng với kết hợp với truyền OFDM hiệu suất cao, là những yếu tố chính dẫn đến việc lựa chọn sử dụng chúng, ngoài ra việc tích hợp phương tiện mã hoá RC4 cung cấp bảo mật WEP và WPA và chuẩn mã hoá AES không làm giảm hiệu suất, hỗ trợ chuẩn 802.11i và FIPS-140.

Bảng 7.6. Công suất mạng cho các chuẩn 802.11a, 802.11b, 802.11g

Tốc độ dữ liệu (Mbps)	802.11a (40mW với ăngten diversity patch có độ khuếch đại 6dBi)	802.11g (30mW với ăngten diversity dipole có độ khuếch đại 2.2dBi)	802.11b (100mW với ăngten diversity dipole có độ khuếch đại 2.2dBi)
54	13m	27m	
48	15m	29m	
36	19m	30m	
24	26m	42m	
18	33m	54m	
12	39m	64m	
11		48m	48m
9	45m	76m	
6	50m	91m	
5.5		67m	67m
2		82m	82m
1		124m	124m

Chuẩn 802.11g hoạt động trên băng tần 2.4 Ghz, đây là băng tần ít sử dụng cho các ứng dụng khác nên khả năng nhiễu là ít, tốc độ chuẩn 802.11g hiện nay đã đạt được 108 Mbps. Tương thích lùi xuống chuẩn 802.11b, một chuẩn mạng không dây đã được phổ biến trước đó khá lâu, làm giảm kinh phí thay mới hoàn toàn khi triển khai mạng 802.11g.

Tất cả điều trên cho chúng ta thấy ưu điểm khi lựa chọn chuẩn 802.11g cho hệ thống mạng không dây của chúng ta.

7.3.5. CHUẨN 802.11H

Chuẩn này được dùng ở châu Âu, hoạt động trên dải tần 5 Ghz. Nó cung cấp tính năng sự lựa chọn kênh động và điều khiển công suất truyền dẫn TPC, nhằm tránh can nhiễu. Ở châu Âu người ta chủ yếu sử dụng thông tin vệ tinh, nên phần lớn các quốc gia ở đây chỉ sử dụng Wireless LAN trong nhà (Indoor).

7.4. CÁC THIẾT BỊ MẠNG KHÔNG DÂY

7.4.1. ĐIỂM TRUY CẬP

Điểm truy cập (Access Point - AP) hoạt động trong phổ tần số cụ thể và sử dụng các chuẩn 802.11 (802.11a, 802.11b, 802.11g) với kỹ thuật điều

Bảng 7.6. Công suất mạng cho các chuẩn 802.11a, 802.11b, 802.11g

Tốc độ dữ liệu (Mbps)	802.11a (40mW với ăngten diversity patch có độ khuếch đại 6dBi)	802.11g (30mW với ăngten diversity dipole có độ khuếch đại 2.2dBi)	802.11b (100mW với ăngten diversity dipole có độ khuếch đại 2.2dBi)
54	13m	27m	
48	15m	29m	
36	19m	30m	
24	26m	42m	
18	33m	54m	
12	39m	64m	
11		48m	48m
9	45m	76m	
6	50m	91m	
5.5		67m	67m
2		82m	82m
1		124m	124m

Chuẩn 802.11g hoạt động trên băng tần 2.4 Ghz, đây là băng tần ít sử dụng cho các ứng dụng khác nên khả năng nhiễu là ít, tốc độ chuẩn 802.11g hiện nay đã đạt được 108 Mbps. Tương thích lùi xuống chuẩn 802.11b, một chuẩn mạng không dây đã được phổ biến trước đó khá lâu, làm giảm kinh phí thay mới hoàn toàn khi triển khai mạng 802.11g.

Tất cả điều trên cho chúng ta thấy ưu điểm khi lựa chọn chuẩn 802.11g cho hệ thống mạng không dây của chúng ta.

7.3.5. CHUẨN 802.11H

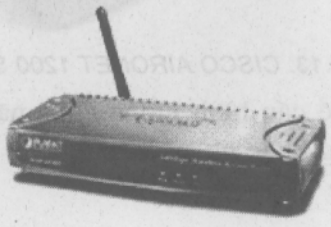
Chuẩn này được dùng ở châu Âu, hoạt động trên dải tần 5 Ghz. Nó cung cấp tính năng sự lựa chọn kênh động và điều khiển công suất truyền dẫn TPC, nhằm tránh can nhiễu. Ở châu Âu người ta chủ yếu sử dụng thông tin vệ tinh, nên phần lớn các quốc gia ở đây chỉ sử dụng Wireless LAN trong nhà (Indoor).

7.4. CÁC THIẾT BỊ MẠNG KHÔNG DÂY

7.4.1. ĐIỂM TRUY CẬP

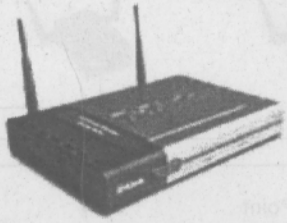
Điểm truy cập (Access Point - AP) hoạt động trong phổ tần số cụ thể và sử dụng các chuẩn 802.11 (802.11a, 802.11b, 802.11g) với kỹ thuật điều

chế cụ thể. Nó thông báo cho các trạm khách biết về sự có mặt của nó và xác nhận và kết nối các trạm khách không dây vào hệ thống mạng không dây. Điểm truy cập cũng cho phép trạm làm việc sử dụng các tài nguyên trên mạng có dây. Trong mỗi AP bao giờ cũng phải có hệ thống ăngten hoạt động trên các dải tần xác định. Trong các AP bao giờ cũng có các chức năng đi kèm như bảo mật, chế độ kết nối... Dưới đây là một vài hình ảnh về AP của các hãng mạng nổi tiếng trên thế giới.

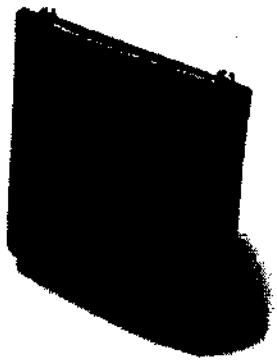


Hình 7.10. *Thiết bị AP của hãng Planet*

Hình 7.11. *Access Point của hãng LinkSys*



Hình 7.12. *AP của hãng Dlink*

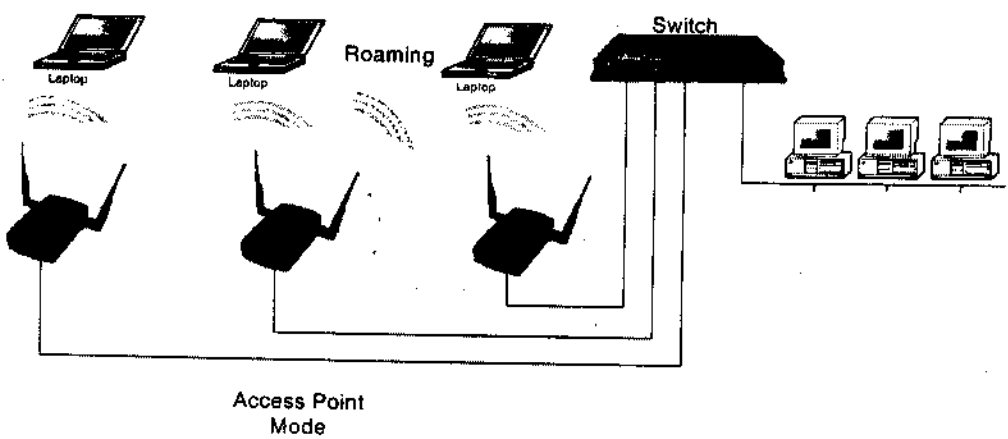


Hình 7.13. CISCO AIRONET 1200 SERIES AP

Access Point có thể cấu hình nhiều chức năng khác nhau phù hợp với nhiều mục đích sử dụng khác nhau như: Access Point, Access Point client, Bridge, Multiple Bridge

7.4.1.1. Access Point Mode

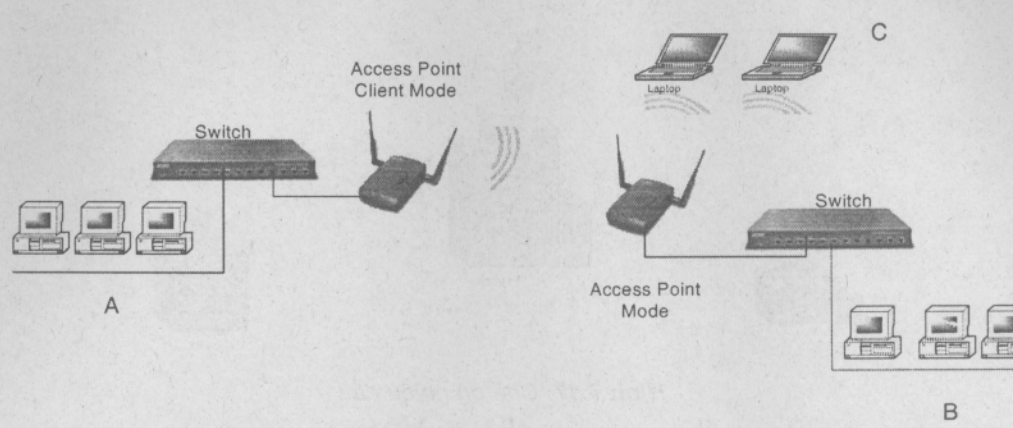
Ở chế độ này khi client di chuyển hoặc chuyển tới một vị trí khác nó sẽ được roaming để liên với các client khác thông qua Access Point gần nhất. Có hai thông số để nhận dạng giữa Access Point và client khi roaming đó là nhận dạng dịch vụ SSID (Service Set Identification) và giao thức mã hóa WEP (Wired Equivalent Protocol)



Hình 7.14. Ở chế độ AP

7.4.1.2. Access Point Client Mode

Trường hợp này khi cấu hình một Access Point là client thì nó sẽ đóng vai trò như Client đối với Access Point khác nào đó., ví dụ như hình 7.13.

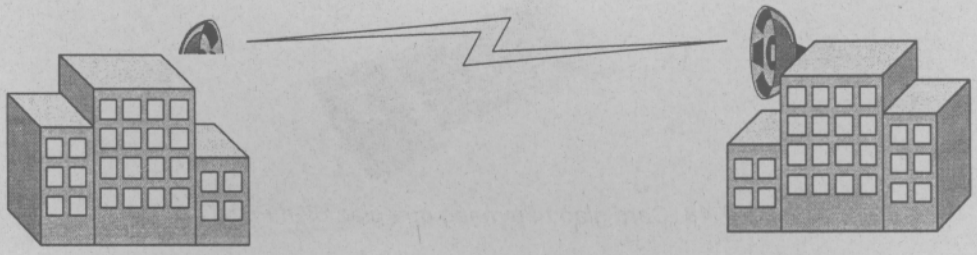


Hình 7.15. Ở chế độ AP client

Trường hợp này áp dụng khi một số máy ở địa điểm A được đặt cố định rất khó đi dây đến đó và Access Point nối vào mạng A này sẽ được cấu hình như một client của Access Point Mode phía B và C.

7.4.1.3. Access Point Brigde

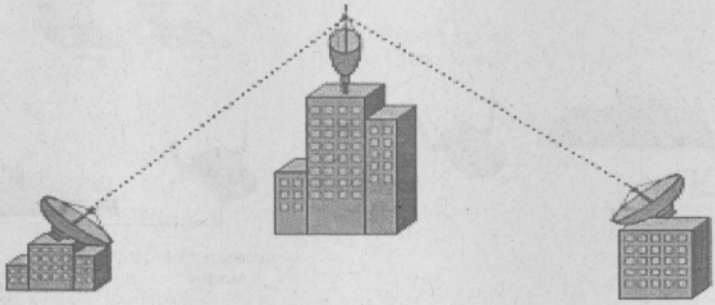
Trường hợp này thường áp dụng khi có 2 mạng LAN ở 2 tòa nhà cách xa nhau muốn nối với nhau thông qua Access Point. Trường hợp này ăngten của Access Point thường là ăngten đẳng hướng. Khi tính toán nếu cần phải dùng loại Access Point có cắm thêm ăngten thì nên dùng ăngten định hướng (thường đặt ngoài trời) và chú ý phải có biện pháp chống sét cho ăngten.



Hình 7.16. Ở chế độ Brigde

7.4.1.4. Access Point Multi Brigde

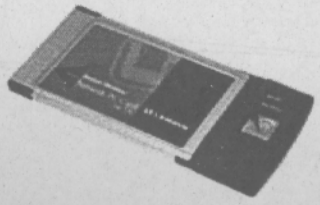
Trường hợp có ít nhất 3 mạng LAN ở 3 tòa nhà cách xa nhau muốn nối mạng với nhau thông qua Access Point, khi đó ta sẽ nhóm các mạng này thành một domain,dùng ăngten định hướng như trường hợp Access Point Bridge. Nếu như giữa hai tòa nhà nào đó mà có vật cản (chẳng hạn một tòa nhà khác cao hơn) thì ta phải định hướng lại ăngten, tăng thêm trạm chuyển tiếp.



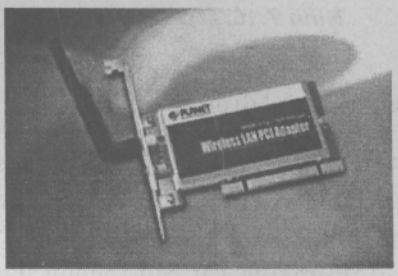
Hình 7.17. Chế độ nhiều cầu

7.4.2. CARD GIAO TIẾP MẠNG HOẶC BỘ ĐIỀU HỢP MÁY KHÁCH

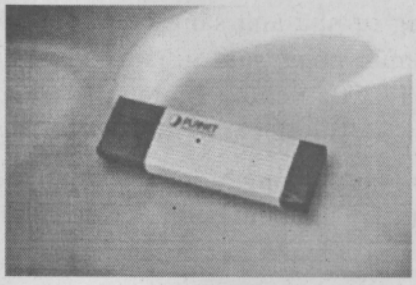
Một máy tính cá nhân hoặc trạm làm việc sử dụng card giao tiếp mạng không dây để kết nối vào mạng không dây. Card giao tiếp mạng sẽ quét phổ tần số có sẵn để kết nối và kết hợp nó tới AP hoặc các điểm trạm không dây khác (ở chế độ Ad-hoc). Card giao tiếp mạng sẽ hoạt động trên nền hệ điều hành thông qua phần mềm điều khiển, các hệ điều hành hỗ trợ hiện nay là các phần mềm Microsoft Windows 98 trở lên, UNIX, LINUX, đồng thời có các chuẩn giao tiếp như USB, PCI, PCMCIA. Dưới đây là hình ảnh của một số card giao tiếp mạng không dây.



Hình 7.18. Card giao tiếp mạng qua giao diện PCMCIA



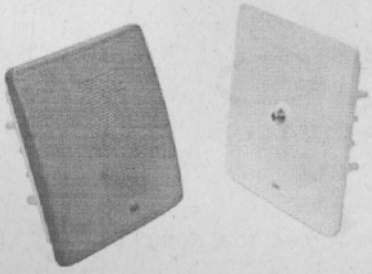
Hình 7.19. Card giao tiếp mạng qua giao diện PCI



***Hình 7.20**. Card giao tiếp mạng qua giao diện USB*

7.4.3. CẦU (BRIDGE)

Cầu không dây được dùng để nối nhiều mạng LAN (cả mạng không dây và có dây) tại mức tầng điều khiển truy cập đường truyền (Media Access Control – MAC). Được sử dụng trong việc kết nối không dây giữa toàn nhà với toà nhà, cầu không dây có thể tăng khoảng cách hơn so với AP nhờ có các loại ăngten và các bộ khuếch đại tín hiệu, ngày nay, hầu hết các hãng sản xuất mạng không dây đã kết hợp hai tính năng AP và Bridge vào trong cùng một thiết bị.



***Hình 7.21**. Cisco Aironet 1400 Series Wireless Bridge*

7.4.4. ĂNGTEN

7.4.4.1. Đặc tính và độ khuếch đại ăngten

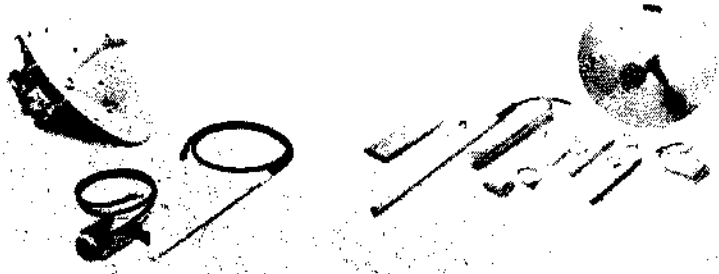
Hệ thống ăngten không dây có 3 đặc tính cơ bản là độ khuếch đại, hướng và trạng thái phân cực. Độ khuếch đại được xác định qua độ tăng công suất. Hướng là kiểu mô hình truyền. Bộ phản hồi tập trung và tăng cường chùm tia sáng trong một hướng riêng, tương tự như ăngten chảo dạng parabol làm đối với nguồn sóng radio trong hệ thống radio.

Độ khuếch đại ăngten xác định bằng dB là tỷ lệ giữa 2 giá trị, độ khuếch đại ăngten là đặc thù khuếch đại của ăngten đẳng hướng và lưỡng cực. Tỷ lệ ăngten đẳng hướng với ăngten lý thuyết giản đồ hướng sóng ba

chiều đồng nhất (tương tự như ánh sáng bóng đèn không có phản xạ). dBi sử dụng để so sánh mức công suất giữa ăngten thực tế và ăngten đẳng hướng theo lý thuyết. FCC lấy chính ăngten đẳng hướng làm ăngten để các ăngten khác so sánh, nên dB trên chính nó sẽ là không.

Không như ăngten đẳng hướng, ăngten lưỡng cực là loại ăngten thực tế sử dụng trong các hệ thống ăngten cho mạng không dây phổ dụng hiện nay. ĂNGTEN lưỡng cực có giản đồ hướng sóng khác với ăngten đẳng hướng. Giản đồ hướng sóng lưỡng cực là 360 độ trong mặt phẳng nằm ngang và 75 độ trong mặt phẳng nằm dọc(Giả định ăngten lưỡng cực nằm dọc) và giống với dạng hình ống xuyến. Vì chùm tia là tập trung mảnh, ăngten lưỡng cực có độ khuếch đại trên ăngten đẳng hướng là 2.11 dB trong mặt phẳng nằm ngang. Ăngten lưỡng cực có độ khuếch đại 2.14 dBi (khi so sánh với ăngten đẳng hướng.

Một vài ăngten có độ khuếch đại là tỷ lệ so sánh với ăngten lưỡng cực, được biểu thị bằng dBd và ăngten lưỡng cực có độ khuếch đại = 0dBd.



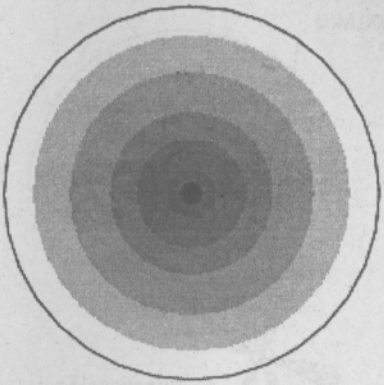
Hình 7.22. Các ăngten hoạt động tại tần số 5.8 GHz và 2.4 GHz

7.4.4.2. Các dạng ăngten

AP và Bridge sử dụng các sản phẩm ăngten tại tần số 2.4 GHz, 5 GHz. Mọi ăngten đang sử dụng hiện nay đều được sự tán thành của FCC. Mỗi dạng ăngten sẽ có khả năng bao phủ khác nhau. Khi có độ khuếch đại ăngten tăng lên vùng bao phủ của ăngten sẽ đạt trạng thái cân bằng. Thông thường độ khuếch đại ăngten sẽ cho ra khoảng cách bao phủ lơn hơn, những chỉ trong các hướng xác định. Giản đồ hướng sóng ở hình dưới đây sẽ giúp chỉ ra vùng bao phủ của các dạng ăng ten: vô hướng, ăngten định hướng loại Yagi và patch.

ĂNGTEN vô hướng

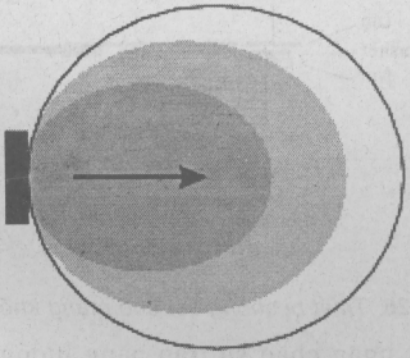
ĂNGTEN vô hướng được thiết kế để cung cấp giản đồ hướng sóng 360 độ. Dạng ăngten này được sử dụng khi sóng phải bao phủ mọi hướng từ ăng ten. Chuẩn 2.14 dBi là một dạng của ăngten vô hướng.



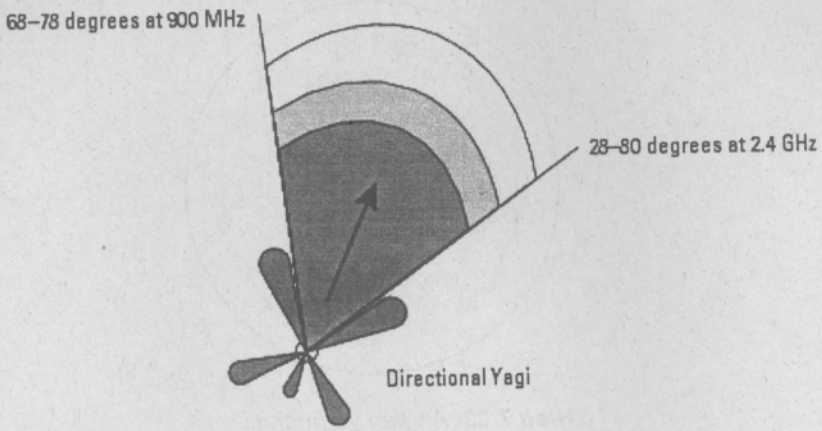
Hình 7.23. Ăngten vô hướng

Ăngten định hướng

Ăngten định hướng có nhiều hướng và hình dạng khác nhau. Ăngten không cấp thêm bất cứ công suất nào cho tín hiệu; Nó chỉ đơn giản là định hướng lại nguồn năng lượng nhận được từ bộ phát. Bằng việc định hướng lại nguồn năng lượng, nó tạo nên ảnh hưởng qua việc cung cấp thêm năng lượng trên một hướng, và giảm năng lượng trong các hướng khác. Khi độ khuếch đại của ăngten định hướng tăng, góc phát xạ thường giảm, làm tăng khoảng cách phủ sóng, nhưng góc phủ sóng lại giảm. Ăngten định hướng bao gồm ăngten yagi, ăngten patch và ăngten chảo parabôn. Chảo parabôn có đường năng lượng sóng radio rất hẹp và người lắp đặt phải định vị rất chính xác các hướng ăngten đấu vào với nhau.



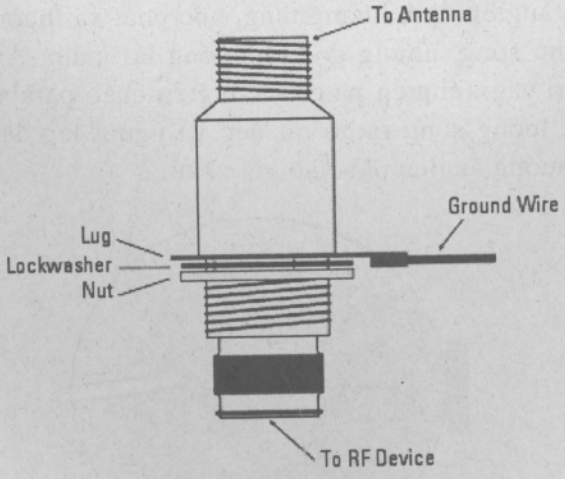
Hình 7.24. Ăngten định hướng loại Patch



Hình 7.25. ĂNGTEN định hướng loại Yagi

Chống sét đánh

Khi sử dụng các ăngten đấu nối ngoài trời, hệ thống mạng không dây có thể bị hỏng do các xung điện có biên độ lớn gây nên. Các thiết bị chống sét đánh được sản xuất để chống lại việc trên



Hình 7.26. Thiết bị chống sét cho mạng không dây

Thiết bị chống sét ngăn chặn sự tràn năng lượng từ thiết bị phát sóng radio bằng đường rẽ nhánh có hiệu quả của thiết bị, sự tràn năng lượng được giới hạn nhỏ hơn 50V trong khoảng 0.0000001 giây (100 nanô giây). Một cú sét đánh tiêu biểu thường diễn ra trong 0.000002 giây (2 micro giây). IEEE đã được công nhận ngăn chặn trong khoảng thời gian 0.000008 giây (8 micro giây).

Trên thực tế thiết bị mạng không dây thường có các số dB tương ứng với số dB trên lý thuyết đã được xác định. Công suất truyền và độ nhạy thu được thể hiện trong lý thuyết ở dạng dBm, ở đây m có nghĩa là 1 mW. Do vậy, 0dBm sẽ bằng 1 mW, 3 dBm sẽ bằng 2 mW, 6 dBm sẽ bằng 4mW, và cứ thế. Bảng dưới đây là các giá trị phổ biến của mW và dBm.

Bảng 7.7. Các giá trị phổ biến của mW và dBm

dBm	mW	dBm	mW
0 dBm	1 mW	0 dBm	1 mW
1 dBm	1.25 mW	-1 dBm	0.8 mW
3 dBm	2 mW	-3 dBm	0.5 mW
6 dBm	4 mW	-6 dBm	0.25 mW
7 dBm	5 mW	-7 dBm	0.20 mW
10 dBm	10 mW	-10 dBm	0.10 mW
12 dBm	16 mW	-12 dBm	0.06 mW
13 dBm	20 mW	-13 dBm	0.05 mW
15 dBm	32 mW	-15 dBm	0.03 mW
17 dBm	50 mW	-17 dBm	0.02 mw
20 dBm	100 mW	-20 dBm	0.01 mW
30 dBm	1000 mW (1 W)	-30 dBm	0.001 mW
40 dBm	10,000 mW (10 W)	-40 dBm	0.0001 mW

Vùng Fresnel

Vùng Fresnel là vùng dạng hình Elip có đường bao như dạng trên hình vẽ, dạng hình elip biến đổi phụ thuộc vào chiều dài đường tín hiệu và tần số của tín hiệu. Vùng Fresnel có thể tính toán được và có thể tạo thành bảng kê khai khi thiết kế đường kết nối mạng không dây (hình 7.27). Khi có bất cứ vật cản nào nằm trong vung Fresnel đều gây ra ảnh hưởng suy giảm đối với đường truyền mạng không dây, để trách suy hao trên đường truyền, hai điểm phải truyền sóng radio trong tầm nhìn thẳng, trong vùng Fresnel không có vật cản.

Ta biết bán kính miền Fresnel được tính bằng công thức:

$$r = \frac{1}{2}\sqrt{\lambda d}$$

Trong đó: r là bán kính miền Fresnel thứ nhất;

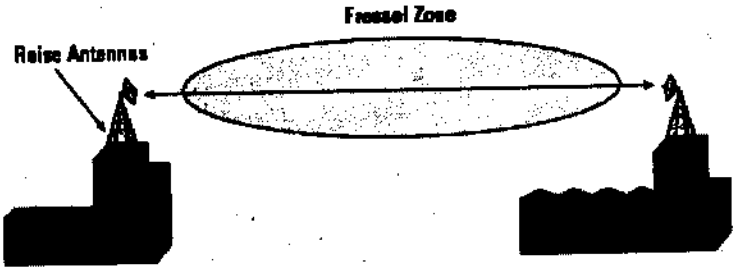
λ là bước sóng, $\lambda = \frac{c}{f}$

d là khoảng cách giữa hai điểm.

Ví dụ: với d = 1km ta có bán kính miền Fresnel sẽ là:

$$r = \frac{1}{2}\sqrt{\frac{3.10^8.10^3}{24.10^8}} = 5,59m$$

Tương tự với d=10km thì r = 16,67m



Hình 2.27. Vùng Fresnel

Dựa vào yêu cầu của vùng Fresnel và line-of-sight, bảng 7.8 cung cấp hướng dẫn về chiều cao của ăngten cho nhiều khoảng cách khác nhau.

Bảng 7.8. Chỉ dẫn đối với yêu cầu độ cao đối với ăngten 2.4 Ghz

Wireless Link Distance (miles)	Approx. Value "F" (60% Fresnel Zone) ft. at 2.4 GHz	Approx. Value "C" (Earth Curvature)	Value "H" (mounting Ht.) Ft. with No Obstructions
1	10	3	13
5	30	5	35
10	44	13	57
15	55	28	83
20	65	50	115
25	72	78	150

7.5. PHƯƠNG PHÁP LẮP ĐẶT

7.5.1. CÁC MODE HOẠT ĐỘNG

7.5.1.2. Ad —hoc Mode

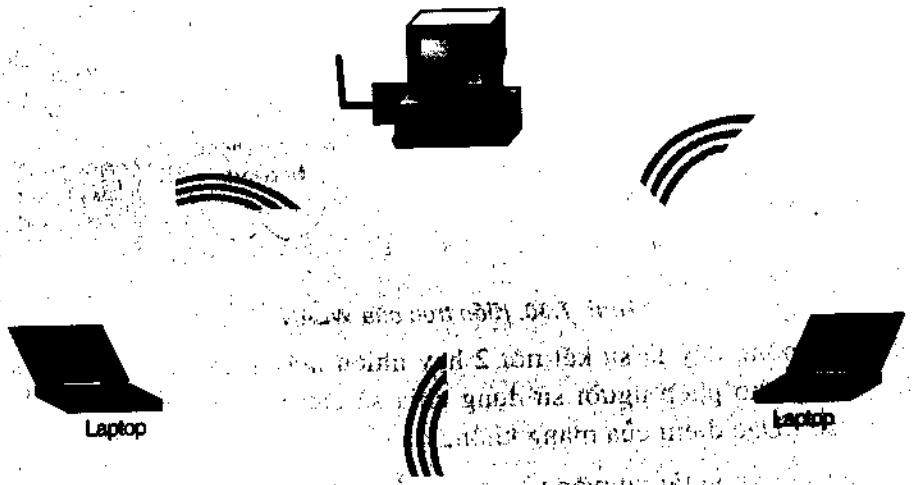
Cho phép các thiết bị không dây truy nhập điểm tới điểm hoặc nhiều điểm với nhau mà không cần AccessPoint (tức là không cần nối với mạng LAN kết nối dây truyền thống). Ở mode này tốc độ truyền dữ liệu cao, hiệu quả và tin cậy, thường áp dụng trong các trường hợp sau :

Các địa điểm khó đi dây như: di tích lịch sử, các tòa nhà cổ, những khu vực mới mở.

Những địa điểm làm việc tạm thời trong thời gian ngắn như: khu triển lãm, công trình xây dựng.

Người sử dụng SOHO (Small Office Home Office – mạng gia đình và văn phòng nhỏ).

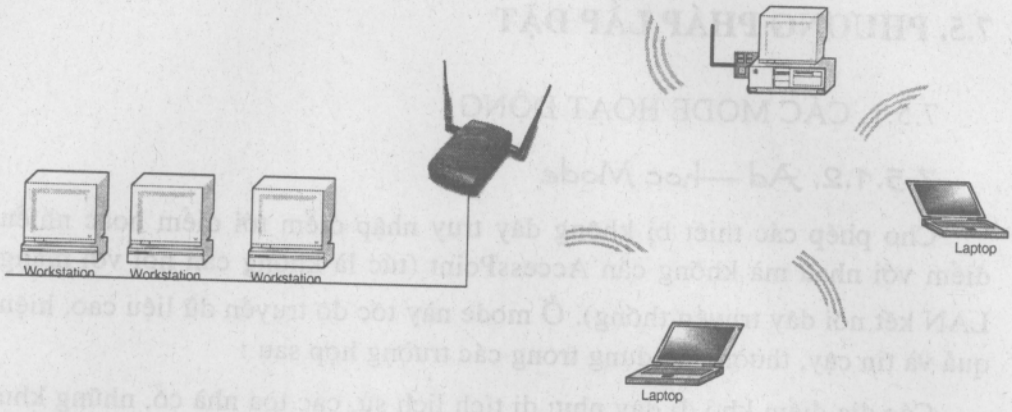
Nơi yêu cầu bảo mật cao.



Hình 7.28. Mô hình ad-hoc

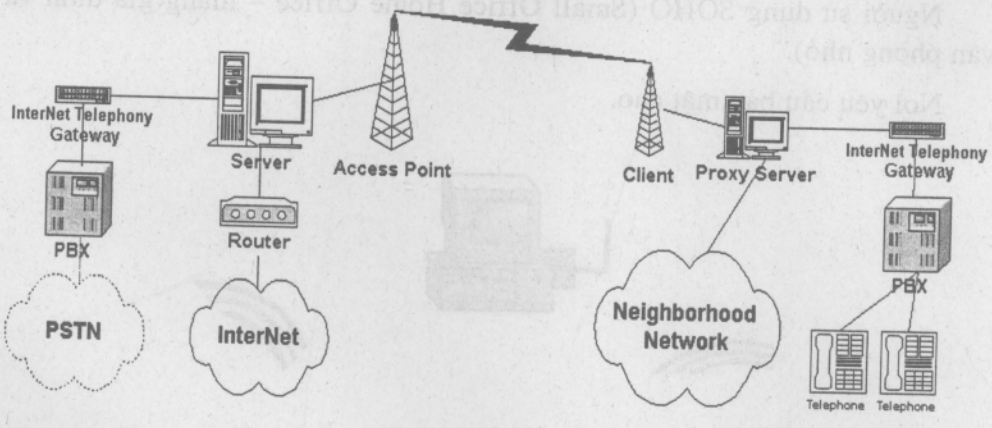
7.5.1.2. Infrastructure Mode

Cho phép các thiết bị không dây truy nhập điểm tới điểm hoặc nhiều điểm với nhau đồng thời truy nhập với các thiết bị khác trên mạng LAN kết nối dây thông qua AccessPoint.



Hình 7.29. Mô hình Infrastructure

7.5.2. MẠNG KHÔNG DÂY HOẠT ĐỘNG NHƯ THẾ NÀO



Hình 7.30. Kiến trúc của WLAN

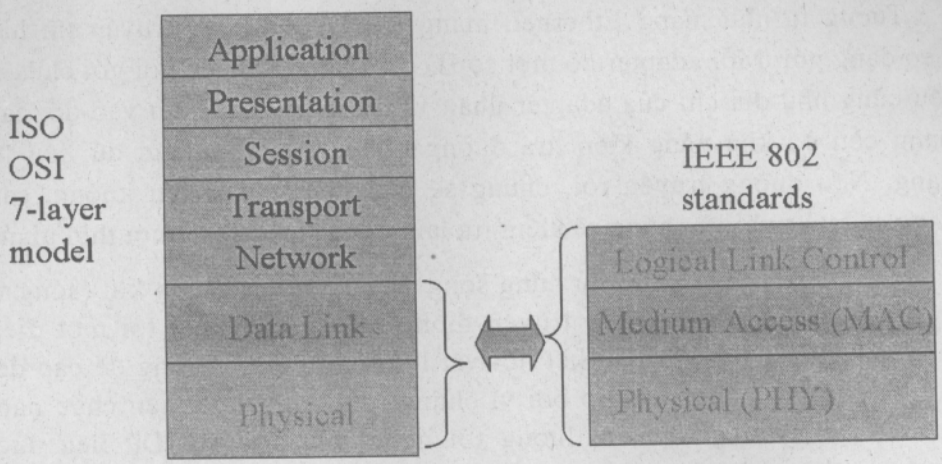
Mạng không dây là sự kết nối 2 hay nhiều máy tính qua tín hiệu sóng radio. Mạng cho phép người sử dụng chia sẻ các tập tin, máy in hay truy cập Internet. Đặc điểm của mạng không dây:

- Chia sẻ nguồn tài nguyên và truyền không cần dây.

- Cài đặt dễ dàng, tính ổn định cao nên thích hợp với sử dụng trong các gia đình cũng như ở công sở.

- Kết nối từ nhiều thiết bị khác nhau.

- Đắt hơn rất nhiều so với công nghệ mạng dây như Ethenet.



***Hình 7.31**. Chuẩn 802.11 trong mô hình OSI.*

Nếu bạn cần kết nối hai hay nhiều máy tính ở những nơi không thể sử dụng hoặc rất khó có thể sử dụng mạng cáp chuẩn thì mạng không dây sẽ đáp ứng được yêu cầu của bạn. Mỗi máy tính cá nhân được trang bị một thiết bị thu phát tín hiệu radio từ các máy tính khác trong mạng, gọi là bộ điều hợp mạng LAN không dây (wireless LAN adapter) hay là các card mạng LAN không dây. Bạn có thể tìm thấy các adapter được tích hợp bên trong hoặc là phụ kiện bên ngoài của các máy tính cá nhân và máy tính xách tay.

Trong khi các mạng LAN không dây hoạt động theo một nguyên lý chung thì tốc độ truyền dữ liệu và tần số sử dụng lại khác nhau, phụ thuộc vào các chuẩn như IEEE 802.11, IEEE 802.11b, OpenAir và HomeRF. Thật đáng tiếc là các chuẩn này lại không làm việc với nhau và do vậy tất cả các adapter trên cùng 1 mạng phải sử dụng cùng một chuẩn.

Các nhà cung cấp mạng LAN thường đưa ra mức truyền dữ liệu lớn nhất của các adapter. Với các card mạng sử dụng chuẩn 802.11, tốc độ truyền dữ liệu là 2Mbps cho cả hai phương pháp nhảy tần và phân đoạn trực tiếp. Với adapter sử dụng chuẩn OpenAir thì tốc độ truyền dữ liệu là 1.6Mbps theo phương pháp nhảy tần. Một chuẩn mới, HomeRF, có thể truyền cả tín hiệu thoại và dữ liệu với tốc độ 1.6Mbps cũng theo phương pháp trên. Bên cạnh đó, đối với các mạng LAN không dây, khi adapter sử dụng chuẩn mức cao IEE802.11b tốc độ còn có thể đạt tới 11Mbps theo giao thức phân đoạn trực tiếp.

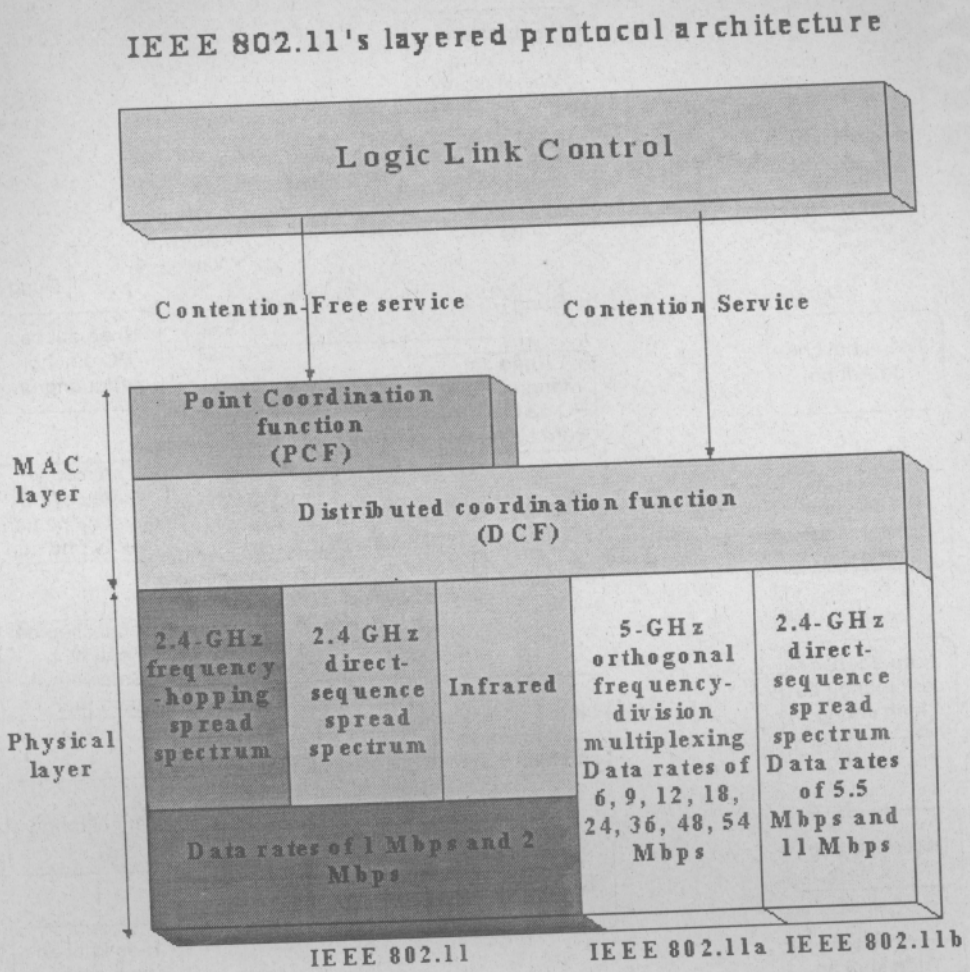
Tương tự như mạng Ethernet, mạng LAN không dây truyền tín hiệu theo dạng gói. Mỗi adapter có một số ID địa chỉ duy nhất. Mỗi gói chứa dữ liệu cũng như địa chỉ của adapter nhận và adapter gửi. Thêm vào đó, card mạng còn có khả năng kiểm tra đường truyền trước khi gửi dữ liệu lên mạng. Nếu đường truyền rỗi, chúng sẽ gửi dữ liệu đi. Nếu không, card mạng sẽ tạm nghỉ và chúng sẽ kiểm tra lại đường truyền sau một thời gian.

Mạng LAN không dây sử dụng sóng điện từ trong không khí (sóng vô tuyến và tia hồng ngoại) để truyền thông tin từ một điểm tới một điểm khác mà không dựa trên sự kết nối vật lý. Sóng radio thường đề cập đến như hãng truyền thông radio bởi vì chúng tuyệt đối thực hiện chức năng của việc chuyển giao năng lượng tới người nhận từ xa. Dữ liệu được truyền là thêm vào dựa trên hãng truyền thông radio vì đó nó có thể được lấy chính xác ở đầu thu, thường được đề cập đến như là sự điều biến của hãng truyền thông bởi những thông tin đã được truyền. Một dữ liệu được thêm vào bên trên hãng truyền thông radio, tín hiệu radio chiếm nhiều hơn tín hiệu tần số, do đó tần số hoặc tốc độ bit của thông tin điều biến thêm vào hãng truyền thông.

Nhiều hãng truyền thông radio có thể tồn tại trong cùng một khoảng trống ở cùng một thời gian mà không gây phiền phức với những cái khác nếu sóng radio được truyền trên một trên một tần số radio khác.Để lấy dữ liệu, một người nhận radio chọn 1 tần số radio trong khi loại tất cả các tín hiệu radio trên các tần số khác nhau.

Trong cấu hình đặc trưng WLAN, việc truyền/nhận thiết bị, gọi là điểm truy cập, kết nối tới mạng có dây từ một vị trí cố định dùng chuẩn cáp Ethernet. Ở một mức tối thiểu nào đó, điểm truy cập nhận, bộ nhớ trung gian, truyền dữ liệu giữa WLAN và thiết bị phụ thuộc vào mạng có dây. Một tín hiệu truy cập có thể hỗ trợ một nhóm nhỏ người dùng và có chức năng trong phạm vi vùng nhỏ hơn 100 hoặc lớn hơn 100 feet. Điểm truy cập thường được lắp đặt cao nhưng về cơ bản thì có thể lắp đặt mọi nơi nhưng trên thực tế chỉ ở một chừng mực nào đó.

Người dùng cuối truy cập WLAN thông qua adapters LAN không dây, adapters thực hiện giống như PC card trong notebook máy tính, hoặc dùng ISA hoặc PCI adapters trên desktop máy tính... WLAN adapters cung cấp một thiết bị ghép tương thích giữa hệ thống hoạt động mạng client (NOS – network operating system) và airwaves (via an ăngten).



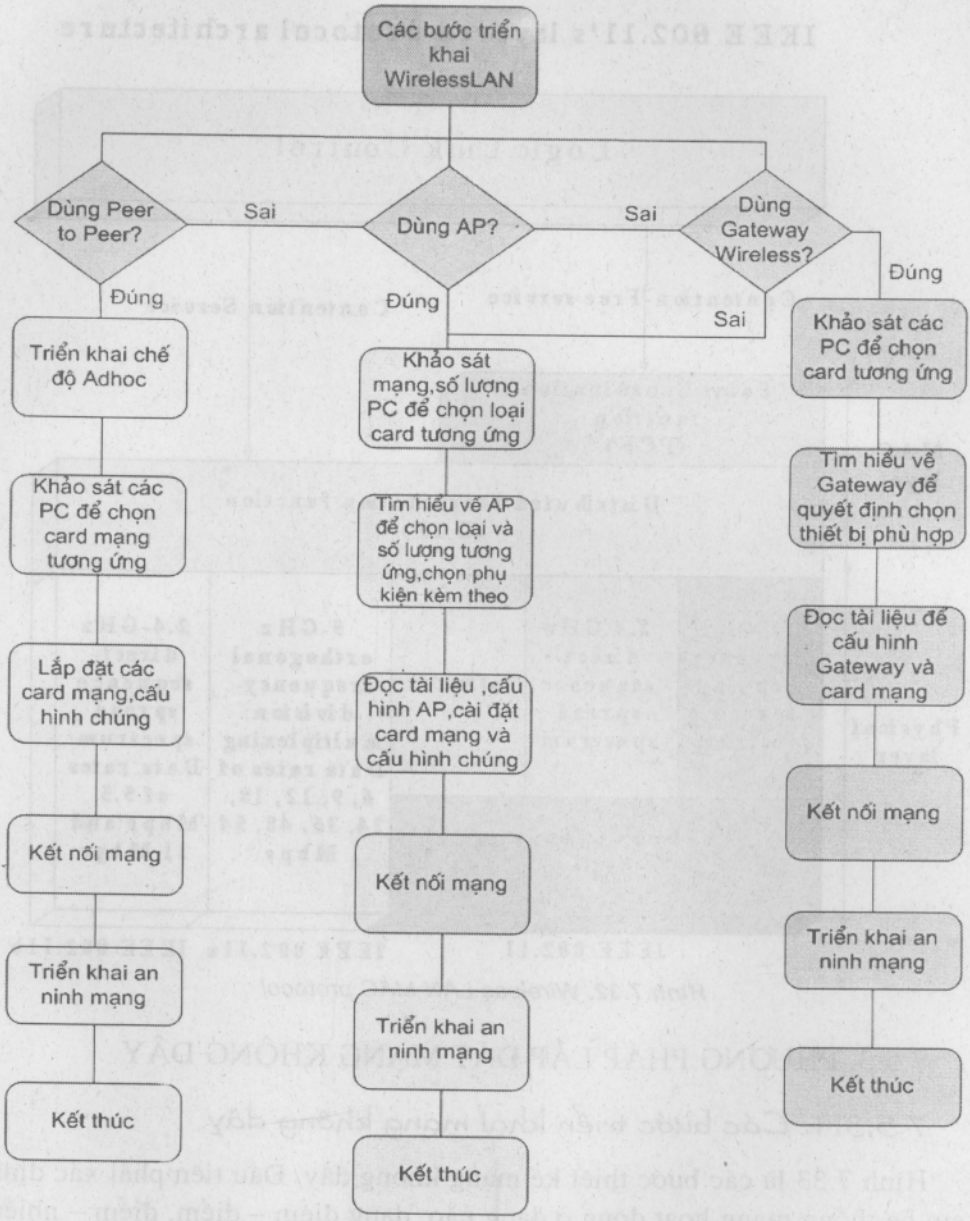
Hình 7.32. Wireless LAN MAC protocol

7.5.3. PHƯƠNG PHÁP LẮP ĐẶT MẠNG KHÔNG DÂY

7.5.3.1. Các bước triển khai mạng không dây

Hình 7.33 là các bước thiết kế mạng không dây. Đầu tiên phải xác định xem hệ thống mạng hoạt động ở dạng nào, dạng điểm – điểm, điểm – nhiều điểm, phải dùng gateway mạng không dây hay khổng?

Trong trường hợp sử dụng mạng điểm tới điểm (toàn máy tính không dây kết nối mạng với nhau), tất cả các thiết bị mạng không dây phải thiết lập hoạt động Ad-Hoc, xác định các giao diện card mạng không dây cho các máy tính trạm, thiết lập cấu hình cho card mạng không dây và kết nối vào mạng, triển khai an ninh mạng (hình 7.34).



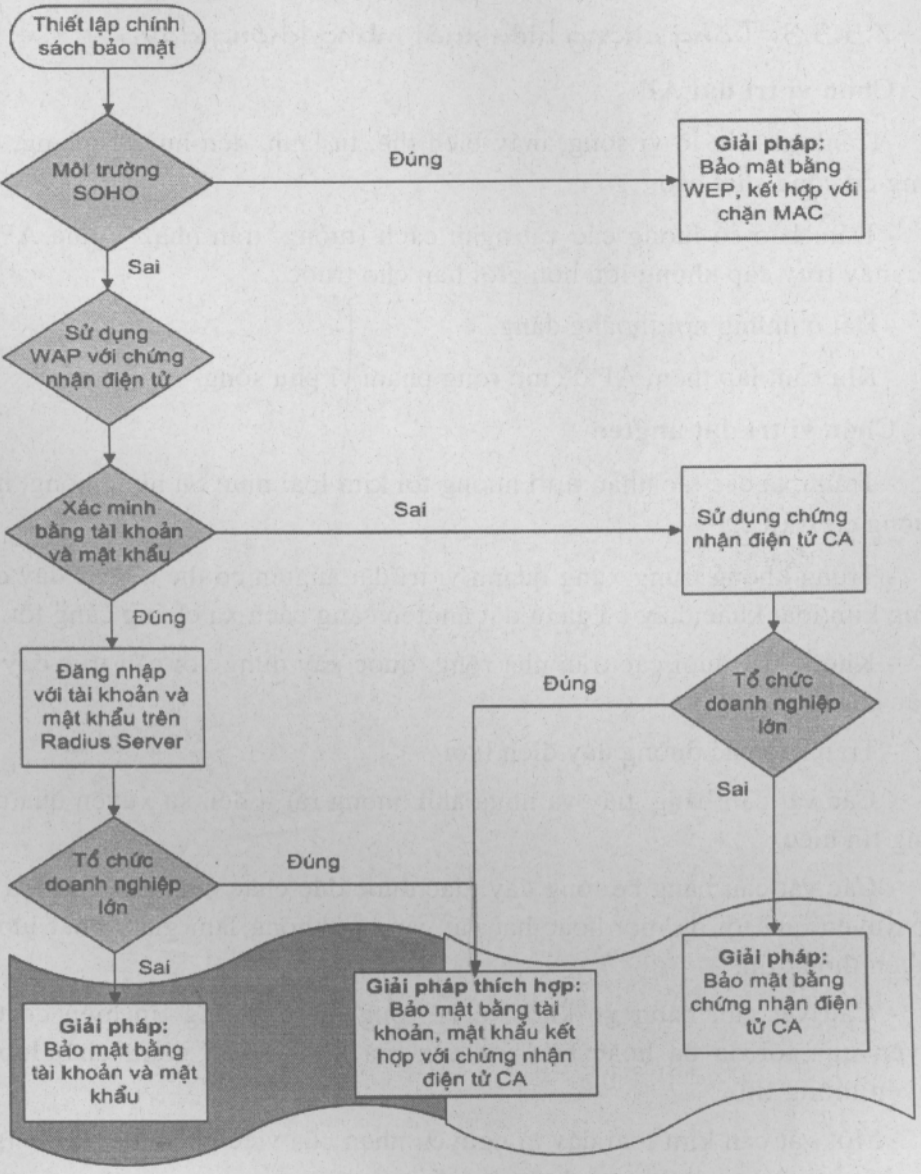
***Hình 7.33.** Các bước thiết kế mạng không dây*

Trong trường hợp sử dụng mạng điểm tới nhiều điểm (mạng không dây kết nối với mạng có dây, hoặc toàn mạng máy tính không dây kết hợp thông qua AP), khảo sát hệ thống mạng không dây cần thiết lập là mạng LAN – LAN qua không dây (thiết lập chế độ hoạt động cho AP ở chế độ Bridge) hoặc mạng Không dây kết hợp với có dây (thiết lập chế độ AP ở AP mode) để lựa chọn đúng AP, tiếp theo khảo sát giao diện các card mạng không dây cần dùng cho mạng, khảo sát số lượng máy trạm không dây cần kết nối vào

mạng, diện tích cần phủ sóng để xác định số lượng AP, tiếp theo thiết lập cấu hình AP và card giao tiếp mạng cho hoạt động ở mode Infrastructure, và cấu hình AP ở mode tương ứng, kết nối mạng và triển khai an ninh.

Trong trường hợp cần triển khai mạng không dây có sử dụng AP làm định tuyến ra Internet, phải chọn AP có tính năng định tuyến (router) và các bước tiếp theo sẽ giống như ở phần sử dụng cho mạng điểm và nhiều điểm.

7.5.3.2. Triển khai bảo mật



***Hình 7.34**. Các bước triển khai bảo mật*

Hình 7.34 thể hiện các bước triển khai bảo mật, bước đầu tiên phải xác nhận đây là mạng không dây cho ứng dụng mạng nhỏ, hay mạng cho các doanh nghiệp, nếu là mạng nhỏ ta chỉ cần sử dụng các tính năng có sẵn trong AP như WEP kết hợp với chặn địa chỉ MAC. Trong trường hợp xác định đó là mạng dành cho các doanh nghiệp ta sử dụng chứng nhận địa chỉ và WEP, sau đó đến đăng nhập tài khoản và mật khẩu trên Radius Server, nếu muốn tăng cường tính bảo mật, ta có thể kết hợp thêm vào bảo mật bằng tài khoản, mật khẩu kết hợp với chứng nhận điện tử CA.

7.5.3.3. Tăng cường hiệu xuất mạng không dây

Chọn vị trí đặt AP

-Tránh xa các lò vi sóng, máy biến thế, tủ lạnh, đèn huỳnh quang, các động cơ công suất cao,...

- Đảm bảo số lượng các vật ngăn cách (tường, trần nhà,..) giữa AP và các máy truy cập không lớn hơn giới hạn cho trước.

- Đặt ở những nơi thoáng đãng.

- Khi cần, lắp thêm AP để mở rộng phạm vi phủ sóng.

Chọn vị trí đặt ăngten

- Tránh xa các tác nhân ảnh hưởng tới kim loại như: Sự nung nóng, môi trường có Axit,...

- Trong không trung xung quanh vị trí đặt ăngten có thể có các dây dẫn bằng kim loại khác, hãy cố gắng đặt ăngten càng cách xa chúng càng tốt.

- Không đặt dưới các trần nhà rộng, được xây dựng với cấu trúc dày và chắc chắn.

- Tránh xa các đường dây điện lưới

- Các vật cản bằng giấy và nhựa ảnh hưởng rất ít đến sự xuyên qua của sóng tín hiệu.

- Các vật cản bằng bê tông dày, đặc được đúc chắc chắn thì tín hiệu có thể xuyên qua tối đa một hoặc hai vật cản mà không làm giảm chất lượng truyền thông tin.

- Các vật cản bằng gỗ khối và bê tông bình thường tín hiệu có thể xuyên qua tối đa ba hoặc bốn vật cản mà không làm giảm chất lượng truyền thông tin.

- Một vật cản kim loại dày là nguyên nhân của việc phản xạ tín hiệu, vì thế chất lượng truyền không được đảm bảo.

Lắp đặt ăngten xa lò vi sóng và điện thoại không dây có tần số 2 Ghz. Các thứ đó có thể là nguyên nhân làm tín hiệu nhiễu bởi vì chúng hoạt động ở khoảng tần số giống như các thiết bị trong ăngten bạn đã kết nối.

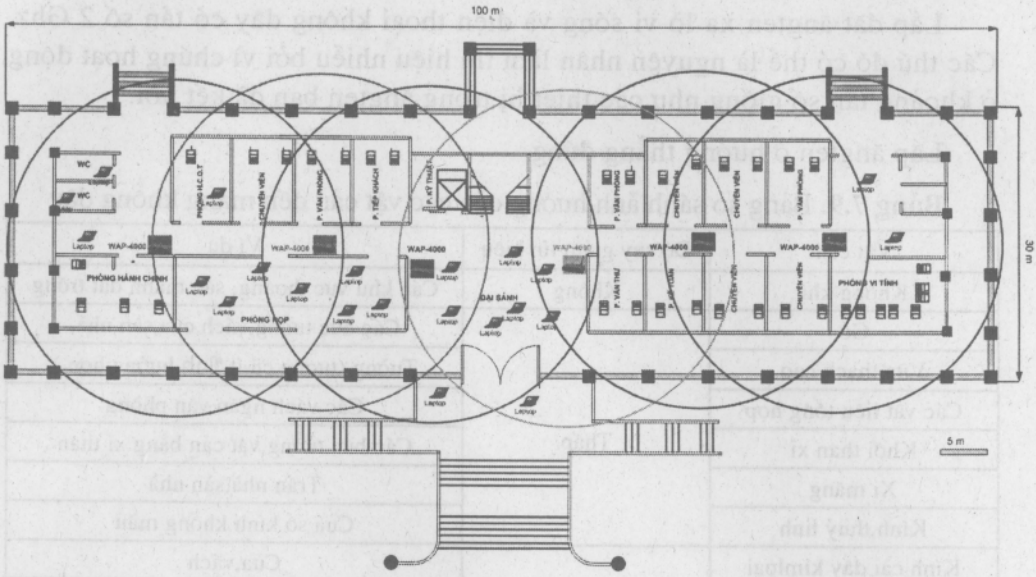
Lắp ăngten ở hướng thẳng đứng.

Bảng 7.9. Bảng so sánh ảnh hưởng của các vật cản đến mạng không dây

Vật cản	Độ suy giảm tín hiệu	Ví dụ
Không khí	Không	Các khu vực thoáng, sân,mành đất trống
Gỗ	Thấp	Các bức tường,vách,cửa,sàn nhà,
Vữa,thạch cao		Tường (tương cũ ít ¶nh hưởng hơn)
Các vật liệu tổng hợp		Các vách ngăn văn phòng
Khối than xỉ		Các bức tường,vật cản bằng xỉ than
Xi măng		Trần nhà,sàn nhà
Kính,thuỷ tinh		Cửa sổ kính không màu
Kính cài dây kimloại	Trung bình	Cửa,vách
Cơ thể người		Nhóm người đang làm việc
Nước		Tường ẩm,bể nuôi cá, các chất hữu cơ
Gạch		Các bức tường,trần nhà
Đá hoa, đá cẩm thạch		Các bức tường, sàn nhà
Gốm	Cao	Trần nhà,nền nhà
Giấy		Kho giấy hoặc các cuộn giấy
Bê tông		Cột trụ,các bức tường kiên cố
Kính chống đạn		Khu vực được bảo vệ
Bạc	Rất cao	Mạ bạc, gương tráng thuỷ
Kim loại		Các vật dụng bằng kim loại

7.5.3.4. Cách xác định số AP dựa trên số lượng các thiết bị cần sử dụng mạng không dây và diện tích phủ sóng

Đầu tiên ta phải khảo sát thật kỹ số lượng AP và sơ đồ mặt bằng khu vực phủ sóng mạng không dây. Ta biết bán kính vùng phủ sóng tối đa đối với 1 AP trong khoảng 30m (trong điều kiện lý tưởng không có vật cản), ta sẽ vẽ các đường tròn làm sao cho chu vi các hình tròn phải bao phủ hết khu vực cần phủ sóng, số các vòng tròn chính là số các AP cần sử dụng, thông thường để đảm bảo tốc độ truyền cho các trạm làm việc, một AP chỉ nên hỗ trợ cho từ 20 đến 30 thiết bị không dây, khi tăng số lượng thiết bị lên ta cần tăng số AP theo. Trên thực tế tất cả các nơi cần phủ sóng bao giờ cũng có nhiều yếu tố là vật cản làm suy hao đường truyền, chính vì vậy bán kính phủ sóng của các AP cũng thay đổi theo chiều hướng giảm và với mỗi địa điểm cần xác định chính xác bán kinh phủ sóng của AP bằng kiểm tra thực tế.



Hình 7.35. Sơ đồ lắp đặt AP

7.5.3.5. Tính toán lựa chọn đúng các thiết bị trong mạng không dây

Công suất đầu ra của một số AP

Ta có công thức tính công suất đầu ra như sau

$$P_{dBm} = 10 \times \text{Log } P_{mw} \quad (7.1)$$

Ví dụ P_{mw} =50mW

Ta có

$$P_{dBm} = 10 \text{x} \log 50 = 16.9897 \text{dBm}$$

Tổn hao trên cáp

Ta có công thức tính tổn hao trên cáp như sau:

$$P_{dB} = 10 \text{x } \log(P_{out}/P_{in}) \quad (7.2)$$

Ví dụ nếu nửa mức công suất tổn hao suy giảm là (P_{out}/P_{in}=2)

Thì mức tổn hao tính theo dB sẽ là

$$P_{dB} = 10 \times \text{Log } (2) = 3\text{dB}$$

Hệ số khuếch đại ăngten

Độ khuếch đại ăngten = 10xLog(cường độ bức xạ theo hướng cho trước/ cường độ bức xạ đẳng hướng) (7.3)

Tổn hao không gian tự do (tổn hao do khoảng cách)

Tổn hao không gian tự do = 32,4 + 20 log F(Mhz) + 20 log R(km) (7.4)

Trong đó:

F là tần số tính bằng Mhz

R là khoảng cách giữa ăngten phát và ăngten thu

Tại tần số 2,4 Ghz thì công thức trên là 100 + 20 log R(km)

Ví dụ cụ thể : R = 10 km thì tổn hao không gian tự do là 100 + 20 log 10 =120 dB.

Độ nhạy thu

Bảng 7.10. Bảng độ nhạy thu trong các chuẩn 802.11b, 802.11g tại các tốc độ

Độ nhạy thu (dBm)	802.11b	802.11g
11 b	1M : -88 2M : -87 5.5M: -85 11M : -82	1M : -88 2M : -87 5.5M: -85 11M : -82
11 b+	22M: -80	
11 g		6/9/12/18/24/36/48/54Mbps: -88/-86/-85/-83/-80/-76/-71/-68

Các thông số trên áp dụng với PER=8%.

Phương pháp tính toán các yếu tố trong mạng không dây

Ví dụ 1:

Hai Access Point chuẩn 802.11b, tốc độ truyền đặt ở 1 Mbps,khoảng cách 1 km, không gian mở, AP có công suất đầu ra là 17dB.

Ta tạo ra bảng liệt kê giống như bảng 7.11 Trong đó các phần sẽ được tính bởi các công thức từ 7.1, 7.2, 7.3, 7.4 và từ bảng độ nhạy thu. ta cộng tất cả các thành phần lại nếu thông số EIRP = tổng các thông số còn lại > 5 (thông thường EIRP mong muốn bằng 5 hoặc cao hơn vì phải dự trữ fading - sự thăng giáng tín hiệu tại điểm thu) là đảm bảo thoả mãn được các yêu cầu và mạng hoạt động tốt.

Bảng 7.11. Phương pháp tính các yếu tố trong mạng không dây cho ví dụ 1

Công suất đầu ra phía phát	17
Tổn hao trên cable phía phát	0
Khuếch đại tín hiệu trên ăngten phát	0
Suy hao tín hiệu trên đường truyền(suy hao khoảng cách)	- 100
Khuếch đại trên ăngten thu	0
Tổn hao trên cable phía thu	0
Độ nhạy thiết bị phía thu	- (- 88)
EIRP(Efffective Isotropic Radiated Power)	5 > 0

Ví dụ 2 :

Hai AP chuẩn 802.11g với công suất đầu ra = 13 dB, gắn thêm ăngten ngoài với độ khuếch đại 20 dBi tốc độ truyền dẫn đặt ở 54Mbps, tổn hao trên cable là 3,5, khoảng cách 5 km, không gian mở.

Bảng 7.12. Phương pháp tính các yếu tố trong mạng không dây

Công suất đầu ra phía phát	13.
Tổn hao trên cable phía phát	- 3,5
Khuếch đại tín hiệu trên ăngten phát	20
Suy hao tín hiệu trên đường truyền (suy hao khoảng cách)	- 114
Khuếch đại trên ăngten thu	20
Tổn hao trên cable phía thu	- 3,5
Độ nhạy thiết bị phía thu	- (- 68)
EIRP (Efffective Isotropic Radiated Power)	0

Kết quả trên cho thấy EIRP = 0, không đạt yêu cầu vì vậy ta có thể dùng ăngten có độ khuếch đại lớn hơn hoặc giảm tốc độ truyền của AP

Trên thực tế, khi gặp các trường hợp vùng Fresnel bị ảnh hưởng bởi các vật cản, nhiễu giao thoa của các sóng cùng tần số sẽ dẫn đến ảnh hưởng đến thông số EIRP vì vậy số này càng lớn hơn 5 càng tốt và để thực sự mạng có thể hoạt động tốt, cần phải kiểm tra trên thực tế.

7.6. VẤN ĐỀ BẢO MẬT

1. Vì sao cần bảo mật cho mạng không dây

Không như mạng có dây, mạng không dây là mạng lan truyền bằng sóng radio, bất cứ một người nào chỉ cần ở trong vùng phủ sóng của mạng là có thể truy cập vật lý vào hệ thống (tức là nhận và phát sóng). Chính vì vậy vấn đề bảo mật đối với mạng có dây đã là yếu tố quan trong thì nay càng quan trọng hơn đối với mạng không dây.

2. Các dạng tấn công qua mạng không dây :

- Unauthorized association to the AP (liên kết trái phép tới AP).
- Rogue APs (Lừa AP).
- Man-in-the-middle (Tấn công qua người trung gian).
- Eavesdropping.
- MAC Spoofing (Bắt trước địa chỉ MAC).
- Denial of Service (phủ nhận dịch vụ).

Unauthorized association to APs và rogue Access Points là vấn đề thời sự và chỉ xảy ra với mạng không dây. Eavesdropping, MAC Spoofing và Denial of Service được thấy cả trong mạng có dây. Hiểu biết về các dạng tấn công sẽ giúp người quản trị mạng đưa ra được những quyết sách đúng về bảo mật.

3 Các công nghệ bảo mật

Yêu cầu đầu tiên đối với bảo mật mạng bao gồm vùng điều khiển, đảm bảo bí mật cho người dùng, tính toàn vẹn của dữ liệu, và bảo vệ chống lại các kiểu tấn công đã biết. Để hoàn thành các yêu cầu trên, hệ thống mạng phải cung cấp các công nghệ thực hiện các chức năng sau (có thể là phần cứng hoặc phần mềm).

- Xác nhận (Authentication)
- Cho phép (Authorization)
- Sự tin cậy (Confidentiality)
- Toàn vẹn dữ liệu (Data Integrity)
- Khoá quản lý (Key management)
- Bảo vệ chống các tấn công đã biết như: MAC spoofing, man-in-the-middle attacks,...

Dưới đây là hiểu biết sơ lược về các chức năng trên.

4. Cơ cấu điều khiển truy cập (Access Control Framework)

Cơ cấu điều khiển truy cập gắn kết thực hiện đầy đủ tất cả các dịch vụ khác. Đặc tả nguyên bản của WEP không bao gồm cơ cấu cho việc xác nhận và cho phép, với WAP, WAP2 và RSN, chuẩn nhóm nhiệm vụ 802.11i chỉ ra việc sr dụng 802.1x như cơ cấu xác nhận và cho phép.

5. Xác nhận

Xác nhận sẽ chuyển đến bộ xác nhận mạng những xác nhận đáng tin cậy từ các điểm truy cập. Phương pháp xác nhận được sử dụng trong các mạng đầy đủ phụ thuộc nhiều thông số như mạng là mạng doanh nghiệp hay mạng công cộng và mục đích của mạng là phục vụ những ai. Với những lý do này, bạn cần phương pháp hỗ trợ phương pháp đa xác nhận. 802.1X sử dụng Extensible Authentication Protocol (EAP) làm phương pháp hỗ trợ đa xác nhận.

6. Cho phép

Chức năng này cho phép những khối truy cập đã được xác nhận truy cập vào tài nguyên mạng đã được xác nhận. Khi các trạm làm việc đã được xác nhận (máy laptop hoặc các thành phần mạng), cổng 802.1x coi như nó đã được cho quyền truy cập vào tài nguyên mạng. Cơ cấu truy nhập phức tạp này có thể nhận được từ chức năng cơ sở của VLAN trong chuyển mạch.

7. Sự tin cẩn

Chức năng này định địa chỉ những thông tin trao đổi kín giữa một hoặc nhiều khối truyền thông. Chức năng này thực hiện bởi khung mã hoá không dây với thuật toán mã hoá mạnh.

8. Toàn vẹn dữ liệu

Chức năng này đảm bảo rằng các thông báo nhận được cách để cảm nhận sự phá rối trong khi định hướng tới nơi cần nhận. trong WEP, toàn vẹn dữ liệu được thực hiện thông qua việc sử dụng Cyclic Redundancy Check (CRC)

9. Key Management

Khoá quản lý cho khả năng tự động phát ra, truyền và sử dụng trong hệ thống bảo mật kết nối truyền thông của xác nhận và khoá mã hoá. Với WEP, 802.11 không cung cấp chức năng tự động key management. Trong WEP, khoá chia sẻ nhập bằng tay nhắc lại cho đến khi thay đổi trên AP và tất cả các trạm làm việc đều sử dụng những AP này.

10. Bảo vệ chống tấn công đã biết

Một hệ thống bảo mật được thiết kế tốt sẽ bảo vệ chống lại các kiểu tấn công đã biết. 802.11i bao gồm các loại bảo vệ chống các tấn công đã biết như MAC spoofing và man-in-the-middle attacks. Sự phản kháng của các tấn công này thường là kết quả của kết hợp giữa xác nhận, cho phép, độ tin cậy và khoá quản lý.

Bảng 7.13. Những đặc tính chủ yếu của WEB, WPA, WPA2, 802.11i (RSN)

Đặc tính	WEP	WPA	WPA2	802.11i (RSN)
Access Control Framework	Không	802.1x	802.1x	802.1x
Authentication Framework	Không	EAP	EAP	EAP
Encryption Algorithm	RC4	RC4	AES	AES
Key size	40 bits hoặc 104 bits	128 bits cho mã hoá và 64 cho xác nhận	128 bits	128 bits
packet key	Concatenation (móc nối)	Mixing Function (chức năng trộn)	Không cần	Không cần
Key management	Static	802.1x + TKIP	802.1x+ CCMP	802.1x+CCMP
Key lifetime	24 bit VI	48 bit VI	48 bit VI	48 bit VI
phương pháp xác nhận	Shared key	Shared key, phương pháp cơ sở EAP	Shared key, phương pháp cơ sở EAP	Shared key, phương pháp cơ sở EAP
Header Integrity	Không	Micheal	Micheal	CBC-MAC
Pre-Authentication	Không	Không	Không	Có
Roaming	Giới hạn	Giới hạn	Giới hạn	có

Khi mạng LAN không dây trở nên phổ cập thì các giải pháp bảo mật mạng lại càng quan trọng. Thông qua việc sử dụng mạng riêng ảo (Virtual Private Networks -VPN) bảo mật cho mạng WLAN 802.11a được tối đa hóa.

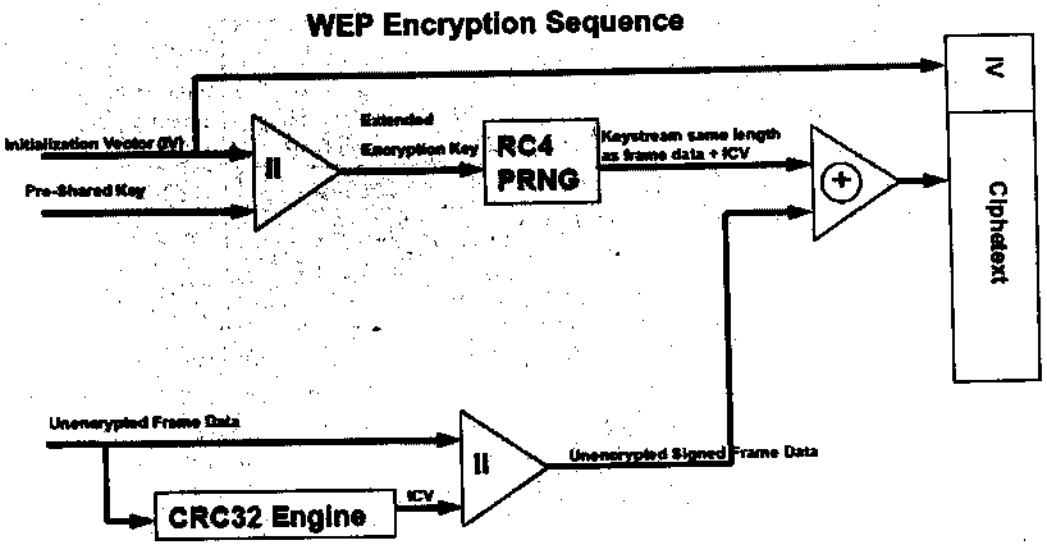
Mạng riêng ảo hiện nay đã được sử dụng rộng rãi cho truy cập từ xa, các VPN sử dụng nhiều cơ chế bảo mật khác nhau, trong đó chỉ tiêu kỹ thuật Bảo mật Giao thức Internet (Internet Procotol Security - IPSec) đang là cơ chế được sử dụng nhiều nhất, để đảm bảo cho những người dùng được cấp quyền mới có thể truy cập vào mạng và dữ liệu không bị chặn bắt trên đường truyền. Chỉ tiêu kỹ thuật của Internet Protocol Security (IPSec) do

IEEE 1394 thiết lập là cơ chế bảo mật được sử dụng nhiều nhất cho lưu thông mạng VPN.

Tổ hợp của VPN và IPSec là giải pháp lý tưởng cho các nhu cầu bảo mật mạng không dây hiện nay. Với giải pháp này việc đặt thông số kỹ thuật cho các điểm truy cập không dây sẽ rất đơn giản cho các truy cập mở không dùng mã hóa vì các kênh VPN đã đảm nhiệm phần bảo mật. Các máy chủ VPN làm nhiệm vụ xác nhận và mã hóa cho toàn bộ mạng WLAN. Việc sử dụng chứng nhận kỹ thuật số cho phép xác nhận quyền tốt hơn và ngay cả trong trường hợp truy cập không được phép cũng không thể đọc hoặc sử dụng được các giao tiếp trên mạng.

Do có thể quản lý tập trung các máy chủ VPN, phí quản lý trên mỗi đầu máy sẽ thấp. Và không giống như việc lọc địa chỉ WEP và MAC, các giải pháp VPN có thể mở rộng ra một lượng rất lớn người sử dụng. Hơn nữa, nhiều tổ chức, doanh nghiệp đã triển khai VPN trên hệ thống mạng của mình. Kết quả là việc mở rộng các giải pháp này cho mạng WLAN cũng dễ dàng và kinh tế hơn.

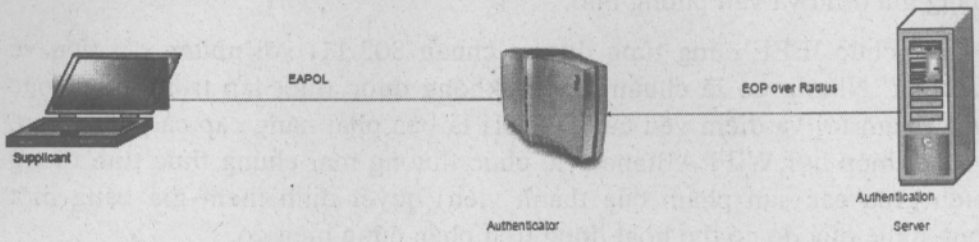
Sự không đồng nhất trong giao thức Wired Equivalent Privacy (WEP) đã cản đường mạng LAN thâm nhập vào các công ty. Hầu hết các nhà quản trị mạng và người dùng cuối đều hiểu lợi ích của việc bỏ đi những đoạn dây trong mạng Ethernet nhưng lại lo ngại về vấn đề bảo mật.



Hình 7.36. Chuỗi mã hoá WEP

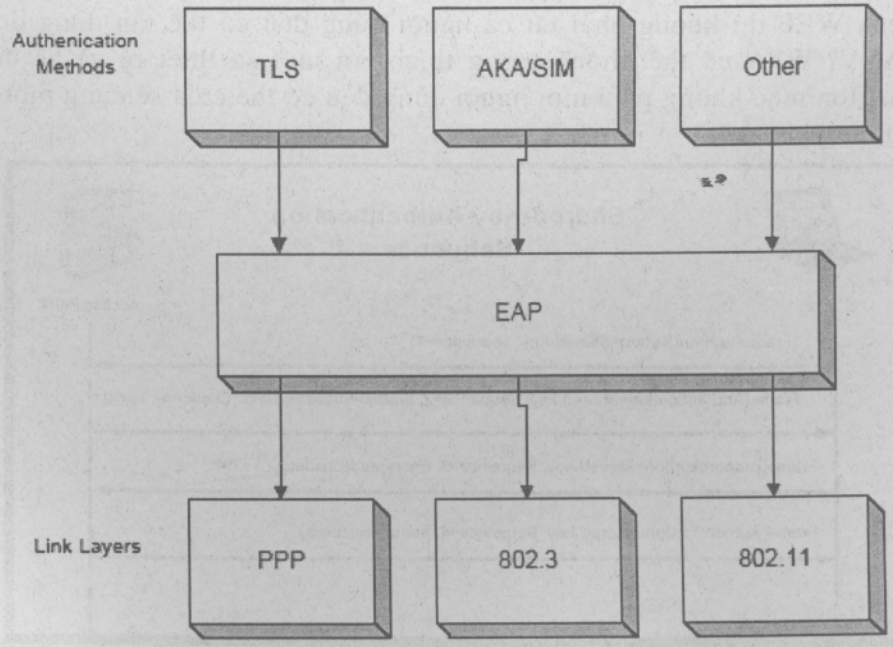
WLAN mở toang mạng và nếu đứng trên khía cạnh bảo mật thì WLAN phải được đối xử như là một mạng truy cập chứ không phải là mạng nội bộ

thông thường. Trong mạng LAN, người dùng cộng tác kết nối qua một bộ chuyển mạch hay hub, và được xem như là người dùng tin cậy. Người quản trị mạng có thể dùng hoặc không dùng một giao thức để định danh ví dụ như 802.1X hay RADIUS.



Hình 7.37. *Cấu trúc 802.1x*

Để giải quyết vấn đề này với WLAN, hiệp hội IEEE 802.11 đã thành lập nhóm Task Group i để xây dựng bản nâng cấp bảo mật cho chuẩn 802.11. Nhóm 802.11i đang dựng chuẩn theo việc định danh dựa trên cổng 802.1X cho người dùng và định danh thiết bị.



Hình 7.38*. Cơ chế EAP*

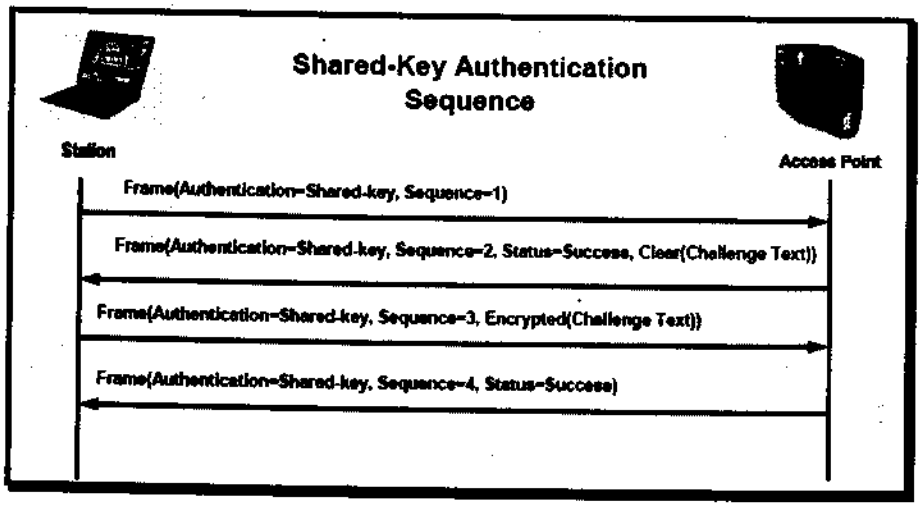
Công nghệ WiFi Protected Access (WPA) thay thế cho thuật toán bảo mật hiện đang được sử dụng nhiều là Wired Equivalent Privacy (WEP), một phần của chuẩn 802.11a, 802.11b và 802.11g hiện nay. WEP đã trở thành

rào cản cho việc chấp nhận mạng WiFi trên diện rộng khi các chuyên gia bảo mật cho thấy tin tặc với công cụ hiện đại có thể dễ dàng thâm nhập mạng. WPA hỗ trợ khả năng tính hợp lệ của người dùng bằng máy chủ chuyên dụng trong mạng cộng tác và vẫn đủ linh hoạt để làm việc tốt trong mạng gia đình và văn phòng nhỏ.

Tổ chức IEEE cũng từng đưa ra chuẩn 802.11i với những cải tiến về bảo mật. Nhưng có lẽ chuẩn này sẽ không được thiết lập trong một hoặc nhiều năm tới và điểm yếu của 802.11i là bạn phải nâng cấp cả phần cứng. Vì thế, hiệp hội WiFi Alliance (tổ chức thương mại chứng thực tính tương thích giữa các sản phẩm của thành viên) quyết định tham gia bằng một công nghệ quá độ có thể hoạt động trên phần cứng hiện có.

WPA thực chất là tập con trong các thành phần của 802.11i. Nó dùng giao thức TKIP (Temporal Key Interchange Protocol) công nghệ mã hóa an toàn hơn so với RC4 của WEP. Khi chuẩn bị xong, 802.11i sẽ kết hợp với một công nghệ mã hóa dựa trên phần cứng mạnh mẽ hơn nữa có tên là AES (Advanced Encryption Standrad).

Trong khi WPA đi được một bước dài trong việc khắc phục những thiếu sót của WEP thì không phải tất cả người dùng đều có thể tận dụng được WPA. Vì WPA có thể không tương thích với một số thiết bị và hệ điều hành. Hơn nữa, không phải mọi người dùng đều có thể chia sẻ cùng một cơ sở hạ tầng bảo mật.



Hình 7.37. Xác nhận khoá chia sẻ

Điểm hạn chế nữa là TKIP/WPA sẽ làm giảm tốc độ hệ thống trừ khi một hệ thống WLAN có phần cứng để tăng tốc giao thức WPA. Đối với hầu hết mạng LAN hiện nay, vấn đề bảo mật và tốc độ xử lý của mạng khá ngang bằng nhau không tính sự tăng tốc phần cứng tại điểm truy cập.

11. Các cách để tăng cường bảo mật mạng không dây

Thay đổi mật khẩu mặc định để truy cập Access Point/Router. Thay đổi SSID (Service Set ID) mặc định của Access Point/Router không dây do nhà sản xuất đã đặt ra.

Kích hoạt mức độ cao nhất của chế độ mã hóa WEP mà Access Point cho phép. Tuy còn thiếu sót nhưng WEP còn cung cấp bảo vệ tối thiểu cho bạn. Chuẩn 802.11b và 802.11g hỗ trợ chế độ mã hóa cao nhất là 128bit, chuẩn 802.11a là 152bit, còn chuẩn 802.11b+ đến 256bit.

Tắt chế độ "Ad-hoc", hãy dùng chế độ "Infrastructure" để tất cả các trạm làm việc không dây chỉ kết nối với nhau thông qua Access Point/Router không dây. Chế độ "Ad-hoc" cho phép các mạng làm việc không dây kết nối ngang hàng với nhau, tin tặc có thể lợi dụng để xâm nhập vào mội trường mạng không dây của bạn.

Thiết lập việc xác thực địa chỉ MAC thông qua danh sách người dùng được phép truy cập – Access Control List (ACL). Bạn thiết lập Access Point/Router chỉ cho phép những trạm không dây có địa chỉ MAC mà bạn đã qui định mới được quyền truy cập vào mạng.

Tắt chế độ "BROADCAST" (quảng bá) tín hiệu SSID của Access Point/Router không dây bởi vì tin tặc có thể dễ dàng dò ra tên SSID của Access Point/Router không dây bằng các tiện ích miễn phí, hoặc ngay cả WindowsXP cũng tìm được tên của những mạng không dây gần đó.

Nếu bạn có dùng đến SNMP (Simple Network Management Protocol) trên Access Point, hãy đổi các tên "community", mặc định của nhà sản xuất, nhằm gây khó dễ cho tin tặc.

Thường xuyên kiểm tra khu vực để phát hiện những Access Point trái phép. Để thực hiện bạn có thể dùng một máy tính xách tay trang bị card mạng không dây và có cài tiện ích miến phí như Netstumbler (hoặc sử dụng tiện ích của WindowsXP) đi quanh khu vực để tìm các thiết bị hoặc Access Point nối vào mạng trái phép.

Thiết lập Access Point/Router không dây thuộc một "subnet"riêng và thiết lập "firewall" giữa "subnet" đó và mạng bên trong của bạn.

Triển khai mạng riêng ảo (VPN – Virtual Private Network) cho mạng không dây. Công nghệ này cho phép người dùng trao đổi thông tin một cách an toàn thông qua các VPN tunnel. Giải pháp này hơi phức tạp vì cần một máy chủ VPN.

Đào tạo người dùng nội bộ về những rủi ro bảo mật của mạng không dây và thiết lập chính sách bảo mật về việc sử dụng mạng không dây.

TÀI LIỆU THAM KHẢO

1. Ed Taylor, The McGraw-*Hill Internetworking handbook*, McGraw-Hill International Editons, 1995.
2. Jack Unger, Deploying License-*Free Wireless Wide-Area Networks*, Cisco Press, 2001.
3. Reference guide, *Cisco Aironet ăngtens and Accessories*, Cisco press, 2003.
4. White Paper, *Capacity, coverage, and deployment considerations*, Cissco Press, 2003.
5. Matthew S.Gast, *802.11 Wireless Networks*, O'REILLY, 2003.
6. Nguyễn Hồng Sơn, *Giáo trình hệ thống mạng máy tính CCNA Sememster 1*, Nhà xuất bản Lao động – Xã hội, 2004.
7. M.F.Rnett, *Inside TCP/IP*, NRP, 1994.
8. Theodore S. Rappaport, *Wireless Communications second Editor*, Prentice-Hall, 2003.
9. D. Bertsekas, R. Gallager, *Data Network*, Prentice- hall, 1987.
10. F. Halsall, *Data communications, computer Networks and open systems*, Addison, 1992.
11. Ed Krol, *The Whole Internet*, O'Reilly Associates, 1998.
12. *John Hammond, Bart Kessler, Juan Rivero, Chad Skinner, Tim Sweeney, Wireless Hotspot Deployment Guide*, Intel Press, 2004.
13. A. S. Tanenbaum, *Computer Networks*, 4th Edition, Prentice-Hall, 2003.
14. L. L. Peterson, B. S. Davie, *Computer Networks: A Systems Approach*, 3rd Edition, Elsevier Science, 2003.
15. J. F. Kurose, K. W. Rose, *Computer Networking: A Top-Down Approach Featuring the Internet*, 2nd Edition, Pearson Education, Inc., 1998.

16. D. E. Comer, R. E. Droms, Computer Networks and Internets, Prentice Hall, 1997.

17. W. R. Stevens, The Protocols (TCP/IP Illustrated, Volume 1),, 1995.

18. T. Lammle, *CCNA Cisco Certified Network Associate Study Guide,* 2nd Edition, Sybex Inc., 2002.

19. C. E. Spurgeon, *Ethernet: The Definitive Guide*, O'Reilly & Associates, 2000.

20. D.Richard Kuhn, Thomas J. Walsh, Steffen Fries, Security Considerations for Voice Over IP Systems, National Institude of Standards and Technology Special Publication, 2005

21. Sean Christensen, Voice over IP Solutions, Juniper NETWWORKS, 2001

22. John Q. Walker, Jeffrey T.Hicks, The Essential Guide to VoIP Implementation and Management, NETIQ, 2002.

23. Vinod K. Bhat, Voice Over IP- The SIP Way, TATA Consultancy Services, 2001.

24. Công ty TNHH Máy tính Nét – NETCOM Co., Ltd., Các tài liệu kinh doanh, 2001-2005.

MỤC LỤC

Chịu trách nhiệm xuất bản :
Chủ tịch HĐQT kiêm Tổng Giám đốc NGÔ TRẦN ÁI
Phó Tổng Giám đốc kiêm Tổng biên tập VŨ DƯƠNG THỤY

Biên tập nội dung :
HOÀNG TRỌNG NGHĨA
Trình bày bìa :
BÙI QUANG TUẤN
Sửa bản in :
HOÀNG TRỌNG NGHĨA
Chế bản :
THU HIỀN

MẠNG MÁY TÍNH

Mã số : 7B616M5 - DAI

In 1.000 bản, khổ 16 x 24cm, tại Xí nghiệp In ACS Hải Phòng.
Số in : 881. Số xuất bản : 167/8-05.
In xong và nộp lưu chiểu tháng 7 năm 2005.

CÔNG TY CỔ PHẦN SÁCH ĐẠI HỌC - DẠY NGHỀ
HEVOBCO
25 HÀN THUYÊN - HÀ NỘI

TÌM ĐỌC SÁCH THAM KHẢO KỸ THUẬT CỦA NHÀ XUẤT BẢN GIÁO DỤC

1	**Đất ngập nước**	GS. TS. Lê Văn Khoa
2	**Động vật học có xương sống**	GS. TS. Lê Vũ Khôi
3	**Sinh thái học côn trùng**	PGS. TS. Phạm Bình Quyến
5	**Cơ sở hoá sinh**	PGS. TS. Trịnh Lê Hùng
6	**Tài nguyên nước Việt Nam**	Nguyễn Thanh Sơn
7	**Virut học**	PGS. TS. Phạm Văn Ty
8	**Vật lý kỹ thuật**	Đặng Hùng
9	**Vật lý siêu dẫn và ứng dụng**	TS. Nguyễn Huy Sinh
10	**Dụng cụ bán dẫn và vi mạch**	Lê Xuân Thê
11	**Mạng máy tính**	Ngac Văn An
12	**Vô tuyến điện tử**	Ngac Văn An
13	**Giáo trình cơ học**	Bạch Thành Công
13	**Kinh tế môi trường**	PGS. TS. Hoàng Xuân Cơ
14	**Tiếng Anh cơ bản cho sinh viên khoa học tự nhiên**	Trần Thị Nga
15	**Bộ sách về công nghệ sinh học**	
	Tập một : **Sinh học phân tử - Cơ sở khoa học của công nghệ sinh học**	PGS. TS. Nguyễn Như Hiến
	Tập hai : **Công nghệ sinh học tế bào**	GS. TS. Vũ Văn Vụ PGS. TS. Nguyễn Mộng Hùng
	Tập ba : **Công nghệ sinh học enzym và protein** (XB - 2006)	TS. Phan Tuấn Nghĩa
	Tập bốn : **Công nghệ sinh học di truyền** (XB - 2006)	GS. TS. Lê Đình Lương
	Tập năm : **Công nghệ sinh học vi sinh và công nghệ môi trường** (XB - 2006)	PGS. TS. Phạm Văn Ty

Bạn đọc có thể mua tại các Công ty Sách - Thiết bị trường học ở địa phương hoặc các Cửa hàng của Nhà xuất bản Giáo dục :

** 25 Hàn Thuyên, 187 Giảng Võ, 23 Tràng Tiền - Hà Nội.*
** 15 Nguyễn Chí Thanh - TP Đà Nẵng*
** 104 Mai Thị Lựu - Quận 1 - TP. Hồ Chí Minh.*

8 934980 541012

Giá : 25.500đ