

CHƯƠNG 1

GIỚI THIỆU VỀ MẠNG

I. CÁC KIẾN THỨC CƠ SỞ

1. Mạng máy tính là gì ?

Mạng máy tính là một nhóm các máy tính, thiết bị ngoại vi được nối kết với nhau thông qua các phương tiện truyền dẫn như cáp, sóng điện từ, tia hồng ngoại... giúp cho các thiết bị này có thể trao đổi dữ liệu với nhau một cách dễ dàng.

2. Các thành phần cơ bản cấu thành nên mạng máy tính

- ♦ Các loại máy tính: **Palm, Laptop, PC, MainFrame...**
- ♦ Các thiết bị giao tiếp: Card mạng (**NIC** hay **Adapter**), **Hub, Switch, Router...**
- ♦ Môi trường truyền dẫn: cáp, sóng điện từ, sóng vi ba, tia hồng ngoại...
- ♦ Các protocol: **TCP/IP, NetBeui, Apple Talk, IPX/SPX...**
- ♦ Các hệ điều hành mạng: **WinNT, Win2000, Win2003, Novell Netware, Unix...**
- ♦ Các tài nguyên: file, thư mục.
- ♦ Các thiết bị ngoại vi: máy in, máy fax, **Modem, Scanner...**
- ♦ Các ứng dụng mạng: phần mềm quản lý kho bãi, phần mềm quản lý đào tạo, phần mềm ứng dụng trong ngành ngân hàng, phần mềm bán vé tàu...

Một số khái niệm

❖ **Server** (máy phục vụ): là máy tính được cài đặt các phần mềm chuyên dụng làm chức năng cung cấp các dịch vụ cho các máy tính khác. Tùy theo dịch vụ mà các máy này cung cấp, người ta chia thành các loại **server** như sau: **File server** (cung cấp các dịch vụ về file và thư mục), **Print server** (cung cấp các dịch vụ về in ấn). Do làm chức năng phục vụ cho các máy tính khác nên cấu hình máy server phải mạnh, thông thường là máy chuyên dụng của các hãng như: Compaq, Intel, IBM...

❖ **Client** (máy trạm): là máy tính sử dụng các dịch vụ mà các máy server cung cấp. Do xử lý số công việc không lớn nên thông thường các máy này không yêu cầu có cấu hình mạnh.

❖ **Peer**: là những máy tính vừa đóng vai trò là máy sử dụng vừa là máy cung cấp các dịch vụ. Máy peer thường sử dụng các hệ điều hành như: **DOS, WinNT Workstation, Win9X, Win Me, Win2K Professional, WinXP...**

❖ **Media** (phương tiện truyền dẫn): là cách thức và vật liệu nối kết các máy lại với nhau.

❖ **Shared data** (dữ liệu dùng chung): là tập hợp các tập tin, thư mục mà các máy tính chia sẻ để các máy tính khác truy cập sử dụng chúng thông qua mạng.

❖ **Resource** (tài nguyên): là tập tin, thư mục, máy in, máy Fax, Modem, Ổ CDROM và các thành phần khác mà người dùng mạng sử dụng.

❖ **User** (người dùng): là người sử dụng máy trạm (**client**) để truy xuất các tài nguyên mạng. Thông thường một user sẽ có một username (**account**) và một password. Hệ thống mạng sẽ dựa vào username và password để biết bạn là ai, có quyền vào mạng hay không và có quyền sử dụng những tài nguyên nào trên mạng.

❖ **Administrator**: là nhà quản trị hệ thống mạng.

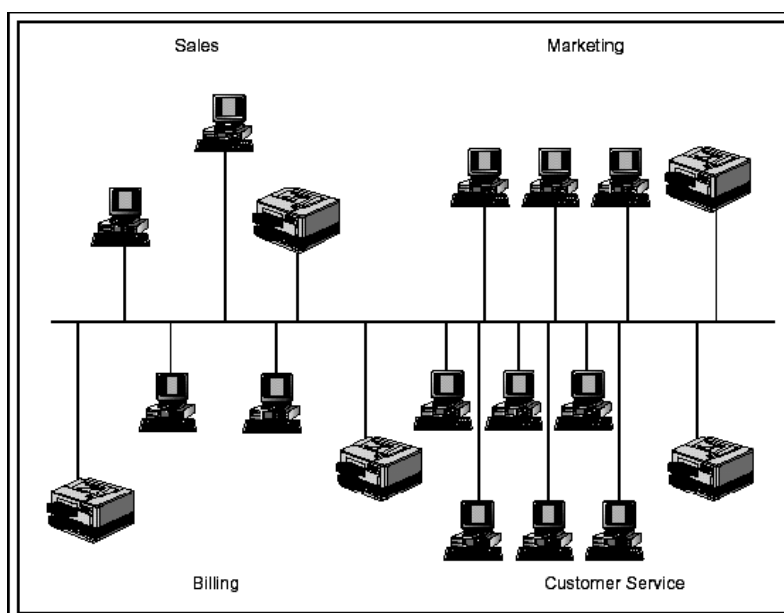
II. CÁC LOẠI MẠNG MÁY TÍNH

1. Mạng cục bộ LAN (Local Area Network)

Mạng LAN là một nhóm máy tính và các thiết bị truyền thông mạng được nối kết với nhau trong một khu vực nhỏ như một tòa nhà cao ốc, khuôn viên trường đại học, khu giải trí ...

Các mạng LAN thường có đặc điểm sau:

- ♦ Băng thông lớn, có khả năng chạy các ứng dụng trực tuyến như xem phim, hội thảo qua mạng.
- ♦ Kích thước mạng bị giới hạn bởi các thiết bị.
- ♦ Chi phí các thiết bị mạng LAN tương đối rẻ.
- ♦ Quản trị đơn giản.



Hình 1.1 – Mô hình mạng cục bộ (LAN)

2. Mạng đô thị MAN (Metropolitan Area Network)

Mạng MAN gần giống như mạng LAN nhưng giới hạn của nó là một thành phố hay một quốc gia. Mạng MAN nối kết các mạng LAN lại với nhau thông qua các

phương tiện truyền dẫn khác nhau (cáp quang, cáp đồng, sóng...) và các phương thức truyền thông khác nhau.

Đặc điểm của mạng MAN:

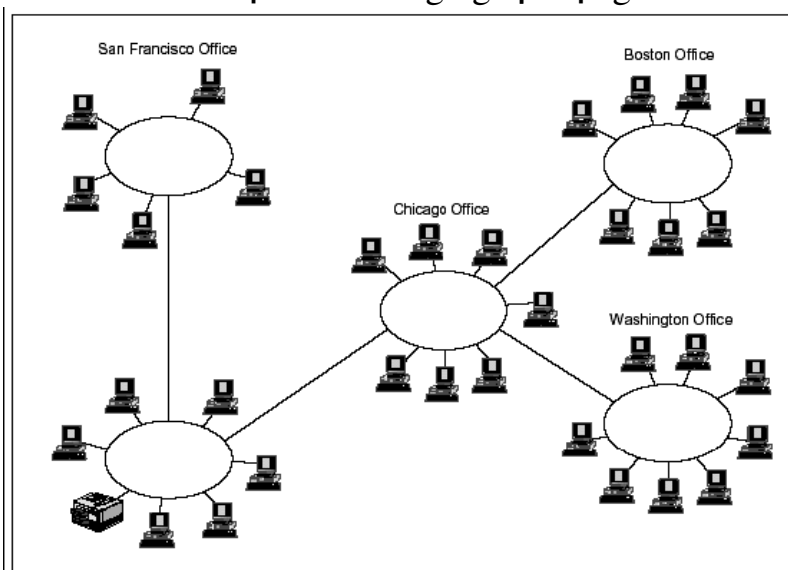
- ♦ Băng thông mức trung bình, đủ để phục vụ các ứng dụng cấp thành phố hay quốc gia như chính
- ♦ phủ điện tử, thương mại điện tử, các ứng dụng của các ngân hàng...
- ♦ Do MAN nối kết nhiều LAN với nhau nên độ phức tạp cũng tăng đồng thời công tác quản trị sẽ khó
- ♦ khản hơn.
- ♦ Chi phí các thiết bị mạng MAN tương đối đắt tiền.

3. Mạng diện rộng WAN (Wide Area Network)

Mạng WAN bao phủ vùng địa lý rộng lớn có thể là một quốc gia, một lục địa hay toàn cầu. Mạng WAN thường là mạng của các công ty đa quốc gia hay toàn cầu, điển hình là mạng Internet. Do phạm vi rộng lớn của mạng WAN nên thông thường mạng WAN là tập hợp các mạng LAN, MAN nối lại với nhau bằng các phương tiện như: vệ tinh (**satellites**), sóng viba (**microwave**), cáp quang, cáp điện thoại...

Đặc điểm của mạng WAN:

- ♦ Băng thông thấp, dễ mất kết nối, thường chỉ phù hợp với các ứng dụng offline như e-mail, web, ftp ...
- ♦ Phạm vi hoạt động rộng lớn không giới hạn.
- ♦ Do kết nối của nhiều LAN, MAN lại với nhau nên mạng rất phức tạp và có tính toàn cầu nên thường là có tổ chức quốc tế đứng ra quản trị.
- ♦ Chi phí cho các thiết bị và các công nghệ mạng WAN rất đắt tiền.



Hình 1.2 – Mô hình mạng diện rộng (WAN)

4. Mạng Internet

Mạng Internet là trường hợp đặc biệt của mạng WAN, nó cung cấp các dịch vụ toàn cầu như mail, web, chat, ftp và phục vụ miễn phí cho mọi người.

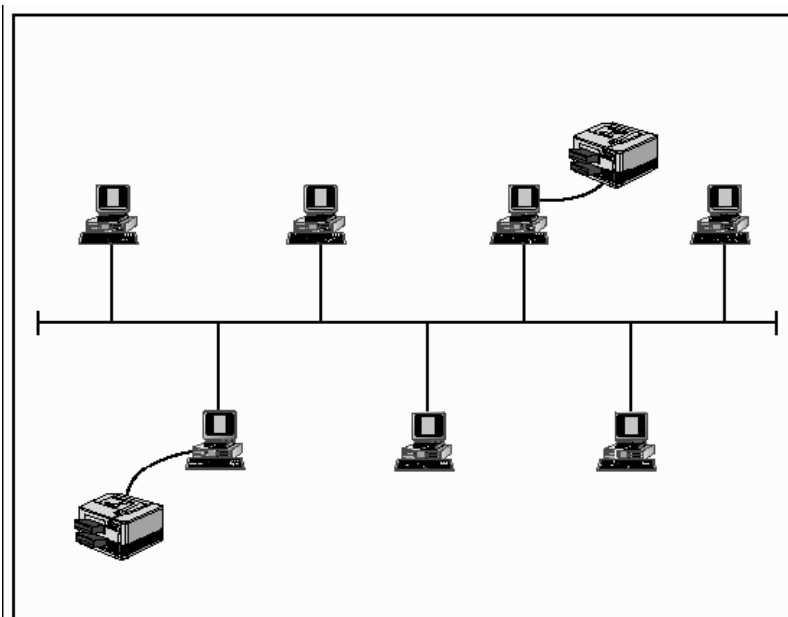
III. CÁC MÔ HÌNH ỨNG DỤNG MẠNG

1. Mạng ngang hàng (peer to peer)

Mạng ngang hàng cung cấp việc kết nối cơ bản giữa các máy tính nhưng không có bất kỳ một máy tính nào đóng vai trò phục vụ. Một máy tính trên mạng có thể vừa là **client**, vừa là **server**. Trong môi trường này, người dùng trên từng máy tính chịu trách nhiệm điều hành và chia sẻ các tài nguyên của máy tính mình. Mô hình này chỉ phù hợp với các tổ chức nhỏ, số người giới hạn (thông thường nhỏ hơn 10 người), và không quan tâm đến vấn đề bảo mật. Mạng ngang hàng thường dùng các hệ điều hành sau: **Win95, Windows for workgroup, WinNT Workstation, Win2000 Professional, OS/2...**

Ưu điểm: do mô hình mạng ngang hàng đơn giản nên dễ cài đặt, tổ chức và quản trị, chi phí thiết bị cho mô hình này thấp.

Khuyết điểm: không cho phép quản lý tập trung nên dữ liệu phân tán, khả năng bảo mật thấp, rất dễ bị xâm nhập. Các tài nguyên không được sắp xếp nên rất khó định vị và tìm kiếm.



Hình 1.3 – Mô hình ứng dụng mạng ngang hàng (**Peer-to-Peer**)

2. Mạng khách chủ (client- server)

Trong mô hình mạng khách chủ có một hệ thống máy tính cung cấp các tài nguyên và dịch vụ cho cả hệ thống mạng sử dụng gọi là các máy chủ (**server**). Một hệ thống máy tính sử dụng các tài nguyên và dịch vụ này được gọi là máy khách (**client**). Các server thường có cấu hình mạnh (tốc độ xử lý nhanh, kích

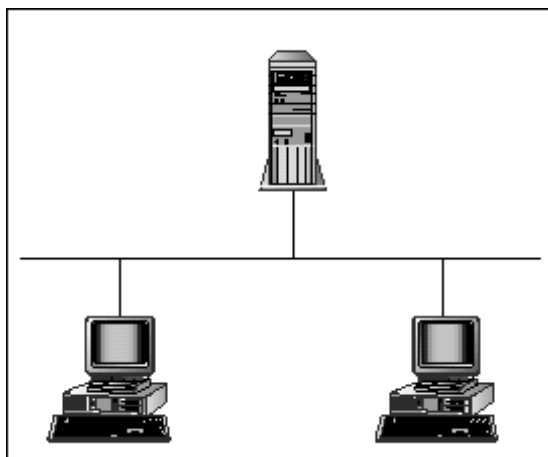
thước lưu trữ lớn) hoặc là các máy chuyên dụng. Dựa vào chức năng có thể chia thành các loại server như sau:

- ♦ **File Server:** phục vụ các yêu cầu hệ thống tập tin trong mạng.
- ♦ **Print Server:** phục vụ các yêu cầu in ấn trong mạng.
- ♦ **Application Server:** cho phép các ứng dụng chạy trên các server và trả về kết quả cho client.
- ♦ **Mail Server:** cung cấp các dịch vụ về gửi nhận e-mail.
- ♦ **Web Server:** cung cấp các dịch vụ về web.
- ♦ **Database Server:** cung cấp các dịch vụ về lưu trữ, tìm kiếm thông tin.
- ♦ **Communication Server:** quản lý các kết nối từ xa.

Hệ điều hành mạng dùng trong mô hình client - server là **WinNT, Novell NetWare, Unix, Win2K...**

Ưu điểm: do các dữ liệu được lưu trữ tập trung nên dễ bảo mật, backup và đồng bộ với nhau. Tài nguyên và dịch vụ được tập trung nên dễ chia sẻ và quản lý và có thể phục vụ cho nhiều người dùng.

Khuyết điểm: các server chuyên dụng rất đắt tiền, phải có nhà quản trị cho hệ thống.



Hình 1.4 – Mô hình Ứng dụng mạng khách chủ (**Client-Server**)

IV. CÁC LỢI ÍCH THỰC TẾ CỦA MẠNG.

1. Tiết kiệm được tài nguyên phần cứng.

Khi các máy tính của một phòng ban được nối mạng với nhau thì chúng ta có thể chia sẻ những thiết bị ngoại vi như máy in, máy FAX, ổ đĩa CDRom... Thay vì trang bị cho từng máy PC thì thông qua mạng chúng ta có thể dùng chung các thiết bị này.

Ví dụ 1: trong một phòng máy thực hành có khoảng 30 máy, nếu trang bị cho tất cả các máy trạm có đĩa cứng thì rất phí mà chúng ta lại không tận dụng được hết năng suất của các đĩa cứng đó. Giải pháp tập trung tất cả các ứng dụng vào server và dùng công nghệ mạng bootrom để chạy các máy trạm sẽ làm giảm chi phí phần

cứng đồng thời tiện dụng cho công tác quản trị phòng máy hạn chế được tình trạng các học viên vô tình làm hỏng các máy trạm.

Ví dụ 2: Một công ty muốn rằng tất cả các phòng ban đều được sử dụng Internet thông qua modem và đường điện thoại. Nếu chúng ta trang bị cho mỗi phòng ban 1 modem và 1 đường điện thoại thì không khả thi vì vậy chúng ta phải tận dụng cơ sở hạ tầng mạng để chia sẻ 1 modem và đường điện thoại cho cả công ty đều có thể truy cập Internet.

2. Trao đổi dữ liệu trở nên dễ dàng hơn.

Theo phương pháp truyền thống muốn chép dữ liệu giữa hai máy tính chúng ta dùng đĩa mềm hoặc dùng cáp **link** để nối hai máy lại với nhau sau đó chép dữ liệu. Chúng ta thấy rằng hai giải pháp trên sẽ không thực tế nếu một máy đặt tại tầng trệt và một máy đặt tại tầng 5 trong một tòa nhà. Việc trao đổi dữ liệu giữa các máy tính ngày càng nhiều hơn, đa dạng hơn, khoảng cách giữa các phòng ban trong công ty ngày càng xa hơn nên việc trao đổi dữ liệu theo phương thức truyền thống không còn được áp dụng nữa, thay vào đó là các máy tính này được nối với nhau qua công nghệ mạng.

3. Chia sẻ ứng dụng.

Các ứng dụng thay vì trên từng máy trạm chúng ta sẽ cài trên một máy server và các máy trạm dùng chung ứng dụng đó trên server. Lúc đó ta tiết kiệm được chi phí bản quyền và chi phí cài đặt, quản trị.

4. Tập trung dữ liệu, bảo mật và backup tốt.

Đối với các công ty lớn dữ liệu lưu trữ trên các máy trạm rời rạc dễ dẫn đến tình trạng hư hỏng thông tin và không được bảo mật. Nếu các dữ liệu này được tập trung về server để tiện việc bảo mật, backup và quét virus.

5. Sử dụng các phần mềm ứng dụng trên mạng.

Nhờ các công nghệ mạng mà các phần mềm ứng dụng phát triển mạnh và được áp dụng vào nhiều lĩnh vực như hàng không (phần mềm bán vé máy bay tại các chi nhánh), đường sắt (phần mềm theo dõi đăng ký vé và bán vé tàu), cấp thoát nước (phần mềm quản lý công ty cấp thoát nước thành phố)...

6. Sử dụng các dịch vụ Internet.

Ngày nay Internet rất phát triển, tất cả mọi người trên thế giới đều có thể trao đổi E-mail với nhau một cách dễ dàng hoặc có thể trò chuyện với nhau mà chi phí rất thấp so với phí viễn thông. Đồng thời các công ty cũng dùng công nghệ Web để quảng cáo sản phẩm, mua bán hàng hóa qua mạng (thương mại điện tử) ...

Dựa trên cơ sở hạ tầng mạng chúng ta có thể xây dựng các hệ thống ứng dụng lớn như chính phủ điện tử, thương mại điện tử, điện thoại Internet nhằm giảm chi phí và tăng khả năng phục vụ ngày càng tốt hơn cho con người.

CHƯƠNG 2

CÁC KIẾN TRÚC VÀ CÔNG NGHỆ MẠNG LAN

I. CÁC KIẾN TRÚC MẠNG (TOPOLOGY).

1. Khái niệm.

Network topology là sơ đồ dùng biểu diễn các kiểu sắp xếp, bố trí vật lý của máy tính, dây cáp và những thành phần khác trên mạng theo phương diện vật lý.

Có hai kiểu kiến trúc mạng chính là: kiến trúc vật lý (mô tả cách bố trí đường truyền thực sự của mạng), kiến trúc logic (mô tả con đường mà dữ liệu thật sự di chuyển qua các node mạng)

2. Các kiểu kiến trúc mạng chính.

a. *Mạng Bus (tuyến)*

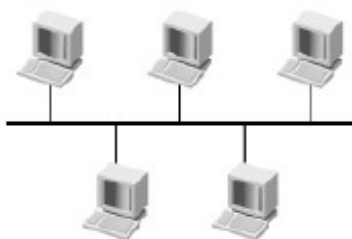
- Kiến trúc **Bus** là một kiến trúc cho phép nối mạng các máy tính đơn giản và phổ biến nhất. Nó dùng một đoạn cáp nối tất cả máy tính và các thiết bị trong mạng thành một hàng. Khi một máy tính trên mạng gửi dữ liệu dưới dạng tín hiệu điện thì tín hiệu này sẽ được lan truyền trên đoạn cáp đến các máy tính còn lại, tuy nhiên dữ liệu này chỉ được máy tính có địa chỉ so khớp với địa chỉ mã hóa trong dữ liệu chấp nhận. Mỗi lần chỉ có một máy có thể gửi dữ liệu lên mạng vì vậy số lượng máy tính trên bus càng tăng thì hiệu suất thi hành mạng càng chậm.

- *Hiện tượng dội tín hiệu*: là hiện tượng khi dữ liệu được gửi lên mạng, dữ liệu sẽ đi từ đầu cáp này đến đầu cáp kia. Nếu tín hiệu tiếp tục không ngừng nó sẽ dội tới lui trong dây cáp và ngăn không cho máy tính khác gửi dữ liệu. Để giải quyết tình trạng này người ta dùng một thiết bị terminator (điện trở cuối) đặt ở mỗi đầu cáp để hấp thụ các tín hiệu điện tự do.

- *Ưu điểm*: kiến trúc này dùng ít cáp, dễ lắp đặt, giá thành rẻ. Khi mở rộng mạng tương đối đơn

giản, nếu khoảng cách xa thì có thể dùng repeater để khuếch đại tín hiệu.

- *Khuyết điểm*: khi đoạn cáp đứt đôi hoặc các đầu nối bị hở ra thì sẽ có hai đầu cáp không nối với terminator nên tín hiệu sẽ dội ngược và làm cho toàn bộ hệ thống mạng sẽ ngừng hoạt động. Những lỗi như thế rất khó phát hiện ra là hỏng chỗ nào nên công tác quản trị rất khó khi mạng lớn (nhiều máy và kích thước lớn).



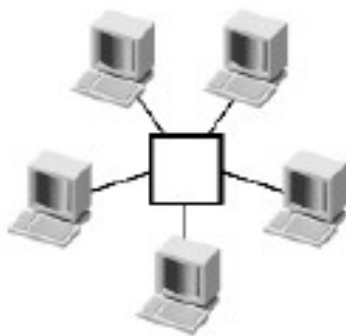
Hình 2.1 – Kiến trúc mạng **Bus**.

b. *Mạng star (sao)*

- Trong kiến trúc này, các máy tính được nối vào một thiết bị đấu nối trung tâm (**Hub** hoặc **Switch**). Tín hiệu được truyền từ máy tính gửi dữ liệu qua hub tín hiệu được khuếch đại và truyền đến tất cả các máy tính khác trên mạng.

- *Ưu điểm*: kiến trúc star cung cấp tài nguyên và chế độ quản lý tập trung. Khi một đoạn cáp bị hỏng thì chỉ ảnh hưởng đến máy dùng đoạn cáp đó, mạng vẫn hoạt động bình thường. Kiến trúc này cho phép chúng ta có thể mở rộng hoặc thu hẹp mạng một cách dễ dàng.

- *Khuyết điểm*: do mỗi máy tính đều phải nối vào một trung tâm điểm nên kiến trúc này đòi hỏi nhiều cáp và phải tính toán vị trí đặt thiết bị trung tâm. Khi thiết bị trung tâm điểm bị hỏng thì toàn bộ hệ thống mạng cũng ngừng hoạt động.

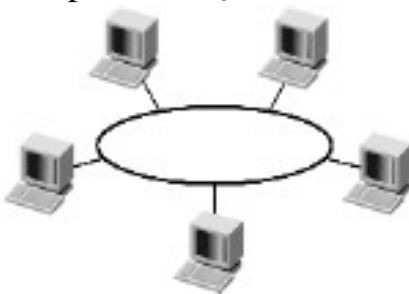


Hình 2.2 – Kiến trúc mạng **Star**.

c. **Mạng Ring (vòng)**

- Trong mạng ring các máy tính và các thiết bị nối với nhau thành một vòng khép kín, không có đầu nào bị hở. Tín hiệu được truyền đi theo một chiều và qua nhiều máy tính. Kiến trúc này dùng phương pháp chuyển thẻ bài (**token passing**) để truyền dữ liệu quanh mạng.

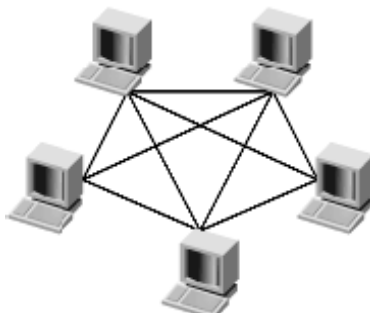
- Phương pháp chuyển thẻ bài là phương pháp dùng thẻ bài chuyển từ máy tính này sang máy tính khác cho đến khi tới máy tính muốn gửi dữ liệu. Máy này sẽ giữ thẻ bài và bắt đầu gửi dữ liệu đi quanh mạng. Dữ liệu chuyển qua từng máy tính cho đến khi tìm được máy tính có địa chỉ khớp với địa chỉ trên dữ liệu. Máy tính đầu nhận sẽ gửi một thông điệp cho máy tính đầu gửi cho biết dữ liệu đã được nhận. Sau khi xác nhận máy tính đầu gửi sẽ tạo thẻ bài mới và thả lên mạng. Vận tốc của thẻ bài xấp xỉ với vận tốc ánh sáng.



Hình 2.3 – Kiến trúc mạng **Ring**.

d. **Mạng Mesh (lưới)**.

Từng cặp máy tính thiết lập các tuyến kết nối liên điểm do đó số lượng tuyến kết nối nhanh chóng gia tăng khi số lượng máy tính trong mạng tăng lên nên người ta ít dùng cho các mạng lưới lớn.



Hình 2.4 – Kiến trúc mạng Mesh.

e. *Mạng Cellular (tế bào).*

Các mạng tế bào chia vùng địa lý đang được phục vụ thành các tế bào, mỗi tế bào được một trạm trung tâm phục vụ. Các thiết bị sử dụng các tín hiệu radio để truyền thông với trạm trung tâm, và trạm trung tâm sẽ định tuyến các thông điệp đến các thiết bị. Ví dụ điển hình của mạng tế bào là mạng điện thoại di động.

II. CÁC CÔNG NGHỆ MẠNG LAN.

1. Khái niệm.

- **Collision Domain:** đây là một vùng có khả năng bị ðụng ðộ do hai hay nhiều máy tính cùng gửi tín hiệu lên môi trường truyền thông.
- **Broadcast Domain:** đây là một vùng mà gói tin phát tán (gói tin **broadcast**) có thể đi qua ðược. Trong vùng **Broadcast Domain** có thể là vùng bao gồm nhiều **Collision Domain**.

2. Ethernet

Đầu tiên, **Ethernet** ðược phát triển bởi các hãng **Xerox, Digital, Intel** vào đầu những năm 1970. Phiên bản đầu tiên của **Ethernet** ðược thiết kế như một hệ thống 2,94 Mbps để nối hơn 100 máy tính vào một sợi cáp dài 1 Km. Sau đó các hãng lớn ðã thảo luận và ðưa ra chuẩn dành cho **Ethernet** 10 Mbps.

Ethernet chuẩn thường có cấu hình bus, truyền với tốc ðộ 10Mbps và ðựa vào **CSMA/CD (Carrier Sense Multiple Access / Collision Detection)** để điều chỉnh lưu thông trên ðường cáp chính. Tóm lại những ðặc ðiểm cơ bản của **Ethernet** như sau:

- Cấu hình: **bus** hoặc **star**.
- Phương pháp chia sẻ môi trường truyền: **CSMA/CD**.
- Quy cách kỹ thuật IEEE 802.3
- Vận tốc truyền: 10 – 100 Mbps.
- Cáp: cáp ðồng trục mảnh, cáp ðồng trục lớn, cáp **UTP**.
- Tên của chuẩn **Ethernet** thể hiện 3 ðặc ðiểm sau:
- Con số đầu tiên thể hiện tốc ðộ truyền tối ða.

- Từ tiếp theo thể hiện tín hiệu dải tần cơ sở được sử dụng (Base hoặc Broad).

+ **Ethernet** dựa vào tín hiệu **Baseband** sẽ sử dụng toàn bộ băng thông của phương tiện

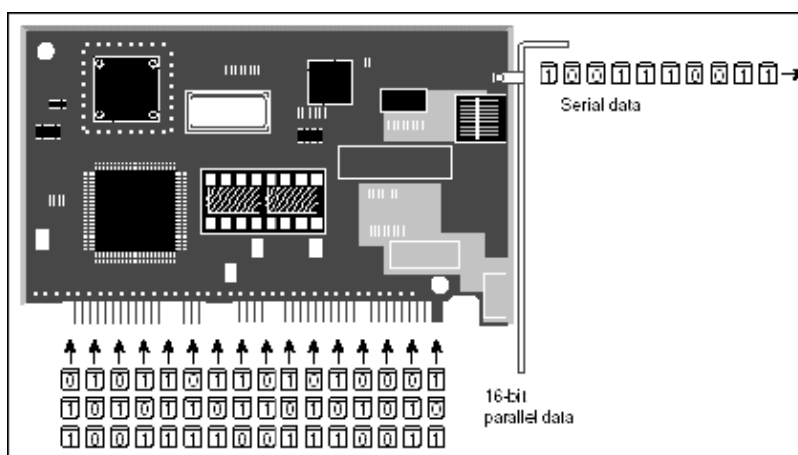
truyền dẫn. Tín hiệu dữ liệu sẽ được truyền trực tiếp trên phương tiện truyền dẫn mà không cần thay đổi kiểu tín hiệu.

+ Trong tín hiệu Broadband (**ethernet** không sử dụng), tín hiệu dữ liệu không bao giờ gửi trực

tiếp lên phương tiện truyền dẫn mà phải thực hiện điều chế.

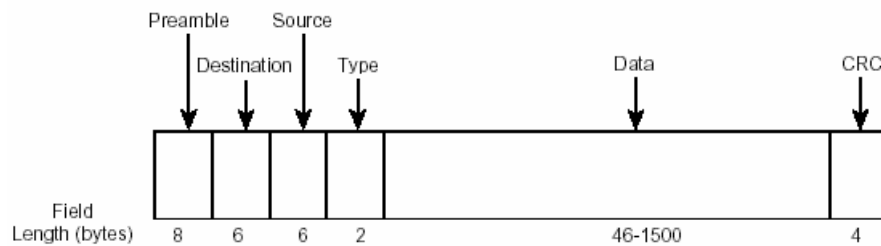
- Các ký tự còn lại thể hiện loại cáp được sử dụng. Ví dụ: chuẩn 10Base2, tốc độ truyền tối đa là 10Mbps, sử dụng tín hiệu **Baseband**, sử dụng cáp **Thinnet**.

Card mạng **Ethernet**: hầu hết các **NIC** cũ đều được cấu hình bằng các **jump** (các chấu cắm chuyển) để ấn định địa chỉ và ngắt. Các **NIC** hiện hành được cấu hình tự động hoặc bằng một chương trình chạy trên máy chứa card mạng, nó cho phép thay đổi các ngắt và địa chỉ bộ nhớ lưu trữ trong một chip bộ nhớ đặc biệt trên **NIC**.



Hình 2.5 – Card mạng **Ethernet**.

Dạng thức khung trong **Ethernet**: **Ethernet** chia dữ liệu thành nhiều khung (**frame**). Khung là một gói thông tin được truyền như một đơn vị duy nhất. Khung trong **Ethernet** có thể dài từ 64 đến 1518 byte, nhưng bản thân khung **Ethernet** đã sử dụng ít nhất 18 byte, nên dữ liệu một khung **Ethernet** có thể dài từ 46 đến 1500 byte. Mỗi khung đều có chứa thông tin điều khiển và tuân theo một cách tổ chức cơ bản. Ví dụ khung **Ethernet** (dùng cho TCP/IP) được truyền qua mạng với các thành phần sau:



Hình 2.6 – Cấu trúc khung **Ethernet**.

Các trường trong **Frame Ethernet**:

- **Preamble**: 8 byte mở đầu.
- **Destination**: 6 byte thể hiện địa chỉ **MAC** đích.
- **Source**: 6 byte thể hiện địa chỉ **MAC** nguồn.
- **Type**: 2 byte thể hiện kiểu giao thức ở tầng trên.
- **Data**: dữ liệu của **Frame**.
- **CRC**: 4 byte dùng để kiểm lỗi của **Frame**.

Các loại **Ethernet** với băng tần cơ sở:

- 10Base2: tốc độ 10, chiều dài cáp nhỏ hơn 200 m, dùng cáp **thinnet** (cáp đồng trục mảnh).
- 10Base5: tốc độ 10, chiều dài cáp nhỏ hơn 500 m, dùng cáp **thicknet** (cáp đồng trục dày).
- 10BaseT: tốc độ 10, dùng cáp xoắn đôi (**Twisted-Pair**).
- 10BaseFL: tốc độ 10, dùng cáp quang (**Fiber optic**).
- 100BaseT: tốc độ 100, dùng cáp xoắn đôi (**Twisted-Pair**).
- 100BaseX: tốc độ 100, dùng cho **multiple media type**.
- 100VG-AnyLAN: tốc độ 100, dùng **voice grade**.

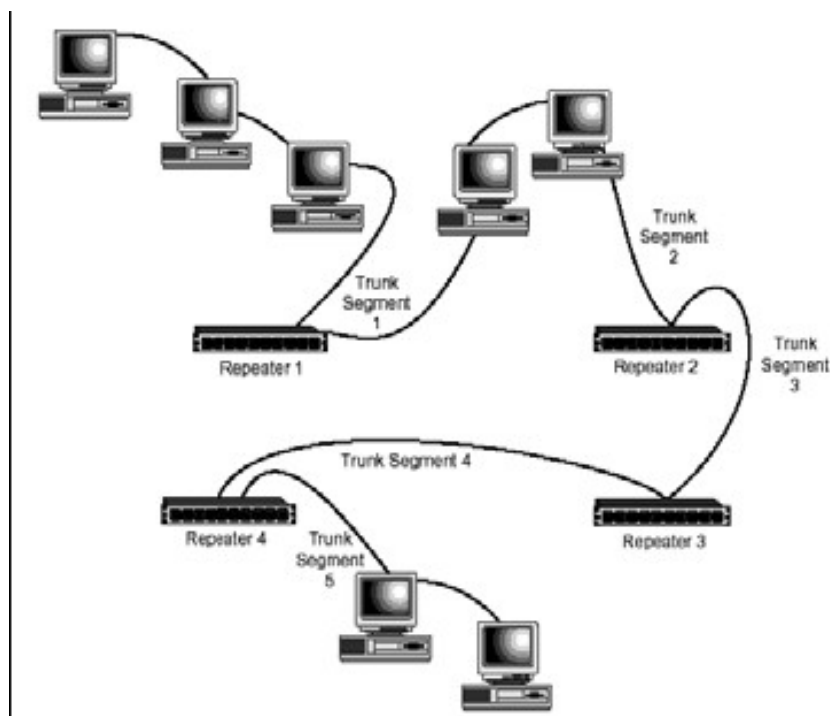
a. *Chuẩn 10Base2*

Cấu hình này được xác định theo tiêu chuẩn IEEE 802.3 và bảo đảm tuân thủ các quy tắc sau:

- Khoảng cách tối thiểu giữa hai máy trạm phải cách nhau 0.5m.
- Dùng cáp **Thinnet** (RG-58).
- Tốc độ 10 Mbps.
- Dùng đầu nối chữ T (**T-connector**).
- Không thể vượt quá phân đoạn mạng tối đa là 185m. Toàn bộ hệ thống cáp mạng không thể vượt quá 925m.
- Số nút tối đa trên mỗi phân đoạn mạng là 30.
- **Terminator** (thiết bị đầu cuối) phải có trở kháng 50 ohm và được nối đất.

- Mỗi mạng không thể có trên năm phân đoạn. Các phân đoạn có thể nối tối đa bốn bộ khuếch đại và chỉ có ba trong số năm phân đoạn có thể có nút mạng (tuân thủ quy tắc 5-4-3).

Quy tắc 5-4-3: quy tắc này cho phép kết hợp đến năm đoạn cáp được nối bởi 4 bộ chuyển tiếp, nhưng chỉ có 3 đoạn là nối trạm. Theo hình dưới ta thấy đoạn 3, 4 chỉ tồn tại nhằm mục đích làm tăng tổng chiều dài mạng và cho phép máy tính trên đoạn 1, 2, 5 nằm cùng trên một mạng.



Hình 2.7 – Quy tắc 5-4-3.

Ưu điểm chuẩn 10Base2: giá thành rẻ, đơn giản.

b. Chuẩn 10Base5

Chuẩn mạng này tuân theo các quy tắc sau:

- Khoảng cách tối thiểu giữa hai nút là 2.5m.
- Dùng cáp **thicknet** (cáp đồng dày).
- Băng tần cơ sở 10Mbps.
- Chiều dài phân đoạn mạng tối đa là 500m.
- Toàn bộ chiều dài mạng không thể vượt quá 2500m.
- Thiết bị đầu cuối (**terminator**) phải được nối đất.
- Cáp thu phát (**tranceiver cable**), nối từ máy tính đến bộ thu phát, có chiều dài tối đa 50m.
- Số nút tối đa cho mỗi phân đoạn mạng là 100 (bao gồm máy tính và tất cả các **repeater**).
- Tuân theo quy tắc 5-4-3.

Ưu điểm: khắc phục được khuyết điểm của mạng 10Base2, hỗ trợ kích thước mạng lớn hơn.

Chú ý: trong các mạng lớn người ta thường kết hợp cáp dày và cáp mảnh. Cáp dày dùng làm cáp chính rất tốt, còn cáp mảnh dùng làm đoạn nhánh.

c. Chuẩn 10BaseT.

Chuẩn mạng này tuân theo các quy tắc sau:

- Dùng cáp UTP loại 3, 4, 5 hoặc **STP**, có mức trở kháng là 85-115 ohm, ở 10Mhz.
- Dùng quy cách kỹ thuật 802.3.
- Dùng thiết bị đấu nối trung tâm **Hub**.
- Tốc độ tối đa 10Mbps.
- Dùng đầu nối RJ-45.
- Số nút tối đa là 512 và chúng có thể nối vào 3 phân đoạn bất kỳ với năm phân tuyến tối đa có sẵn.
- Chiều dài tối đa một phân đoạn cáp là 100m.
- Dùng mô hình vật lý **star**.
- Có thể nối các phân đoạn mạng 10BaseT bằng cáp đồng trục hay cáp quang.
- Số lượng máy tính tối đa là 1024.
- Khoảng cách tối thiểu giữa hai máy tính là 2,5m.
- Khoảng cách cáp tối thiểu từ một **Hub** đến một máy tính hoặc một **Hub** khác là 0,5m.

Ưu điểm: do trong mạng 10BaseT dùng thiết bị đấu nối trung tâm nên dữ liệu truyền tin cậy hơn, dễ quản lý. Điều này cũng tạo thuận lợi cho việc định vị và sửa chữa các phân đoạn cáp bị hỏng. Chuẩn này cho phép bạn thiết kế và xây dựng trên từng phân đoạn một trên LAN và có thể tăng dần khi mạng cần phát triển. 10BaseT cũng tương đối rẻ tiền so với các phương án đấu cáp khác.

d. Chuẩn 10BaseFL.

Các đặc điểm của 10BaseFL:

- Tốc độ tối đa 10 Mbps.
- Truyền qua cáp quang.

Ưu điểm:

- Do dùng cáp quang nối các **Repeater** nên khoảng cách tối đa cho một đoạn cáp là 2000m.
- Không sợ bị nhiễu điện từ.
- Số nút tối đa trên một đoạn cáp lớn hơn nhiều so với 10Base2, 10Base5, 10BaseT.

e. Chuẩn 10BaseFL.

Các đặc điểm của 10BaseFL:

- Tốc độ tối đa 10 Mbps.
- Truyền qua cáp quang.

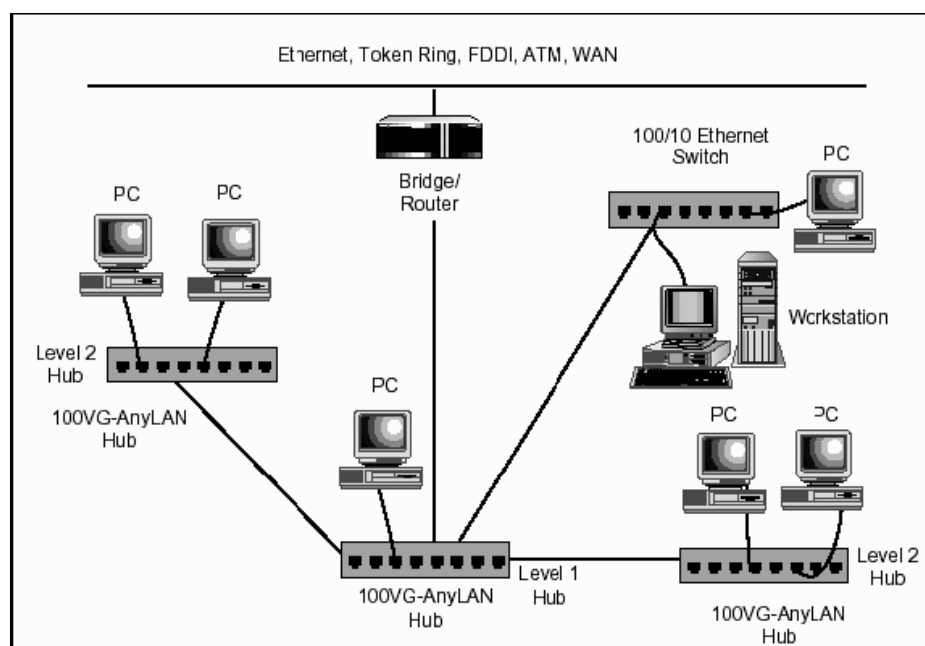
Ưu điểm:

- Do dùng cáp quang nối các **Repeater** nên khoảng cách tối đa cho một đoạn cáp là 2000m.
- Không sợ bị nhiễu điện từ.
- Số nút tối đa trên một đoạn cáp lớn hơn nhiều so với 10Base2, 10Base5, 10BaseT.

f. *Chuẩn 100VG-AnyLAN.*

100VG (Voice Grade) **AnyLan** là công nghệ mạng kết hợp các thành phần của **Ethernet** và **Token Ring**, dùng quy cách kỹ thuật 802.12. Các đặc điểm kỹ thuật:

- Tốc độ truyền dữ liệu tối thiểu là 100Mbps.
- Sử dụng cáp xoắn đôi gồm bốn cặp xoắn (**UTP** loại 3, 4, 5 hoặc **STP**) và cáp quang.
- Khả năng hỗ trợ sàng lọc từng khung có địa chỉ tại **Hub** nhằm tăng cường tính năng bảo mật.
- Chấp nhận cả khung **Ethernet** lẫn gói **Token Ring**.
- Định nghĩa trong IEEE 802.12.
- Mô hình vật lý: **cascaded star**, mọi máy tính được nối với một **Hub**. Có thể mở rộng mạng bằng cách thêm **Hub** con vào **Hub** trung tâm, **Hub** con đóng vai trò như máy tính đối với **Hub** mẹ.
- Chiều dài tối đa của đoạn chạy cáp nối hai **Hub** là 250m.

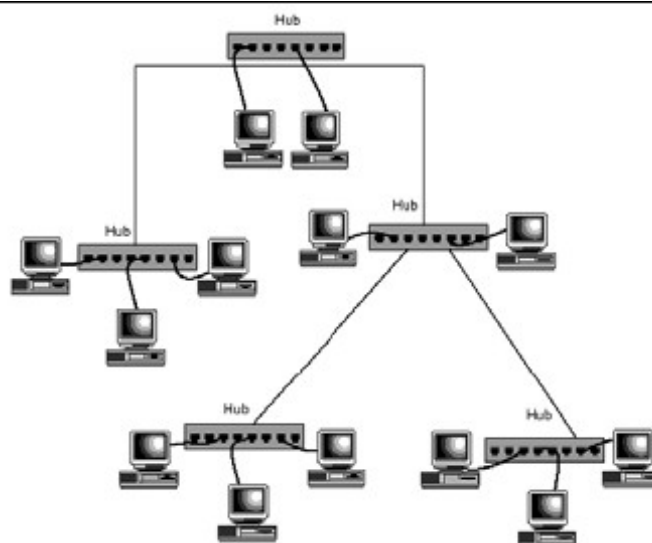


Hình 2.8 – Một ví dụ về chuẩn 100VG-AnyLAN.

g. **Chuẩn 100BaseX.**

Tiêu chuẩn 100BaseX **Ethernet** còn gọi là **Fast Ethernet** là sự mở rộng của tiêu chuẩn **Ethernet** có sẵn. Tiêu chuẩn này dùng cáp **UTP Cat5** và phương pháp truy cập **CSMA/CD** trong cấu hình **star bus** với mọi đoạn cáp nối vào một **Hub** tương tự 10BaseT. Tốc độ 100Mbps. Chuẩn 100BaseX có các đặc tả ứng với các loại đường truyền khác nhau:

- 100BaseT4: dùng cáp **UTP** loại 3, 4, 5 có bốn cặp xoắn đôi.
- 100BaseTX: dùng cáp **UTP** loại 5 có hai cặp xoắn đôi hoặc **STP**.
- 100BaseFX: dùng cáp quang có hai dây lõi.



Hình 2.9 – Một ví dụ về chuẩn 100Base-X.

Bảng dưới đây sẽ tóm tắt lại các thông số của một số loại cáp.

Chuẩn	Loại cáp	Chiều dài tối đa	Đầu nối
10Base2	Thinnet	185m	BNC
10Base5	Thicknet	500m	AUI
100Base-TX	UTP cat 5, 2 cặp dây	100m	RJ45
100Base-FX	Cáp quang Multimode, lõi 62.5 hoặc 125 micro	400m	MIC, ST, SC
1000Base-CX	STP	25m	RJ45
1000Base-T	UTP cat 5, 4 cặp dây	100m	RJ45
1000Base-SX	Cáp quang ultimode, lõi 62.5 hoặc 50 micro	62.5 micro thì được 275m 50 micro thì được 550m	SC
1000Base-LX	Cáp quang Multimode, lõi 62.5 hoặc 50 micro Cáp quang Singlemode,	62.5 micro thì được 440m 50 micro thì	SC

	lõi 9 micro	được 550m 9 micro thì được 3-10Km	
--	-------------	-----------------------------------	--

CHƯƠNG 3

MÔ HÌNH THAM CHIẾU OSI

I. MÔ HÌNH THAM CHIẾU OSI 7 LỚP.

1. Khái niệm giao thức (protocol).

Là quy tắc giao tiếp (tiêu chuẩn giao tiếp) giữa hai hệ thống giúp chúng hiểu và trao đổi dữ liệu được với nhau.

Ví dụ: **Internetwork Packet Exchange (IPX)**, **Transmission control protocol/ Internetwork Protocol (TCP/IP)**, **NetBIOS Extended User Interface (NetBEUI)**

...

2. Các tổ chức định chuẩn.

ITU (International Telecommunication Union): Hiệp hội Viễn thông quốc tế.

IEEE (Institute of Electrical and Electronic Engineers): Viện các kỹ sư điện và điện tử.

ISO (International Standardization Organization): Tổ chức Tiêu chuẩn quốc tế, trụ sở tại Geneve, Thụy Sĩ. Vào năm 1977, ISO được giao trách nhiệm thiết kế một chuẩn truyền thông dựa trên lý thuyết về kiến trúc các hệ thống mở làm cơ sở để thiết kế mạng máy tính. Mô hình này có tên là OSI (**Open System Interconnection** - tương kết các hệ thống mở)

3. Mô hình OSI.

Mô hình OSI (**Open System Interconnection**): là mô hình được tổ chức ISO đề xuất từ 1977 và công bố lần đầu vào 1984. Để các máy tính và các thiết bị mạng có thể truyền thông với nhau phải có những quy tắc giao tiếp được các bên

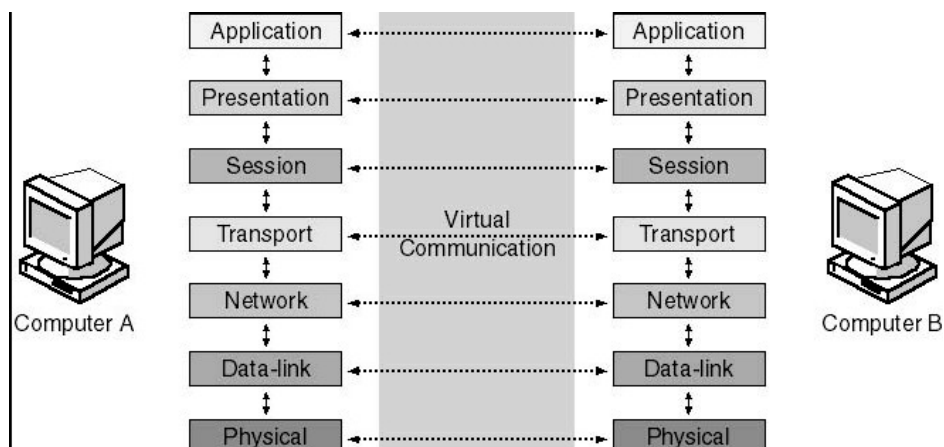
chấp nhận. Mô hình OSI là một khuôn mẫu giúp chúng ta hiểu dữ liệu đi xuyên qua mạng như thế nào đồng thời cũng giúp chúng ta hiểu được các chức năng mạng diễn ra tại mỗi lớp.

Trong mô hình OSI có bảy lớp, mỗi lớp mô tả một phần chức năng độc lập. Sự tách lớp của mô hình này mang lại những lợi ích sau:

- Chia hoạt động thông tin mạng thành những phần nhỏ hơn, đơn giản hơn giúp chúng ta dễ khảo sát và tìm hiểu hơn.
 - Chuẩn hóa các thành phần mạng để cho phép phát triển mạng từ nhiều nhà cung cấp sản phẩm.
 - Ngăn chặn được tình trạng sự thay đổi của một lớp làm ảnh hưởng đến các lớp khác, như vậy giúp mỗi lớp có thể phát triển độc lập và nhanh chóng hơn.
- Mô hình tham chiếu OSI định nghĩa các qui tắc cho các nội dung sau:
- Cách thức các thiết bị giao tiếp và truyền thông được với nhau.
 - Các phương pháp để các thiết bị trên mạng khi nào thì được truyền dữ liệu, khi nào thì không được.
 - Các phương pháp để đảm bảo truyền đúng dữ liệu và đúng bên nhận.
 - Cách thức vận tải, truyền, sắp xếp và kết nối với nhau.
 - Cách thức đảm bảo các thiết bị mạng duy trì tốc độ truyền dữ liệu thích hợp.
 - Cách biểu diễn một bit thiết bị truyền dẫn.

Mô hình tham chiếu OSI được chia thành bảy lớp với các chức năng sau:

- **Application Layer** (lớp ứng dụng): giao diện giữa ứng dụng và mạng.
- **Presentation Layer** (lớp trình bày): thỏa thuận khuôn dạng trao đổi dữ liệu.
- **Session Layer** (lớp phiên): cho phép người dùng thiết lập các kết nối.
- **Transport Layer** (lớp vận chuyển): đảm bảo truyền thông giữa hai hệ thống.
- **Network Layer** (lớp mạng): định hướng dữ liệu truyền trong môi trường liên mạng.
- **Data link Layer** (lớp liên kết dữ liệu): xác định việc truy xuất đến các thiết bị.
- **Physical Layer** (lớp vật lý): chuyển đổi dữ liệu thành các bit và truyền đi.



Hình 3.1 – Mô hình tham chiếu OSI

4. Chức năng của các lớp trong mô hình tham chiếu OSI

Lớp ứng dụng (Application Layer): là giao diện giữa các chương trình ứng dụng của người dùng và mạng. Lớp **Application** xử lý truy nhập mạng chung, kiểm soát luồng và phục hồi lỗi. Lớp này không cung cấp các dịch vụ cho lớp nào mà nó cung cấp dịch vụ cho các ứng dụng như: truyền file, gửi nhận E-mail, Telnet, HTTP, FTP, SMTP...

Lớp trình bày (Presentation Layer): lớp này chịu trách nhiệm thương lượng và xác lập dạng thức dữ liệu được trao đổi. Nó đảm bảo thông tin mà lớp ứng dụng của một hệ thống đầu cuối gửi đi, lớp ứng dụng của hệ thống khác có thể đọc được. Lớp trình bày thông dịch giữa nhiều dạng dữ liệu khác nhau thông qua một dạng chung, đồng thời nó cũng nén và giải nén dữ liệu. Thứ tự byte, bit bên gửi và bên nhận qui ước qui tắc gửi nhận một chuỗi byte, bit từ trái qua phải hay từ phải qua trái. Nếu hai bên không thống nhất thì sẽ có sự chuyển đổi thứ tự các byte bit vào trước hoặc sau khi truyền.

Lớp **presentation** cũng quản lý các cấp độ nén dữ liệu nhằm giảm số bit cần truyền. Ví dụ: **JPEG, ASCII, EBCDIC...**

Lớp phiên (Session Layer): lớp này có chức năng thiết lập, quản lý, và kết thúc các phiên thông tin giữa hai thiết bị truyền nhận. Lớp phiên cung cấp các dịch vụ cho lớp trình bày. Lớp **Session** cung cấp sự đồng bộ hóa giữa các tác vụ người dùng bằng cách đặt những điểm kiểm tra vào luồng dữ liệu. Bằng cách này, nếu mạng không hoạt động thì chỉ có dữ liệu truyền sau điểm kiểm tra cuối cùng mới phải truyền lại. Lớp này cũng thi hành kiểm soát hội thoại giữa các quá trình giao tiếp, điều chỉnh bên nào truyền, khi nào, trong bao lâu. Ví dụ như: **RPC, NFS...** Lớp này kết nối theo ba cách: **Half-duplex, Simplex, Full-duplex.**

Lớp vận chuyển (Transport Layer): lớp vận chuyển phân đoạn dữ liệu từ hệ thống máy truyền và tái thiết lập dữ liệu vào một luồng dữ liệu tại hệ thống máy nhận đảm bảo rằng việc bàn giao các thông điệp giữa các thiết bị đáng tin

cây. Dữ liệu tại lớp này gọi là **segment**. Lớp này thiết lập, duy trì và kết thúc các mạch ảo đảm bảo cung cấp các dịch vụ sau:

- Xếp thứ tự các phân đoạn: khi một thông điệp lớn được tách thành nhiều phân đoạn nhỏ để bàn giao, lớp vận chuyển sẽ sắp xếp thứ tự các phân đoạn trước khi ráp nối các phân đoạn thành thông điệp ban đầu.

- Kiểm soát lỗi: khi có phân đoạn bị thất bại, sai hoặc trùng lặp, lớp vận chuyển sẽ yêu cầu truyền lại.

- Kiểm soát luồng: lớp vận chuyển dùng các tín hiệu báo nhận để xác nhận. Bên gửi sẽ không truyền đi phân đoạn dữ liệu kế tiếp nếu bên nhận chưa gửi tín hiệu xác nhận rằng đã nhận được phân đoạn dữ liệu trước đó đầy đủ.

Lớp mạng (**Network Layer**): lớp mạng chịu trách nhiệm lập địa chỉ các thông điệp, diễn dịch địa chỉ và tên logic thành địa chỉ vật lý đồng thời nó cũng chịu trách nhiệm gửi packet từ mạng nguồn đến mạng đích. Lớp này quyết định đường đi từ máy tính nguồn đến máy tính đích. Nó quyết định dữ liệu sẽ truyền trên đường nào dựa vào tình trạng, ưu tiên dịch vụ và các yếu tố khác. Nó cũng quản lý lưu lượng trên mạng chẳng hạn như chuyển đổi gói, định tuyến, và kiểm soát sự tắc nghẽn dữ liệu. Nếu bộ

thích ứng mạng trên bộ định tuyến (router) không thể truyền đủ đoạn dữ liệu mà máy tính nguồn gửi đi, lớp **Network** trên bộ định tuyến sẽ chia dữ liệu thành những đơn vị nhỏ hơn, nói cách khác, nếu máy tính nguồn gửi đi các gói tin có kích thước là 20Kb, trong khi **Router** chỉ cho phép các gói tin có kích thước là 10Kb đi qua, thì lúc đó lớp **Network** của **Router** sẽ chia gói tin ra làm 2, mỗi gói tin có kích thước là 10Kb. Ở đầu nhận, lớp **Network** ráp nối lại dữ liệu. Ví dụ: một số giao thức lớp này: IP, IPX,...

Dữ liệu ở lớp này gọi packet hoặc datagram.

Lớp liên kết dữ liệu (**Data link Layer**): cung cấp khả năng chuyển dữ liệu tin cậy xuyên qua một liên kết vật lý. Lớp này liên quan đến:

- Địa chỉ vật lý.
- Mô hình mạng.
- Cơ chế truy cập đường truyền.
- Thông báo lỗi.
- Thứ tự phân phối frame.
- Điều khiển dòng.

Tại lớp **data link**, các bit đến từ lớp vật lý được chuyển thành các frame dữ liệu bằng cách dùng một số nghi thức tại lớp này. Lớp **data link** được chia thành hai lớp con:

- Lớp con LLC (**logical link control**).
- Lớp con MAC (**media access control**).

Lớp con LLC là phần trên so với các giao thức truy cập đường truyền khác, nó cung cấp sự mềm dẻo về giao tiếp. Bởi vì lớp con LLC hoạt động độc lập với

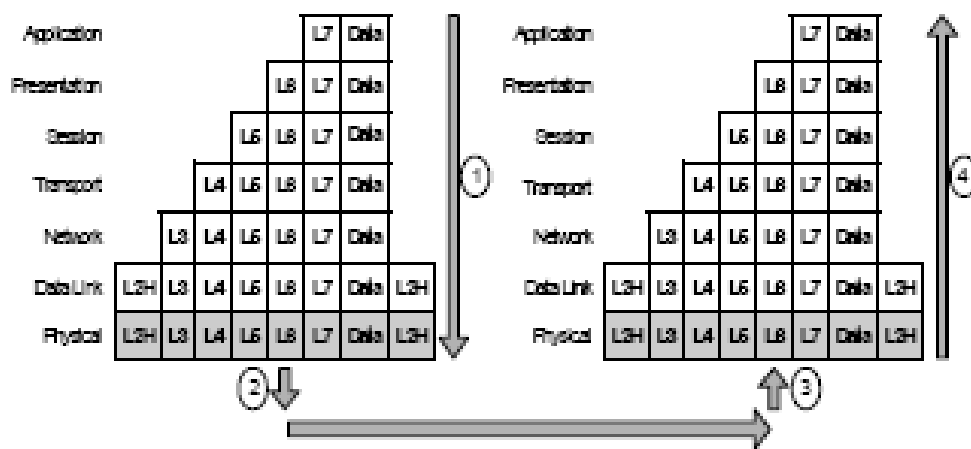
các giao thức truy cập đường truyền, cho nên các giao thức lớp trên hơn (ví dụ như IP ở lớp mạng) có thể hoạt động mà không phụ thuộc vào loại phương tiện LAN. Lớp con LLC có thể lệ thuộc vào các lớp thấp hơn trong việc cung cấp truy cập đường truyền.

Lớp con MAC cung cấp tính thứ tự truy cập vào môi trường LAN. Khi nhiều trạm cùng truy cập chia sẻ môi trường truyền, để định danh mỗi trạm, lớp cho MAC định nghĩa một trường địa chỉ phần cứng, gọi là địa chỉ MAC address. Địa chỉ MAC là một con số đơn nhất đối với mỗi giao tiếp LAN (card mạng).

Lớp vật lý (**Physical Layer**): định nghĩa các qui cách về điện, cơ, thủ tục và các đặc tả chức năng để kích hoạt, duy trì và dừng một liên kết vật lý giữa các hệ thống đầu cuối. Một số các đặc điểm trong lớp vật lý này bao gồm:

- Mức điện thế.
- Khoảng thời gian thay đổi điện thế.
- Tốc độ dữ liệu vật lý.
- Khoảng đường truyền tối đa.
- Các đầu nối vật lý.

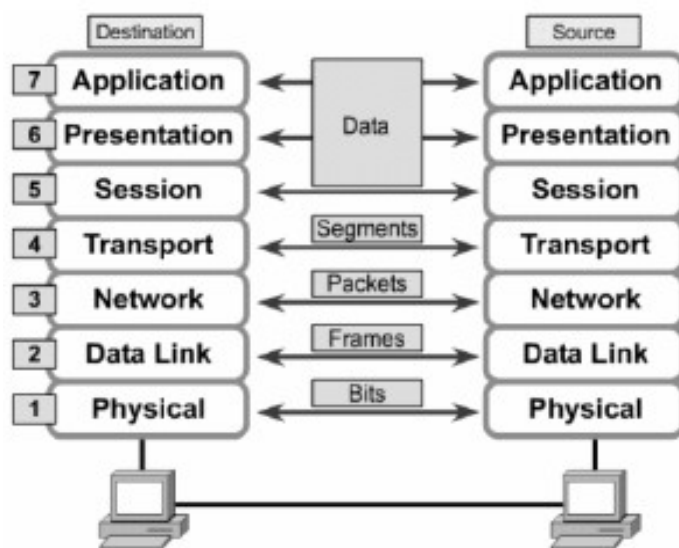
II. QUÁ TRÌNH XỬ LÝ VÀ VẬN CHUYỂN CỦA MỘT GÓI DỮ LIỆU.



Hình 3.2 – Quá trình xử lý và vận chuyển của gói tin

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

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



Hình 3.3 – Tên gọi dữ liệu ở các tầng trong mô hình OSI

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

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

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

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

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

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

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

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

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

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

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

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

Bước 4: Các chương trình phần cứng, phần mềm (trên máy nhận) gỡ bỏ **header** và **trailer** và xử lý phần dữ liệu (quá trình xử lý dữ liệu tại máy nhận). Giữa bước 1 và bước 2 là quá trình tìm đường đi của gói tin. Thông thường, máy gửi đã biết địa chỉ IP của máy nhận. Vì thế, sau khi xác định được địa chỉ IP của máy nhận thì lớp Network của máy gửi sẽ so sánh địa chỉ IP của máy nhận và địa chỉ IP của chính nó:

- Nếu cùng địa chỉ mạng thì máy gửi sẽ tìm trong bảng **MAC Table** của mình để có được địa chỉ MAC của máy nhận. Trong trường hợp không có được địa chỉ MAC tương ứng, nó sẽ thực hiện giao thức ARP để truy tìm địa chỉ MAC. Sau khi tìm được địa chỉ MAC, nó sẽ lưu địa chỉ MAC này vào trong bảng **MAC Table** để lớp **Datalink** sử dụng ở các lần gửi sau. Sau khi có địa chỉ MAC thì máy gửi sẽ gửi gói tin đi (giao thức ARP sẽ được nói thêm trong chương 6).

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

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

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

3. Chi tiết quá trình xử lý tại máy nhận

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

Bước 2: Lớp **Data Link** kiểm tra lỗi frame bằng cách kiểm tra FCS trong trailer. Nếu có lỗi thì frame bị bỏ. Sau đó kiểm tra địa chỉ lớp **Data Link** (địa chỉ MAC) xem có trùng với địa chỉ máy nhận hay không. Nếu đúng thì phần dữ liệu sau khi loại header và trailer sẽ được chuyển lên cho lớp Network.

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

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

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

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

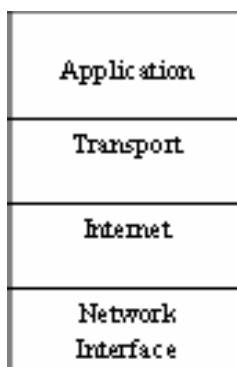
Bước 7: Lớp **Application** xử lý **header** cuối cùng. **Header** này chứa các tham số thỏa thuận giữa hai trình ứng dụng. Do vậy tham số này thường chỉ được trao đổi lúc khởi động quá trình truyền thông giữa hai trình ứng dụng.

III. MÔ HÌNH THAM CHIẾU TCP/IP 4 LỚP

1. Vai trò của mô hình tham chiếu TCP/IP.

Các bộ phận, văn phòng của Chính phủ Hoa Kỳ đã nhận thức được sự quan trọng và tiềm năng của kỹ thuật Internet từ nhiều năm trước, cũng như đã cung cấp tài chính cho việc nghiên cứu, để thực sự có được một mạng Internet toàn cầu. Sự hình thành kỹ thuật Internet là kết quả nghiên cứu dưới sự tài trợ của **Defense/Advanced Research Projects Agency (ARPA/DARPA)**. Kỹ thuật ARPA bao gồm một tập hợp của các chuẩn mạng, đặc tả chi tiết cách thức mà các máy tính thông tin liên lạc với nhau, cũng như các quy ước cho các mạng **interconnecting** và định tuyến giao thông. Tên chính thức là **TCP/IP Internet Protocol Suite** và thường được gọi là **TCP/IP**, có thể dùng để thông tin liên lạc qua tập hợp bất kỳ các mạng **interconnected**. Nó có thể dùng để liên kết mạng trong một công ty, không nhất thiết phải nối kết với các mạng khác bên ngoài.

2. Các lớp của mô hình tham chiếu TCP/IP.



Hình 3.4 – Mô hình tham chiếu TCP/IP

Mô hình tham chiếu TCP/IP tương tự như kiến trúc OSI, sau đây là một số tính chất của các lớp trong mô hình tham chiếu TCP/IP:

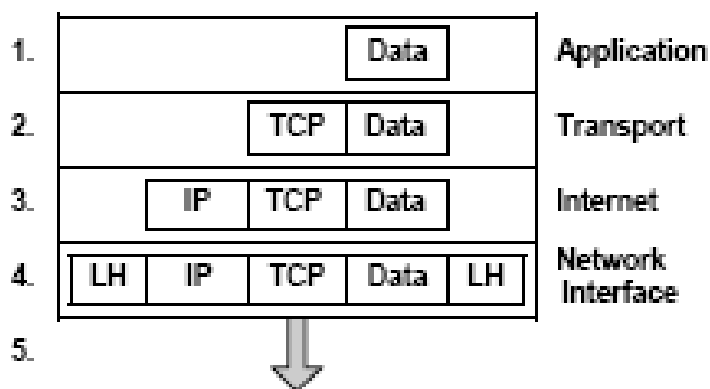
- Lớp **Application**: quản lý các giao thức, như hỗ trợ việc trình bày, mã hóa, và quản lý cuộc gọi. Lớp **Application** cũng hỗ trợ nhiều ứng dụng, như: **FTP (File Transfer Protocol)**, **HTTP (Hypertext Transfer Protocol)**, **SMTP (Simple Mail Transfer Protocol)**, **DNS (Domain Name System)**, **TFTP (Trivial File Transfer Protocol)**.

- Lớp **Transport**: đảm nhiệm việc vận chuyển từ nguồn đến đích. Tầng **Transport** đảm nhiệm việc truyền dữ liệu thông qua hai nghi thức: TCP (**Transmission Control Protocol**) và UDP (**User Datagram Protocol**).

- Lớp **Internet**: đảm nhiệm việc chọn lựa đường đi tốt nhất cho các gói tin. Nghi thức được sử dụng chính ở tầng này là nghi thức IP (**Internet Protocol**).

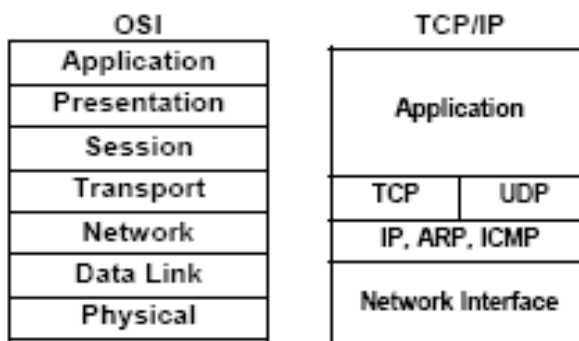
- Lớp **Network Interface**: có tính chất tương tự như hai lớp **Data Link** và **Physical** của kiến trúc OSI.

3. Các bước đóng gói dữ liệu trong mô hình TCP/IP.



Hình 3.5 – Các bước đóng gói trong mô hình TCP/IP

4. So sánh mô hình OSI và TCP/IP.



Hình 3.6 – So sánh mô hình OSI và mô hình TCP/IP

Các điểm giống nhau:

- Cả hai đều có kiến trúc phân lớp.
- Đều có lớp **Application**, mặc dù các dịch vụ ở mỗi lớp khác nhau.

- Đều có các lớp **Transport** và **Network**.
- Sử dụng kỹ thuật chuyển packet (**packet-switched**).
- Các nhà quản trị mạng chuyên nghiệp cần phải biết rõ hai mô hình trên.

Các điểm khác nhau:

- Mô hình TCP/IP kết hợp lớp **Presentation** và lớp **Session** vào trong lớp **Application**.

- Mô hình TCP/IP kết hợp lớp **Data Link** và lớp **Physical** vào trong một lớp.
- Mô hình TCP/IP đơn giản hơn bởi vì có ít lớp hơn.
- Nghi thức TCP/IP được chuẩn hóa và được sử dụng phổ biến trên toàn thế giới.

IV. KHẢO SÁT CHI TIẾT CÁC LỚP TRONG MÔ HÌNH OSI

1. Lớp DataLink (Lớp 2)

Lớp 1 liên quan đến môi trường, liên quan các tín hiệu, các luồng bit di chuyển trên môi trường, các thành phần dựa dữ liệu ra môi trường và các cấu hình khác nhau. Nó thực hiện vai trò thiết yếu cho hoạt động truyền tin khả thi giữa các máy tính, nhưng với nỗ lực một mình của nó thì không đủ. Mỗi chức năng có các hạn chế của nó. Lớp 2 hướng tới khắc phục hạn chế này. Ứng với mỗi hạn chế trong lớp 1, lớp 2 có một giải pháp. Ví dụ lớp 1 không thể thông tin với các lớp trên, lớp 2 làm việc này thông qua **LLC (Logical Link Control)**. Lớp 1 không đặt tên hay định danh cho máy tính thì lớp 2 dùng một lược đồ địa chỉ. Lớp 1 không thể quyết định máy tính nào sẽ truyền dữ liệu nhị phân từ một nhóm cùng muốn truyền tại cùng một thời điểm. Lớp 2 dùng một hệ thống gọi là **MAC (Media Access Control)**.

a. Lớp con LLC.

Lớp con **LCC** tạo ra tính năng 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** với vai trò 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 đặc biệt được yêu cầu cho đóng gói tiếp theo. Lớp phụ **LLC** quản lý hoạt động thông tin giữa các thiết bị qua một liên kết đơn trên một mạng. **LLC** được định nghĩa trong đặc tả **IEEE 802.2** và hỗ trợ các dịch vụ kết nối có cả tạo cầu nối và không tạo cầu nối, được dùng bởi các giao thức lớp cao hơn. **IEEE 802.2** định nghĩa ra một số **field** trong các **frame** của lớp liên kết dữ liệu cho phép nhiều giao thức lớp cao hơn chia sẻ một liên kết vật lý đơn.

b. Lớp con MAC.

Lớp con **MAC** đề cập đến các giao thức chủ yếu phải theo để truy xuất vào môi trường vật lý. Tóm lại, lớp 2 có 4 khái niệm chính mà cần phải biết:

- Lớp 2 thông tin với các lớp trên thông qua **LLC**.
- Lớp 2 dùng chuẩn địa chỉ hóa ngang bằng (đó là gán các định danh duy nhất các địa chỉ).
- Lớp 2 dùng kỹ thuật đóng frame để tổ chức hay nhóm dữ liệu.
- Lớp 2 dùng **MAC** để chọn máy tính nào sẽ truyền các dữ liệu nhị phân, từ một nhóm trong đó tất cả các máy tính đều muốn truyền cùng một lúc.

c. Quá trình tìm địa chỉ MAC

Với mạng **TCP/IP**, thì gói tin phải chứa cả địa chỉ **MAC** đích và địa chỉ **IP** đích. Nếu một trong hai địa chỉ này không đúng thì gói tin cũng xem như là không gửi được đến đích. **ARP** là một giao thức dùng để tìm địa chỉ **MAC** của một thiết bị mạng dựa trên địa chỉ **IP** đã biết.

Một vài thiết bị có lưu trữ bảng chứa địa chỉ **IP** và địa chỉ **MAC** tương ứng với **IP** đó (của các thiết bị trong cùng mạng **LAN** với nó). Bảng này được gọi là bảng **ARP**. Bảng **ARP** này được lưu giữ trong **RAM**, và khi thiết bị gửi gói tin lên mạng thì nó sử dụng thông tin trong bảng **ARP** này.

Có 2 cách để thu thập thông tin cho bảng địa chỉ **MAC**.

- Khi có một gói tin được gửi trên đường truyền, thiết bị luôn kiểm tra địa chỉ đích của gói tin (địa chỉ **IP** và địa chỉ **MAC**) có phải là của mình hay không? Sau khi kiểm tra, địa chỉ **IP** và địa chỉ **MAC** đều được lưu vào trong bảng **ARP**.

- Cách thu thập thông tin thứ 2 là thu thập qua gói tin broadcast **ARP request**. Khi máy tính gửi một gói tin **broadcast** dạng **ARP request** thì tất cả các máy khác trên mạng đều phân tích gói tin này.

+ Nếu như địa chỉ **IP** đích của thiết bị mạng cần tìm là địa chỉ thuộc cùng đường mạng với địa chỉ máy gửi.

❖ Nếu máy đó nhận được gói tin thì máy sẽ trả lời bằng một gói tin **ARP reply** (trong đó có địa chỉ **MAC** và địa chỉ **IP** của máy).

❖ Nếu địa chỉ đích không tồn tại hoặc thiết bị chưa hoạt động thì sẽ không có gói tin **ARP reply**.

+ Nếu địa chỉ **IP** đích của thiết bị mạng cần tìm là địa chỉ khác đường mạng thì việc tìm địa chỉ **MAC** thường được làm thông qua **Router**, có hai cách để thực hiện:

❖ Nếu **Router** bật tính năng cho phép thực hiện **Proxy ARP**. Thì khi nhận được gói tin **broadcast ARP request**, **Router** sẽ kiểm tra xem địa chỉ đích có khác đường mạng với địa chỉ nguồn không? Nếu khác địa chỉ nguồn thì **Router** sẽ trả về một **ARP response**

- ❖ để trả lời (trong gói tin này sẽ chứa địa chỉ **MAC** – địa chỉ **MAC** của **interface** nhận gói tin **ARP request**).
- ❖ Nếu máy tính gửi có khai báo địa chỉ **Default Gateway** thì máy tính sẽ gửi gói tin đến **Default Gateway** để **Default Gateway** gửi tiếp.

Nếu máy tính nguồn không khai báo **Default Gateway** và tính năng thực hiện **Proxy ARP** không bật thì hai máy tính có địa chỉ đường mạng khác nhau sẽ không thể liên lạc được với nhau.

d. Các phương pháp truy cập đường truyền.

Cắm sóng đa truy (CSMA/CD).

Khía cạnh thú vị nhất của **Ethernet** là kỹ thuật đường dùng trong việc phối hợp truyền thông. Mạng **Ethernet** không điều khiển tập trung đến việc các máy luân phiên chia sẻ đường cáp. Lúc đó các máy nối với **Ethernet** sẽ tham gia vào một lược đồ phối hợp phân bố gọi là Cắm sóng đa truy (**CSMA – Carrier Sence with Multiple Access**). Để xác định cáp có đang dùng không, máy tính có thể kiểm tra sóng mang (**carrier** - dạng tín hiệu mà máy tính truyền trên cáp). Nếu có sóng mang, máy phải chờ cho đến khi bên gửi kết thúc. Về mặt kỹ thuật, kiểm tra một sóng mang được gọi là cắm sóng (**carrier sence**), và ý tưởng sử dụng sự hiện hữu của tín hiệu để quyết định khi nào thì truyền gọi là Cắm sóng đa truy (**CSMA**).

Vì **CSMA** cho phép mỗi máy tính xác định đường cáp chia sẻ có đang được máy khác sử dụng hay không nên nó ngăn cấm một máy cắt ngang việc truyền đang diễn ra. Tuy nhiên, **CSMA** không thể ngăn ngừa tất cả các xung đột có thể xảy ra. Để hiểu lý do tại sao, hãy tưởng tượng chuyện gì xảy ra nếu hai máy tính ở hai đầu cáp đang nghỉ nhận được yêu cầu gửi khung. Cả hai cùng kiểm tra tín hiệu mang, cùng thấy cáp đang trống và cả hai bắt đầu gửi khung. Các tín hiệu phát từ hai máy sẽ gây nhiễu lẫn nhau. Hai tín hiệu gây nhiễu lẫn nhau gọi là xung đột hay đụng độ (**collision**). Vùng có khả năng xảy ra đụng độ khi truyền gói tin được gọi là **Collision Domain**. Máy đầu tiên trên đường truyền phát hiện được xung đột sẽ phát sinh tín hiệu xung đột cho các máy khác. Tuy xung đột không làm hỏng phần cứng nhưng nó tạo ra một sự truyền thông méo mó và hai khung nhận được sẽ không chính xác. Để xử lý các biến cố như vậy, **Ethernet** yêu cầu mỗi bên gửi tín hiệu giám sát (**monitor**) trên cáp để bảo đảm không có máy nào khác truyền đồng thời. Khi máy gửi phát hiện đụng độ, nó ngưng truyền ngay lập tức, và tiếp tục bắt đầu lại quá trình chuẩn bị việc truyền tin sau một khoảng thời gian ngẫu nhiên. Việc giám sát cáp như vậy gọi là phát hiện đụng (**CD – collision detect**), và kỹ thuật **Ethernet** đó được gọi là Cắm sóng đa truy với phát hiện đụng độ (**CSMA/CD**).

Chuyển thẻ bài (Token-passing):

Chúng ta đã biết mạng **LAN** vòng nối các máy thành một vòng tròn kín. Hầu hết các **LAN** dùng đồ hình vòng cũng sử dụng một kỹ thuật truy cập gọi là chuyển

thẻ bài (**token-passing**). Khi một máy cần chuyển dữ liệu, nó phải chờ phép trước khi truy cập mạng. Khi giữ được thẻ bài, máy gửi hoàn toàn giữ quyền điều khiển vòng – không có các truyền thông nào khác xảy ra đồng thời. Khi máy gửi truyền frame, các bit chuyển từ máy gửi sang máy kế, và chuyển tiếp sang máy kế và cứ thế cho đến khi các **bit** đi hết vòng và trở về máy gửi.

Tín bài là một khuôn mẫu bit khác với khung dữ liệu thông thường. Thực chất là tín bài trao quyền cho một máy được gửi khung. Như vậy trước khi gửi khung, máy phải chờ tín bài đến. Khi tín bài đến, máy tạm thời loại bỏ tín bài ra khỏi vòng và bắt đầu truyền dữ liệu trên vòng. Tuy có thể có nhiều khung đang chờ gửi đi nhưng máy chỉ gửi một **frame** và truyền lại tín bài. Không như khung dữ liệu dữ liệu đi hết một vòng khi được gửi, tín bài chỉ đi thẳng từ một máy đến máy kế tiếp.

Nếu tất cả các máy trên mạng vòng cần gửi dữ liệu, chuyển tín bài bảo đảm chúng sẽ đến lượt và mỗi máy sẽ gửi một frame trước khi chuyển tín bài. Lưu ý là lược đồ này bảo đảm truy cập công bằng: khi tín bài chuyển trên vòng, mỗi máy sẽ có cơ hội sử dụng mạng. Nếu một máy nào đó không gửi dữ liệu khi nhận được tín bài, nó chỉ việc chuyển tín bài mà không trì hoãn. Trong trường hợp đặc biệt không có máy nào truyền dữ liệu, tín bài sẽ quay vòng liên tục, mỗi máy khi nhận được tín bài sẽ chuyển ngay lập tức đến máy kế. Thời gian chuyển tín bài một vòng trong trường hợp này là cực ngắn, vì 2 lý do. Thứ nhất, vì tín bài nhỏ nên có thể chuyển rất nhanh trên đường dây. Thứ hai, sự chuyển tiếp trên mỗi máy được thực hiện bởi phần cứng vòng, điều đó có nghĩa tốc độ không phụ thuộc vào CPU của máy.

2. Lớp Network (lớp 3)

Chức năng quan trọng nhất của lớp **Network** là định tuyến (**Routing**), định tuyến là quá trình chuyển thông tin qua mạng từ nơi gửi tới nơi nhận. Định tuyến có hai thành phần là chuyển mạch (**switching**) và chọn đường (**path determination**).

Trong quá trình **switching**, bên gửi (**source or sender**) thêm vào địa chỉ bên gửi, địa chỉ bên nhận, địa chỉ vật lý (**MAC**), địa chỉ của **Router** đầu tiên (hay là địa chỉ **Default-Gateway**) mà packet tới. Khi packet tới **Router**, **Router** sẽ xác định địa chỉ **IP** đích của **packet** (còn gọi là **destination IP address**), nếu như **Router** không nhận ra **IP** đích thì nó sẽ bỏ **packet**, nếu ngược lại thì **Router** sẽ chuyển **packet** tới địa chỉ đích hoặc chuyển packet tới **Router** kế tiếp (**next Router**), khi đó **Router** nó sẽ thay thế **MAC** nguồn, và **MAC** đích bằng **MAC** trên **interface** của nó và **MAC** trên **next hop Router**, khi **packet** chuyển qua mạng lớn (qua nhiều **Router**) thì địa chỉ **IP** nguồn (**source address**) và địa chỉ **IP** đích (**destination address**) không thay đổi nhưng địa chỉ vật lý (địa chỉ **MAC**) bị thay đổi tại mỗi hop.

Thành phần thứ hai của **routing** là **Path-Determination**, **Router** cần có một số cách xác định con đường đi ngắn nhất để chuyển packet tới đích, **Router** cần có nhiều thông tin từ người quản trị (người quản trị phải làm công việc định tuyến) hay từ các **Router** khác để xây dựng bảng **routing** (**Router** tự học định tuyến thông qua các giao thức) mà thông tin này giúp cho nó định tuyến packet đi tới đích.

Trong bảng **routing** địa chỉ mạng đích được ánh xạ tới **interface** (cổng) thích hợp trên **Router**, thông qua **interface** này packet có thể đi tới nó.

Khi có sự thay đổi trên mạng các **Router** trao đổi với nhau bằng các **exchanging message** để cập nhật lại bảng **routing**. Các **exchanging message** bao gồm:

- **Routing update message**.
- **Link-state advertiment** (trạng thái của sender's link).

Theo định nghĩa của một số nghi thức **routing** như **RIP**, **IGRP**,... cứ sau một khoảng thời gian (**interval time**) nó sẽ gửi **update message** tới các **Router** khác để cập nhật về sự thay đổi thông tin trên mạng. Khi các **Router** này nhận được thông tin **update**, nó sẽ kiểm tra trong bảng **routing table** của nó với thông tin **update** nếu có sự thay đổi thì nó sẽ xóa **entry** tương ứng và cập nhật thông tin mới vào, ngược lại thì nó sẽ không cập nhật thông tin.

Routing Algorithm là thuật toán định tuyến cho phép chọn **Router**, chọn con đường đi tốt nhất để gửi dữ liệu đến đích. **Routing Algorithm** tùy thuộc vào các yếu tố sau :

- **Design**.
- **Metrics**.
- **Type**.

Design bao gồm:

- Tính đơn giản (**simplicity**) là thành phần rất quan trọng trong hệ thống giúp giới hạn tài nguyên vật lý (**physical resource**).

- Tính linh hoạt (**plexibility**) để cho phép mạng thích ứng nhanh với sự thay đổi và phát triển của hệ thống, ví dụ như sự thay đổi về băng thông kích thước hàng đợi, độ trễ,...

- Sự hội tụ (**convergence**) tính hội tụ thông tin là mục đích quan trọng của thuật toán **routing**, tính hội tụ nhanh làm cho thông tin trong bảng **routing** được thống nhất một cách nhanh chóng. Ngược lại nó sẽ làm phá vỡ tính thống nhất thông tin định tuyến giữa các **Router**.

- Tính tối ưu (**optimality**): là khả năng mà nghi thức định tuyến lựa chọn đường đi tốt nhất để truyền dữ liệu, để xác định con đường đi tốt nhất **Router** dựa vào metric và **weighting** (trọng lượng) của mỗi **metric**.

Metric được sử dụng trong thuật toán định tuyến để lựa chọn con đường đi tốt nhất, nó bao gồm:

- **Hop count và path length.**
- **Reliability.**
- **Load.**
- **Delay.**
- **Bandwidth.**
- **Maximum Transmission Unit (MTU).**

Hop count là số lượng host (hay là số lượng **Router**) mà packet phải đi qua từ nguồn tới đích.

Mỗi một đường truyền được gán bởi một giá trị, chỉ có người quản trị mạng mới thay đổi giá trị này, tổng giá trị của các đường truyền đó gọi là **path length**.

Reliability là **metric** cho phép đánh giá mức độ lỗi của một đường truyền.

Load khả năng tải hiện tại trên đường truyền (**busy link**) dựa vào số lượng packet được truyền trong thời gian 1 giây, mức độ xử lý hiện tại của cpu (**CPU Utilization**).

Delay metric thực sự để đo lường một số tác động của một số đại lượng trên đường truyền như băng thông (**bandwidth**), tắc nghẽn đường truyền (**congestion**), khoảng cách đường truyền (**distance**), khả năng mang thông tin trên đường truyền còn gọi là băng thông của đường truyền được tính bằng số bit/giây mà đường truyền đó có thể truyền thông tin, số lượng traffic trên đường truyền quá nhiều sẽ làm giảm băng thông có sẵn cho đường truyền.

MTU là chiều dài tối đa của thông điệp (tính bằng **byte**) mà nó có thể truyền trên đường truyền. MTU của mỗi môi truyền truyền vật lý thì khác nhau. Ví dụ **MTU** cho **ethernet** là 1500.

3. Lớp Transport (lớp 4)

Các dịch vụ trên lớp **transport** cho phép phân mảnh và tập hợp dữ liệu vào cùng transport-layer data stream, **Transport-layer data stream** là một kết nối logic giữa bên gửi và bên nhận trên mạng. Lớp **Transport** cung cấp các đặc tính sau :

- **Reliability** (tin cậy) bằng cách đánh số thứ tự của các **segment (source sequence)**, bên nhận thông báo cho bên gửi biết rằng nó đã nhận được dữ liệu bằng cách thông báo các **ACK (acknowledgements)**.

- **Flow Control**: là kỹ thuật cho phép điều khiển buffer bên nhận, bên nhận sử dụng kỹ thuật này để ngăn không cho bên gửi gửi dữ liệu quá nhanh làm tràn buffer của bên nhận.

- Hai **protocol** ở lớp **transport layer** là **TCP** và **UDP**,

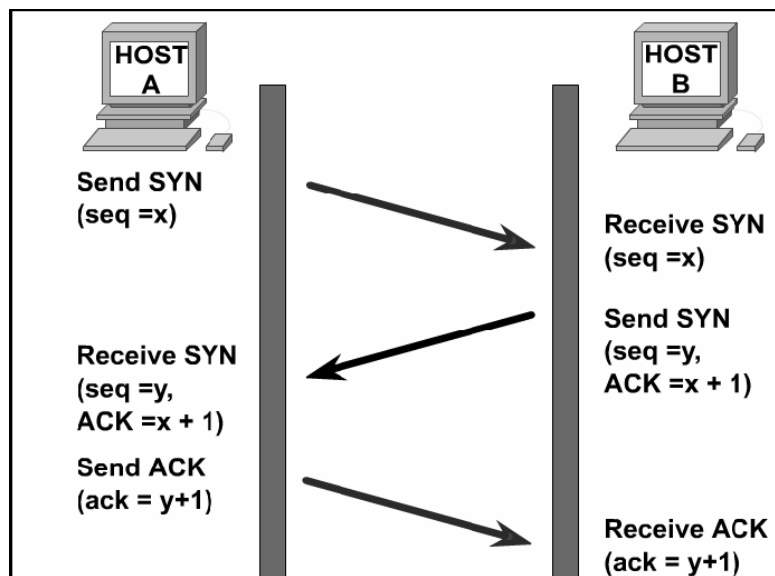
a. Giao thức TCP (TCP protocol).

TCP cung cấp kết nối tin cậy giữa hai máy tính, kết nối được thiết lập trước khi dữ liệu bắt đầu truyền. **TCP** còn gọi là nghi thức hướng kết nối, với nghi thức **TCP** thì quá trình hoạt động trải qua ba bước sau:

- Thiết lập kết nối (**connection establishment**).
- Truyền dữ liệu (**data transfer**).
- Kết thúc kết nối (**connection termination**).

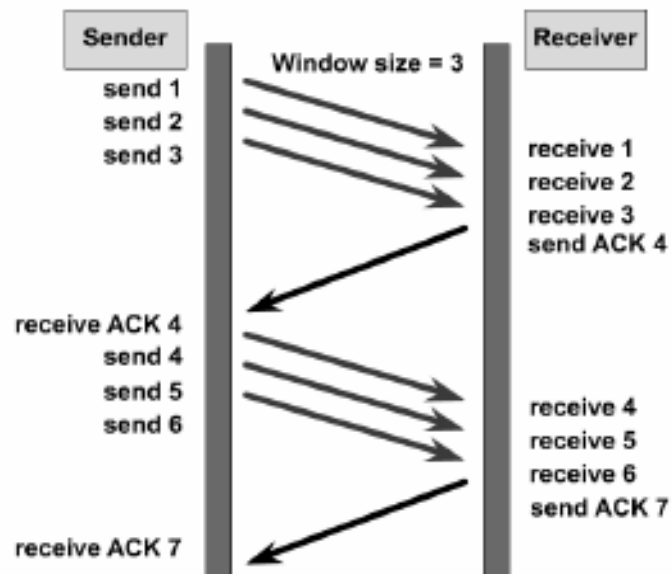
TCP phân chia các thông điệp thành các segment, sau đó nó ráp các segment này lại tại bên nhận, và nó có thể truyền lại những gói dữ liệu nào đã bị mất. Với **TCP** thì dữ liệu đến đích là đúng thứ tự, **TCP** cung cấp **Virtual Circuit** giữa các ứng dụng bên gửi và bên nhận.

Giao thức **TCP** thiết lập một kết nối bằng phương pháp “Bắt tay 3 lần” (**three-way handshake**).



Hình 3.7 – Cách thiết lập kết nối của giao thức **TCP**.

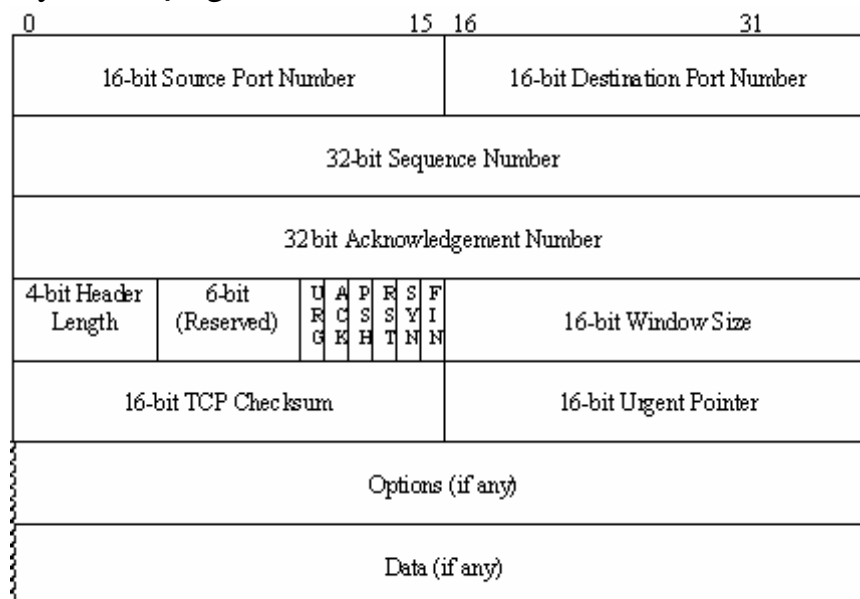
Hình vẽ dưới đây là một ví dụ về cách thức truyền, nhận gói tin bằng giao thức **TCP**.



Hình 3.8 – Minh họa cách truyền, nhận gói tin trong giao thức TCP.

Giao thức TCP là giao thức có độ tin cậy cao, nhờ vào phương pháp truyền gói tin, như cơ chế điều khiển luồng (**flow control**), các gói tin ACK,...

Hình vẽ sau đây thể hiện gói tin của TCP.



Hình 3.9 – Cấu trúc gói tin của TCP.

Các thành phần trong gói tin:

- **Source port:** port nguồn
- **Destination Port:** port đích
- **Sequence number:** số tuần tự (để sắp xếp các gói tin theo đúng trật tự của nó).

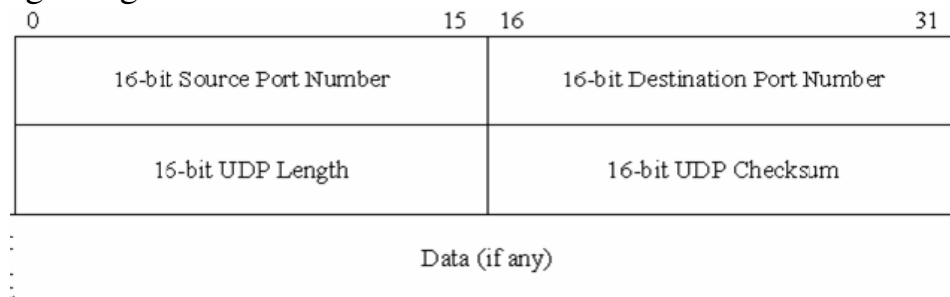
- **Acknowledgment number (ACK số):** số thứ tự của Packet mà bên nhận đang chờ đợi.
- **Header Length:** chiều dài của gói tin.
- **Reserved:** trả về 0
- **Code bit:** các cờ điều khiển.
- **Windows:** kích thước tối đa mà bên nhận có thể nhận được
- **Checksum:** máy nhận sẽ dùng 16 bit này để kiểm tra dữ liệu trong gói tin có đúng hay không.
- **Data:** dữ liệu trong gói tin (nếu có).

b. *Giao thức UDP (UDP protocol).*

UDP không giống như **TCP**, **UDP** là nghi thức phi kết nối, nghĩa là dữ liệu gửi tới đích là không tin cậy. Bởi vì kết nối không được tạo trước khi dữ liệu truyền, do đó **UDP** nhanh hơn **TCP**.

UDP là nghi thức không tin cậy, nó không đảm bảo dữ liệu đến đích là không bị mất, đúng thứ tự mà nó nhờ các nghi thức ở lớp trên đảm nhận chức năng này. **UDP** có ưu thế hơn **TCP**:

- Nhờ vào việc không phải thiết lập kết nối trước khi thật sự truyền dẫn dữ liệu nên truyền với tốc độ nhanh hơn.
- Bên nhận không cần phải trả về gói tin xác nhận (**ACK**) nên giảm thiểu sự lãng phí băng thông.



Hình 3.10 – Cấu trúc gói tin của **UDP**.

Các thành phần trong gói tin **UDP**:

- **Source Port:** port nguồn.
- **Destination Port:** port đích.
- **UDP Length:** chiều dài của gói tin.
- **UDP Checksum:** dùng để kiểm tra gói tin có bị sai lệch hay không
- **Data:** dữ liệu đi kèm trong gói tin (nếu có).

c. *Khái niệm Port.*

Trong cùng một thời điểm, một máy tính có thể có nhiều chương trình đang chạy. Vậy làm sao để xác định một gói tin sẽ được chương trình nào sử dụng?

Khái niệm **Port** ra đời để giải quyết chuyện đó. Mỗi chương trình ứng dụng mạng đều có một **Port** xác định. Để gửi gói tin đến một chương trình tại máy tính A, ta chỉ cần gửi gói tin đến địa chỉ **IP** của máy A, và **Port** mà chương trình đó đang sử dụng.

TCP hoặc **UDP** dùng **port** hoặc **socket**, nó là con số mà thông qua đó thông tin được truyền lên các lớp cao hơn. Các con số **port** được dùng trong việc lưu vết các cuộc hội thoại khác nhau trên mạng xảy ra trong cùng một thời điểm. **Port** là một loại địa chỉ **logic** trên một máy tính, là con số 2 byte. Các **port** có giá trị nhỏ hơn 1024 được dùng làm các **port** chuẩn. Các ứng dụng dùng port riêng có giá trị lớn hơn 1024. Các giá trị **port** được chứa trong phần địa chỉ nguồn và đích của mỗi **segment TCP**.

Một ứng dụng có thể sử dụng port riêng trong miền cho mình để giao dịch trên mạng nhưng chú ý là không được trùng với các **port** chuẩn.

Ví dụ một số port chuẩn mà các phần mềm sử dụng

- **HTTP**: Port number 80
- **FTP**: Port number 21
- **DNS**: Port number 53
- **Telnet**: Port number 23
- **SMTP**: Port number 25
- **TFTP**: Port number 69
- **SNMP**: Port number 161
- **RIP**: Port number 520

CHƯƠNG 4

ĐỊA CHỈ IP

I. TỔNG QUAN VỀ ĐỊA CHỈ IP

Là địa chỉ có cấu trúc, được chia làm hai hoặc ba phần là: **network_id**&**host_id** hoặc **network_id**&**subnet_id**&**host_id**.

Là một con số có kích thước 32 bit. Khi trình bày, người ta chia con số 32 bit này thành bốn phần, mỗi phần có kích thước 8 bit, gọi là **octet** hoặc **byte**. Có các cách trình bày sau:

- Ký pháp thập phân có dấu chấm (**dotted-decimal notation**). Ví dụ: 172.16.30.56.
- Ký pháp nhị phân. Ví dụ: 10101100 00010000 00011110 00111000.
- Ký pháp thập lục phân. Ví dụ: AC 10 1E 38.

Không gian địa chỉ IP (gồm 232 địa chỉ) được chia thành nhiều lớp (class) để dễ quản lý. Đó là các lớp: A, B, C, D và E; trong đó các lớp A, B và C được triển

khai để đặt cho các host trên mạng **Internet**; lớp D dùng cho các nhóm **multicast**; còn lớp E phục vụ cho mục đích nghiên cứu.

Địa chỉ IP còn được gọi là địa chỉ **logical**, trong khi địa chỉ **MAC** còn gọi là địa chỉ vật lý (hay địa chỉ **physical**).

II. MỘT SỐ KHÁI NIỆM VÀ THUẬT NGỮ LIÊN QUAN.

Network_id: là giá trị để xác định đường mạng. Trong số 32 bit dùng địa chỉ IP, sẽ có một số bit đầu tiên dùng để xác định **network_id**. Giá trị của các bit này được dùng để xác định đường mạng.

Host_id: là giá trị để xác định host trong đường mạng. Trong số 32 bit dùng làm địa chỉ IP, sẽ có một số bit cuối cùng dùng để xác định **host_id**. **Host_id** chính là giá trị của các bit này.

Địa chỉ **host**: là địa chỉ IP, có thể dùng để đặt cho các interface của các host. Hai host nằm thuộc cùng một mạng sẽ có **network_id** giống nhau và **host_id** khác nhau.

Mạng (**network**): một nhóm nhiều host kết nối trực tiếp với nhau. Giữa hai host bất kỳ không bị phân cách bởi một thiết bị layer 3. Giữa mạng này với mạng khác phải kết nối với nhau bằng thiết bị layer 3.

Địa chỉ mạng (**network address**): là địa chỉ IP dùng để đặt cho các mạng. Địa chỉ này không thể dùng để đặt cho một **interface**. Phần **host_id** của địa chỉ chỉ chứa các bit 0. Ví dụ 172.29.0.0 là một địa chỉ mạng.

Mạng con (**subnet network**): là mạng có được khi một địa chỉ mạng (thuộc lớp A, B, C) được phân chia nhỏ hơn (để tận dụng số địa chỉ mạng được cấp phát). Địa chỉ mạng con được xác định dựa vào địa chỉ IP và mặt nạ mạng con (**subnet mask**) đi kèm (sẽ đề cập rõ hơn ở phần sau).

Địa chỉ **broadcast**: là địa chỉ IP được dùng để đại diện cho tất cả các host trong mạng. Phần **host_id** chỉ chứa các bit 1. Địa chỉ này cũng không thể dùng để đặt cho một host được. Ví dụ 172.29.255.255 là một địa chỉ **broadcast**.

Các phép toán làm việc trên bit:

Phép AND			Phép OR		
A	B	A and B	A	B	A or B
1	1	1	1	1	1
1	0	0	1	0	1
0	1	0	0	1	1
0	0	0	0	0	0

Ví dụ sau minh họa phép AND giữa địa chỉ 172.29.14.10 và mask 255.255.0.0

$$172.29.14.10 = 10101100000111010000111000001010 \text{ AND}$$

$$255.255.0.0 = 11111111111111110000000000000000$$

$$172.29.0.0 = 10101100000111010000000000000000$$

Mặt nạ mạng (**network mask**): là một con số dài 32 bit, là phương tiện giúp máy xác định được địa chỉ mạng của một địa chỉ IP (bằng cách AND giữa địa chỉ IP với mặt nạ mạng) để phục vụ cho công việc routing. Mặt nạ mạng cũng cho biết số bit nằm trong phần **host_id**. Được xây dựng theo cách: bật các bit tương ứng với phần **network_id** (chuyển thành bit 1) và tắt các bit tương ứng với phần **host_id** (chuyển thành bit 0).

Mặt nạ mặc định của lớp A: sử dụng cho các địa chỉ lớp A khi không chia mạng con, mặt nạ có giá trị 255.0.0.0.

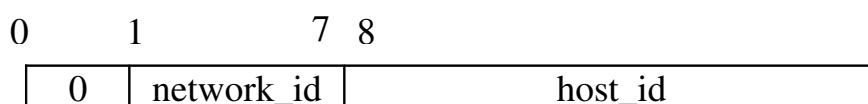
Mặt nạ mặc định của lớp B: sử dụng cho các địa chỉ lớp B khi không chia mạng con, mặt nạ có giá trị 255.255.0.0.

Mặt nạ mặc định của lớp C: sử dụng cho các địa chỉ lớp C khi không chia mạng con, mặt nạ có giá trị 255.255.255.0.

III. GIỚI THIỆU CÁC LỚP ĐỊA CHỈ.

1. Lớp A.

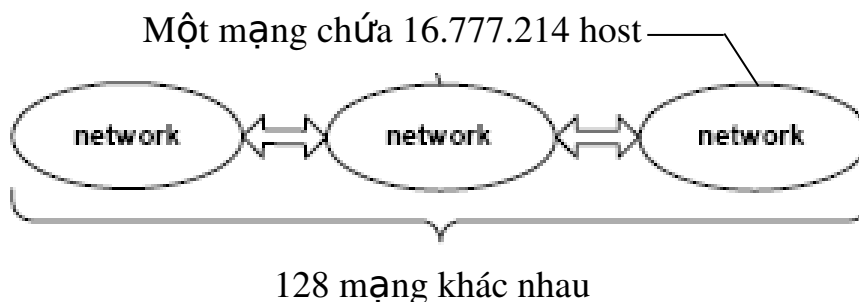
Dành một byte cho phần **network_id** và ba byte cho phần **host_id**.



Để nhận diện ra lớp A, bit đầu tiên của byte đầu tiên phải là bit 0. Dưới dạng nhị phân, byte này có dạng 0xxxxxxx. Vì vậy, những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 0 (00000000) đến 127 (01111111) sẽ thuộc lớp A. Ví dụ địa chỉ 50.14.32.8 là một địa chỉ lớp A ($50 < 127$).

Byte đầu tiên này cũng chính là **network_id**, trừ đi bit đầu tiên làm ID nhận dạng lớp A, còn lại bảy bit để đánh thứ tự các mạng, ta được 128 (2⁷) mạng lớp A khác nhau. Bỏ đi hai trường hợp đặc biệt là 0 và 127. Kết quả là lớp A chỉ còn 126 (2⁷-2) địa chỉ mạng, 1.0.0.0 đến 126.0.0.0.

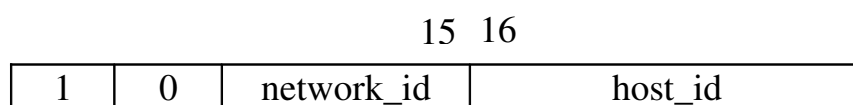
Phần **host_id** chiếm 24 bit, tức có thể đặt địa chỉ cho 16.777.216 (2²⁴) host khác nhau trong mỗi mạng. Bỏ đi một địa chỉ mạng (phần **host_id** chứa toàn các bit 0) và một địa chỉ **broadcast** (phần **host_id** chứa toàn các bit 1) như vậy có tất cả 16.777.214 (2²⁴-2) host khác nhau trong mỗi mạng lớp A. Ví dụ, đối với mạng 10.0.0.0 thì những giá trị host hợp lệ là 10.0.0.1 đến 10.255.255.254.



Hình 4.1 – Mô tả các mạng lớp A kết nối với nhau

2. Lớp B.

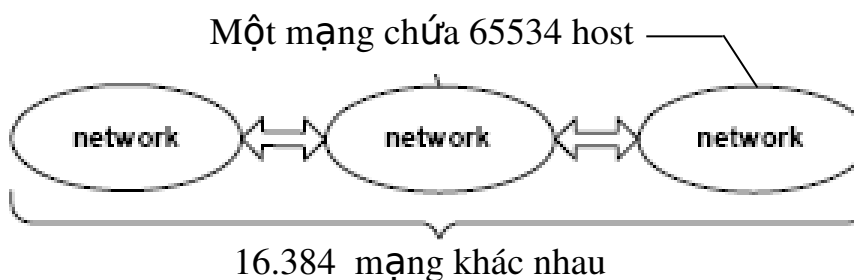
Dành hai byte cho mỗi phần **network_id** và **host_id**.



Dấu hiệu để nhận dạng địa chỉ lớp B là byte đầu tiên luôn bắt đầu bằng hai bit 10. Dưới dạng nhị phân, octet có dạng 10xxxxxx. Vì vậy những địa chỉ nằm trong khoảng từ 128 (10000000) đến 191 (10111111) sẽ thuộc về lớp B. Ví dụ 172.29.10.1 là một địa chỉ lớp B ($128 < 172 < 191$).

Phần **network_id** chiếm 16 bit bỏ đi 2 bit làm ID cho lớp, còn lại 14 bit cho phép ta đánh thứ tự 16.384 (214) mạng khác nhau (128.0.0.0 đến 191.255.0.0)

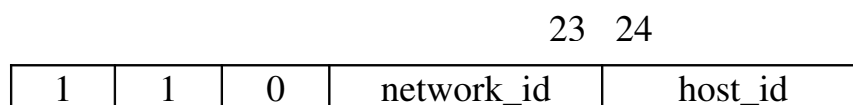
Phần **host_id** dài 16 bit hay có 65536 (216) giá trị khác nhau. Trừ 2 trường hợp đặc biệt còn lại 65534 host trong một mạng lớp B. Ví dụ, đối với mạng 172.29.0.0 thì các địa chỉ host hợp lệ là từ 172.29.0.1 đến 172.29.255.254.



Hình 4.2 – Mô tả các mạng lớp B kết nối với nhau

3. Lớp C.

Dành ba byte cho phần **network_id** và một byte cho phần **host_id**.



Byte đầu tiên luôn bắt đầu bằng ba bit 110 và dạng nhị phân của octet này là 110xxxxx. Như vậy những địa chỉ nằm trong khoảng từ 192 (11000000) đến 223

(**11011111**) sẽ thuộc về lớp C. Ví dụ một địa chỉ lớp C là 203.162.41.235 ($192 < 203 < 223$).

Phần **network_id** dùng ba byte hay 24 bit, trừ đi 3 bit làm ID của lớp, còn lại 21 bit hay 2.097.152 (221) địa chỉ mạng (từ **192.0.0.0** đến **223.255.255.0**).

Phần **host_id** dài một byte cho 256 (28) giá trị khác nhau. Trừ đi hai trường hợp đặc biệt ta còn 254 host khác nhau trong một mạng lớp C. Ví dụ, đối với mạng 203.162.41.0, các địa chỉ host hợp lệ là từ 203.162.41.1 đến 203.162.41.254.

4. Lớp D và E.

Các địa chỉ có byte đầu tiên nằm trong khoảng 224 đến 255 là các địa chỉ thuộc lớp D hoặc E.

1	1	1	0	multicast address
---	---	---	---	-------------------

1	1	1	1	0	để dành
---	---	---	---	---	---------

- Lớp D : Dùng để gửi IP datagram tới nhóm các host trên một mạng
- Lớp E : Dự phòng trong tương lai
- ❖ Một địa chỉ có host_id = 0 được dùng để hướng tới tất cả các host nối vào mạng định danh bởi network_id và gọi là địa chỉ broadcast trực tiếp.
- ❖ Nếu tất cả toàn số 1 dùng để hướng tới tất cả các host trong liên mạng (nhân giải b-node).
- ❖ Địa chỉ 0.0.0.0 được sử dụng trong bảng routing để chỉ đến điểm vào mạng cho địa chỉ bộ routing mặc định.

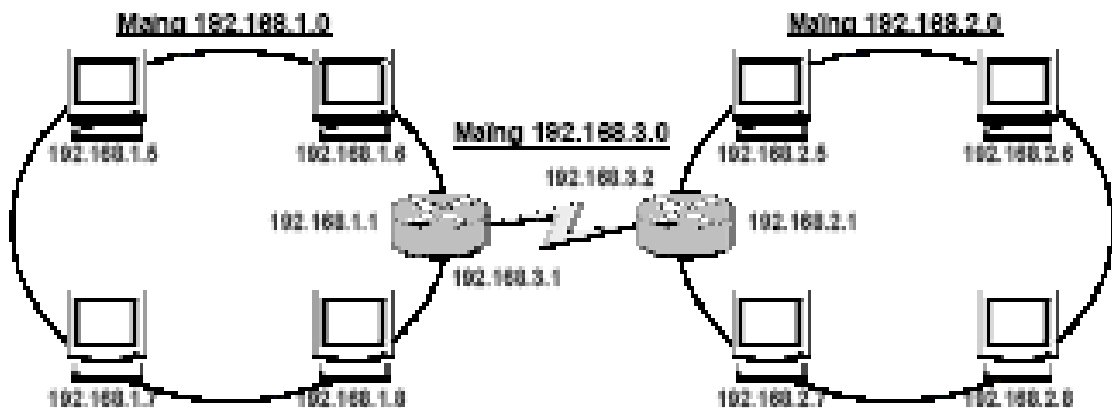
5. Bảng tổng kết.

	Lớp A	Lớp B	Lớp C
Giá trị của byte đầu tiên	0 – 127	128 – 191	192 – 223

Số byte phần Network_id	1	2	3
Số byte phần Host_id	3	2	1
Network mask	255.0.0.0	255.255.0.0	255.255.255.0
Network Address	XX.0.0.0	XX.XX.0.0	XX.XX.XX.0
Số đường mạng	128	16.384	2.097.152
Số host trên mỗi đường mạng	16.777.214	65.534	254

* Ghi chú: XX là số bất kỳ trong miền cho phép.

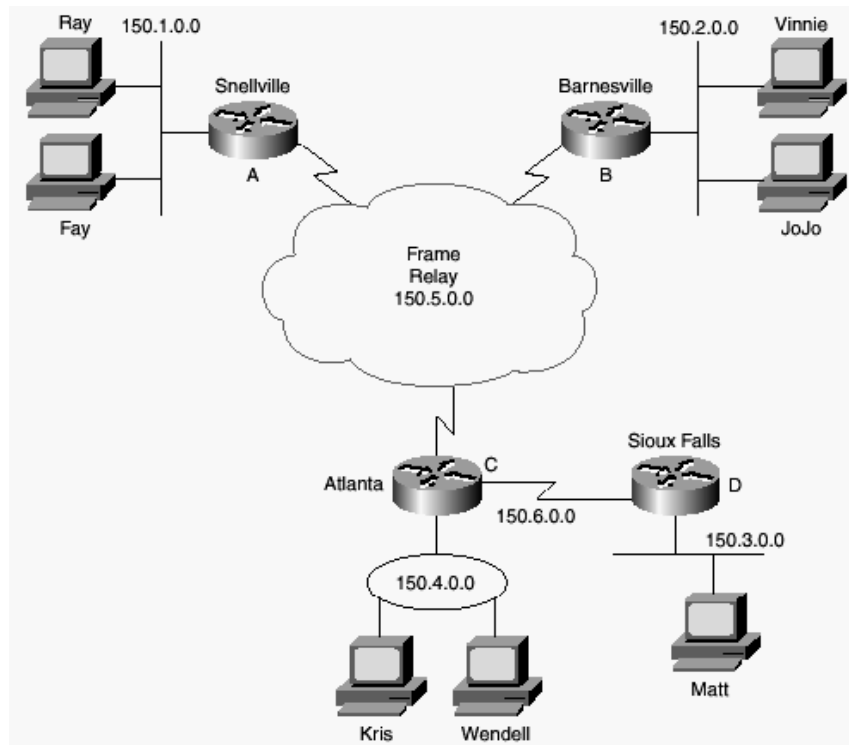
6. Ví dụ cách triển khai đặt địa chỉ IP cho một hệ thống mạng.



Hình 4.3 – Minh họa một hệ thống mạng

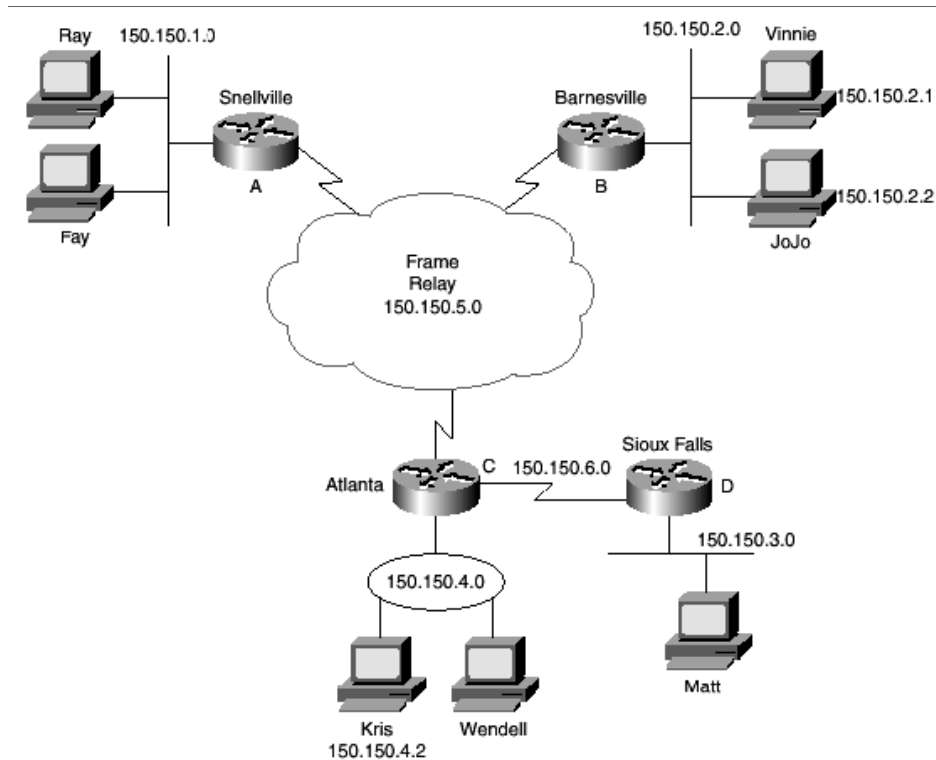
7. Chia mạng con (subnetting).

Giả sử ta phải tiến hành đặt địa chỉ IP cho hệ thống có cấu trúc như sau:



Hình 4.4 – Hệ thống mạng có 6 đường mạng

Theo hình trên, ta bắt buộc phải dùng đến tất cả là sáu đường mạng riêng biệt để đặt cho hệ thống mạng của mình, mặc dù trong mỗi mạng chỉ dùng đến vài địa chỉ trong tổng số 65534 địa chỉ hợp lệ, đó là một sự phí phạm to lớn. Thay vì vậy, khi sử dụng kỹ thuật chia mạng con, ta chỉ cần sử dụng một đường mạng 150.150.0.0 và chia đường mạng này thành sáu mạng con theo hình bên dưới:



Hình 4.5 – Hệ thống mạng có 6 đường mạng (sau khi chia Subnet)

Rõ ràng khi tiến hành cấp phát địa chỉ cho các hệ thống mạng lớn, người ta phải sử dụng kỹ thuật chia mạng con trong tình hình địa chỉ IP ngày càng khan hiếm. Ví dụ trong hình trên hoàn toàn chưa phải là chiến lược chia mạng con tối ưu. Thật sự người ta còn có thể chia mạng con nhỏ hơn nữa, đến một mức độ không bỏ phí một địa chỉ IP nào khác.

Xét về khía cạnh kỹ thuật, chia mạng con chính là việc mượn một số bit trong phần **host_id** ban đầu để đặt cho các mạng con. Lúc này, cấu trúc của địa chỉ IP gồm có ba phần: **network_id**, **subnet_id** và **host_id**. Số bit dùng cho phần **subnet_id** bao nhiêu là tùy thuộc vào chiến lược chia mạng con của người quản trị, có thể là một con số tròn byte (8 bit) hoặc một số bit lẻ vẫn được. Tuy nhiên **subnet_id** không thể chiếm trọn số bit có trong **host_id** ban đầu, cụ thể là (số bit làm **subnet_id**) \leq (số bit làm **host_id**)-2. Cụ thể đối với 3 lớp A, B, C như sau :

network_id	subnet_id	host_id
7 8	15 16	23 24 31
network_id	subnet_id	host_id
network_id	subnet_id	Host id
		26 27 31

Số lượng host trong mỗi mạng con được xác định bằng số bit trong phần **host_id**; $2^x - 2$ là số địa chỉ hợp lệ có thể đặt cho các host trong mạng con. Tương tự, số bit trong phần **subnet_id** xác định số lượng mạng con. Giả sử số bit là y $2^y - 2$ là số lượng mạng con có được (trường hợp đặc biệt thì có thể sử dụng được 2^y mạng con).

Một số khái niệm mới:

- **Địa chỉ mạng con (địa chỉ đường mạng)**: bao gồm cả phần **network_id** và **subnet_id**, phần **host_id** chỉ chứa các bit 0. Theo hình bên trên thì ta có các địa chỉ mạng con sau: 150.150.1.0, 150.150.2.0, ...

- **Địa chỉ broadcast trong một mạng con**: Giữ nguyên các bit dùng làm địa chỉ mạng con, đồng thời bật tất cả các bit trong phần **host_id** lên 1. Ví dụ địa chỉ **broadcast** của mạng con 150.150.1.0 là 150.150.1.255.

- **Mặt nạ mạng con (subnet mask)**: giúp máy tính xác định được địa chỉ mạng con của một địa chỉ host. Để xây dựng mặt nạ mạng con cho một hệ thống địa chỉ, ta bật các bit trong phần **network_id** và **subnet_id** lên 1, tắt các bit trong phần **host_id** thành 0. Ví dụ mặt nạ mạng con dùng cho hệ thống mạng trong hình trên là 255.255.255.0.

Vấn đề đặt ra là khi xác định được một địa chỉ IP (ví dụ 172.29.8.230) ta không thể biết được host này nằm trong mạng nào (không thể biết mạng này có chia mạng con hay không, và nếu có chia thì dùng bao nhiêu bit để chia). Chính vì vậy khi ghi nhận địa chỉ IP của một host, ta cũng phải cho biết **subnet mask** là bao nhiêu (**subnet mask** có thể là giá trị thập phân, cũng có thể là số bit dùng làm **subnet mask**).

+ Ví dụ địa chỉ IP ghi theo giá trị thập phân của **subnet mask** là 172.29.8.230/255.255.255.0

+ Hoặc địa chỉ IP ghi theo số bit dùng làm **subnet mask** là 172.29.8.230/24.

8. Địa chỉ riêng (private address) và cơ chế chuyển đổi địa chỉ mạng (Network Address Translation - NAT)

Tất cả các IP host khi kết nối vào mạng Internet đều phải có một địa chỉ IP do tổ chức IANA (**Internet Assigned Numbers Authority**) cấp phát – gọi là địa chỉ hợp lệ (hay là được đăng ký). Tuy nhiên số lượng host kết nối vào mạng ngày càng gia tăng dẫn đến tình trạng khan hiếm địa chỉ IP. Một giải pháp đưa ra là sử dụng cơ chế NAT kèm theo là RFC 1918 qui định danh sách địa chỉ riêng. Các địa chỉ này sẽ không được IANA cấp phát - hay còn gọi là địa chỉ không hợp lệ. Bảng sau liệt kê danh sách các địa chỉ này:

Nhóm địa chỉ	Lớp	Số lượng mạng
10.0.0.0 đến 10.255.255.255	A	1

172.16.0.0 đến 172.31.255.255	B	16
192.168.0.0 đến 192.168.255.255	C	256

9. Cơ chế NAT

NAT được sử dụng trong thực tế là tại một thời điểm, tất cả các host trong một mạng LAN thường không truy xuất vào Internet đồng thời, chính vì vậy ta không cần phải sử dụng một số lượng tương ứng địa chỉ IP hợp lệ. NAT cũng được sử dụng khi nhà cung cấp dịch vụ Internet (ISP) cung cấp số lượng địa chỉ IP hợp lệ ít hơn so với số máy cần truy cập Internet. NAT được sử dụng trên các router đóng vai trò là gateway cho một mạng. Các host bên trong mạng LAN sẽ sử dụng một lớp địa chỉ riêng thích hợp. Còn danh sách các địa chỉ IP hợp lệ sẽ được cấu hình trên **Router NAT**. Tất cả các packet của các host bên trong mạng LAN khi gửi đến một host trên Internet đều được router NAT phân tích và chuyển đổi các địa chỉ riêng có trong packet thành một địa chỉ hợp lệ trong danh sách rồi mới chuyển đến host đích nằm trên mạng Internet. Sau đó nếu có một packet gửi cho một host bên trong mạng LAN thì **Router NAT** cũng chuyển đổi địa chỉ đích thành địa chỉ riêng của host đó rồi mới chuyển cho host ở bên trong mạng LAN.

Một cơ chế mở rộng của NAT là **PAT (Port Address Translation)** cũng dùng cho mục đích tương ứng. Lúc này thay vì chỉ chuyển đổi địa chỉ IP thì cả địa chỉ cổng dịch vụ (port) cũng được chuyển đổi (do **Router NAT** quyết định).

IV. MỘT SỐ CÂU HỎI ĐẶT RA KHI LÀM VIỆC VỚI ĐỊA CHỈ IP.

1. Ví dụ 1.

Người ta ghi nhận được địa chỉ IP của một host như sau: 172.29.32.30/255.255.240.0, hãy trả lời các câu hỏi sau:

- Hãy cho biết mạng chứa host đó có chia mạng con hay không? Nếu có thì cho biết có bao nhiêu mạng con tương tự như vậy? Và có bao nhiêu host trong mỗi mạng con?

- Hãy cho biết host nằm trong mạng có địa chỉ là gì?

- Hãy cho biết địa chỉ broadcast dùng cho mạng đó?

- Liệt kê danh sách các địa chỉ host nằm chung mạng con với host trên.

Hướng dẫn trả lời:

Hãy cho biết mạng chứa host đó có chia mạng con hay không? Nếu có thì cho biết có bao nhiêu mạng con tương tự như vậy? Và có bao nhiêu host trong mỗi mạng con?

1. Xác định lớp địa chỉ xác định mặt nạ mặc định của lớp, so khớp với mặt nạ của địa chỉ kết luận có chia mạng con hay không?

2. Xác định số bit trong subnet_id = x số mạng con = $2^x - 2$.
3. Xác định số bit trong host_id = y số host trong mạng con = $2^y - 2$.
 - ☞ Như vậy, Host này có địa chỉ IP thuộc lớp B, trong khi subnet mask của Host lại là 255.255.240.0 (khác với subnet mask mặc định của lớp B) nên host trên nằm trong mạng có chia mạng con.

Subnet mask mặc định của lớp B	255.255.0.0	=	11111111 11111111 00000000 00000000
Subnet mask của Host	255.255.240.0	=	11111111 11111111 1111 0000 00000000

- ☞ So sánh số bit dùng làm subnet mask của Host với số bit dùng làm subnet mask mặc định của lớp B, sẽ có được số bit dùng làm subnet_id là 4 bit. Nên số bit dùng làm host_id sẽ là $(16-4) = 12$ bit.
- ☞ Số mạng con tương tự là 14.
- ☞ Số host trong mỗi mạng con là 4094.

Hãy cho biết host nằm trong mạng có địa chỉ là gì?

1. Duyệt mặt nạ mạng con và địa chỉ IP theo từng byte tương ứng, từ trái qua phải.
 - + Byte nào của subnet mask mang giá trị 255 thì ghi lại byte tương ứng của địa chỉ IP.
 - + Byte nào của subnet mask là 0 thì ghi lại byte tương ứng ở địa chỉ IP là 0.
 - + Nếu giá trị của byte nào ở subnet mask khác 255 và 0 thì để trống byte tương ứng ở địa chỉ IP và gọi byte này là **số khó chịu**
2. Tìm số cơ sở = 256 - số khó chịu.
3. Tìm bội số lớn nhất của số cơ sở nhưng bội số này phải bé hơn hoặc bằng số tương ứng trong địa chỉ IP và ghi lại số này.
 - ☞ 172.29.__.0. **Số khó chịu** = 240.
 - ☞ **Số cơ sở** = 256 - 240 = 16.
 - ☞ Bội số của 16 lớn nhất nhưng bé hơn hoặc bằng 32 là 32
 - ☞ địa chỉ đường mạng cần tìm là 172.29.32.0.

Hãy cho biết địa chỉ broadcast dùng cho mạng đó?

1. Duyệt mặt nạ mạng con và địa chỉ IP theo từng byte tương ứng, từ trái qua phải.
 - + Byte nào của subnet mask mang giá trị 255 thì ghi lại byte tương ứng của địa chỉ IP,
 - + Byte nào của subnet mask là 0 thì ghi vào byte tương ứng của địa chỉ IP là 255

+ Nếu byte của subnet mask có giá trị khác 255 và 0 thì để trống byte tương ứng ở địa chỉ IP và gọi byte này là **số khó chịu**.

2. Tìm số cơ sở = 256 - số khó chịu.

3. Tìm bội số nhỏ nhất của **số cơ sở** nhưng bội số này phải lớn hơn số tương ứng trong địa chỉ IP, đem số này trừ đi 1 thì được kết quả.

📄 172.29.__.255. **Số khó chịu** = 240.

📄 **Số cơ sở** = 256 - 240 = 16.

📄 Bội số nhỏ nhất của 16 nhưng lớn hơn 32 là 48. 48 - 1 = 47

📄 Địa chỉ broadcast cần tìm là 172.29.47.255.

Liệt kê danh sách các địa chỉ host nằm chung mạng con với host trên?

Các địa chỉ host hợp lệ có thể đặt cho các host nằm chung mạng con với host ở trên là: các địa chỉ sau địa chỉ mạng và trước địa chỉ broadcast.

Các địa chỉ từ 172.29.32.1 đến 172.29.47.254.

1. Ví dụ 2.

Cho host có địa chỉ 10.8.100.49/19. Hãy trả lời các câu hỏi trên cho host này.

- **Subnet mask** là 19 bit hay 255.255.224.0 có chia mạng con. Số bit trong subnet_id là 11 số subnet = $2^{11}-2 = 2046$. Số bit trong host_id là 13 số host hợp lệ = $2^{13}-2 = 8190$.

- Địa chỉ mạng: 10.8.__.0. **Số khó chịu** = 224 **Số cơ sở** = 256 - 224 = 32.

Bội số lớn nhất của 32 nhưng bé hơn 100 là 96 địa chỉ mạng là 10.8.96.0.

- Địa chỉ broadcast: 10.8.127.255.

- Các địa chỉ hợp lệ của mạng con: 10.8.96.1 đến 10.8.127.254

CHƯƠNG 5

PHƯƠNG TIỆN TRUYỀN DẪN VÀ CÁC THIẾT BỊ MẠNG

I. GIỚI THIỆU VỀ MÔI TRƯỜNG TRUYỀN DẪN

1. Khái niệm

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

- Hữu tuyến (**bounded media**)
- Vô tuyến (**boundless media**)

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

2. Các đặc tính của phương tiện truyền dẫn

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

- Chi phí
- Yêu cầu cài đặt
- Độ bảo mật

- Băng thông (**bandwidth**): được xác định bằng tổng lượng thông tin có thể truyền dẫn trên đường truyền tại một thời điểm. Băng thông là một số xác định, bị giới hạn bởi phương tiện truyền dẫn, kỹ thuật truyền dẫn và thiết bị mạng được

sử dụng. Băng thông là một trong những thông số dùng để phân tích độ hiệu quả của đường mạng. Đơn vị của băng thông:

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

+ Kbps (**Kilobits per second**): $1 \text{ Kbps} = 10^3 \text{ bps} = 1000 \text{ Bps}$

+ Mbps (**Megabits per second**): $1 \text{ Mbps} = 10^3 \text{ Kbps}$

+ Gbps (**Gigabits per second**): $1 \text{ Gbps} = 10^3 \text{ Mbps}$

+ Tbps (**Terabits per second**): $1 \text{ Tbps} = 10^3 \text{ Gbps}$.

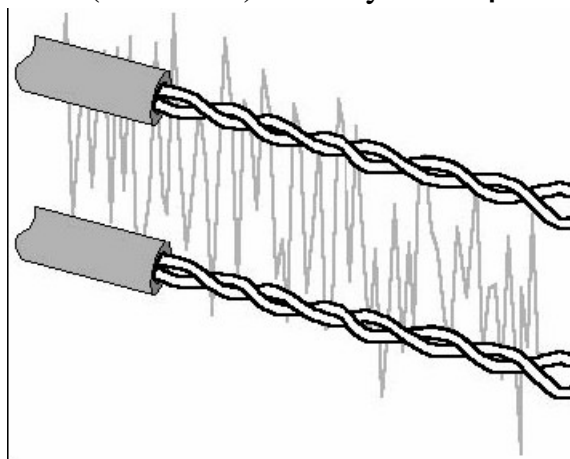
- Thông lượng (**Throughput**): lượng thông tin thực sự được truyền dẫn trên thiết bị tại một thời điểm.

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

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

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

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



Hình 5.1 – Mô phỏng trường hợp nhiễu xuyên kênh (**crosstalk**)

3. Các kiểu truyền dẫn.

Có các kiểu truyền dẫn như sau:

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

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

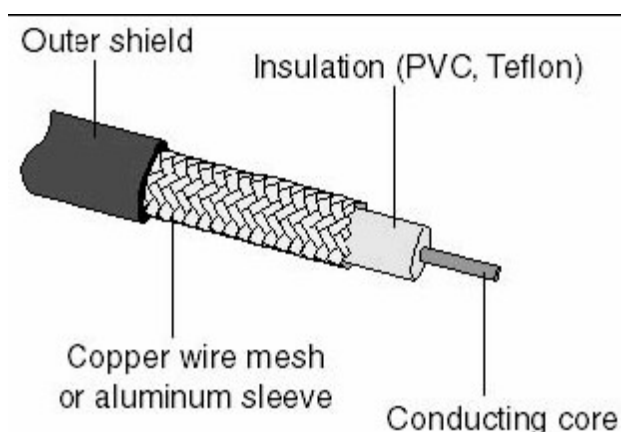
+ Song công (**Full-Duplex**): trong kiểu truyền dẫn này, tại một thời điểm, thiết bị có thể vừa phát vừa thu. Điện thoại là một minh họa cho kiểu truyền dẫn này.

II. CÁC LOẠI CÁP.

1. Cáp đồng trục (coaxial).

Là kiểu cáp đầu tiên được dùng trong các LAN, cấu tạo của cáp đồng trục gồm:

- Dây dẫn trung tâm: dây đồng hoặc dây đồng bện.
- Một lớp cách điện giữa dây dẫn phía ngoài và dây dẫn phía trong.
- Dây dẫn ngoài: bao quanh dây dẫn trung tâm dưới dạng dây đồng bện hoặc lá. Dây này có tác dụng bảo vệ dây dẫn trung tâm khỏi nhiễu điện từ và được nối đất để thoát nhiễu.
- Ngoài cùng là một lớp vỏ **plastic** bảo vệ cáp.



Hình 5.2 – Chi tiết cáp đồng trục

Ưu điểm của cáp đồng trục: là rẻ tiền, nhẹ, mềm và dễ kéo dây.

Cáp mỏng (**thin cable/thinnet**): có đường kính khoảng 6mm, thuộc họ RG-58, chiều dài đường chạy tối đa là 185 m.

- Cáp RC-58, trở kháng 50 ohm dùng với Ethernet mỏng.
- Cáp RC-59, trở kháng 75 ohm dùng cho truyền hình cáp.
- Cáp RC-62, trở kháng 93 ohm dùng cho ARCnet.

Cáp dày (**thick cable/thicknet**): có đường kính khoảng 13mm thuộc họ RG-58, chiều dài đường chạy tối đa 500m.

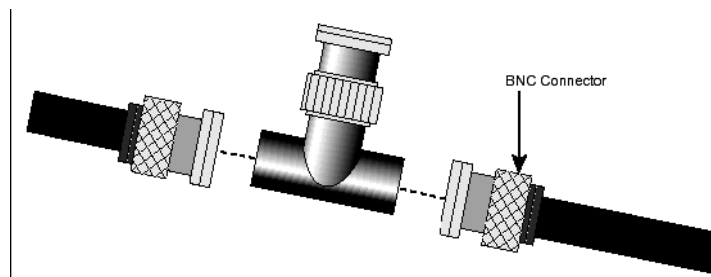


Hình 5.3 – So sánh cáp đồng trục: **Thicknet** và **Thinnet**.

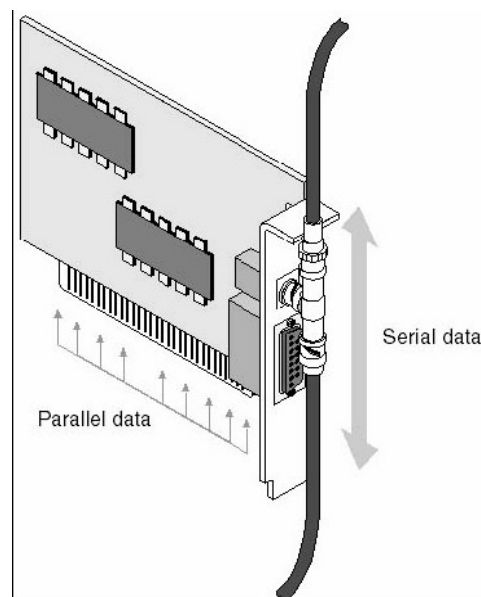
So sánh giữa cáp đồng trục mỏng và đồng trục dày:

- Chi phí: cáp đồng trục thinnet rẻ nhất, cáp đồng trục **thicknet** đắt hơn.
- Tốc độ: mạng Ethernet sử dụng cáp thinnet có tốc độ tối đa 10Mbps và mạng ARCNet có tốc độ tối đa 2.5Mbps.
- **EMI**: có lớp chống nhiễu nên hạn chế được nhiễu.
- Có thể bị nghe trộm tín hiệu trên đường truyền.

Cách lắp đặt dây: muốn nối các đoạn cáp đồng trục mỏng lại với nhau ta dùng đầu nối chữ T và đầu **BNC** như hình vẽ.

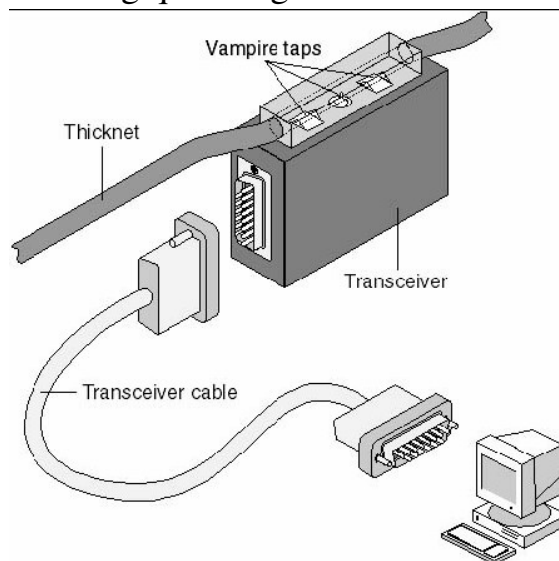


Hình 5.4 – Đầu nối BNC và đầu nối chữ T



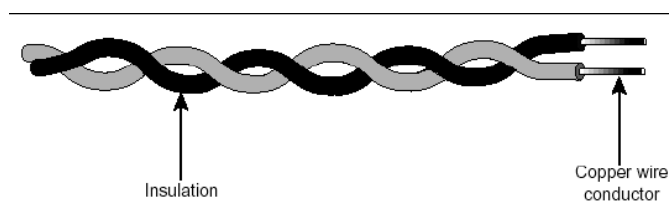
Hình 5.5 – Đầu chuyển đổi (gắn vào máy tính)

Muốn đấu nối cáp đồng trục dày ta phải dùng một đầu chuyển đổi **transceiver** và nối kết vào máy tính thông qua cổng **AUI**.



Hình 5.6 – Kết nối cáp **Thicknet** vào máy tính.

2. Cáp xoắn đôi.



Hình 5.7 – Mô tả cáp xoắn đôi

Cáp xoắn đôi gồm nhiều cặp dây đồng xoắn lại với nhau nhằm chống phát xạ nhiễu điện từ. Do giá thành thấp nên cáp xoắn được dùng rất rộng rãi. Có hai loại cáp xoắn đôi được sử dụng rộng rãi trong LAN là: loại có vỏ bọc chống nhiễu và loại không có vỏ bọc chống nhiễu.

Cáp xoắn đôi có vỏ bọc chống nhiễu STP (Shielded Twisted- Pair).

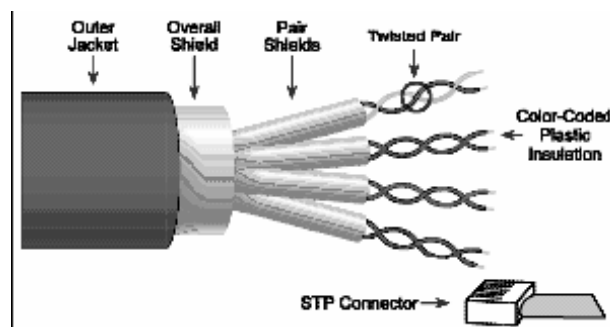
- Gồm nhiều cặp xoắn được phủ bên ngoài một lớp vỏ làm bằng dây đồng bện. Lớp vỏ này có tác dụng chống **EMI** từ ngoài và chống phát xạ nhiễu bên trong. Lớp vỏ bọc chống nhiễu này được nối đất để thoát nhiễu. Cáp xoắn đôi có bọc ít bị tác động bởi nhiễu điện và truyền tín hiệu xa hơn cáp xoắn đôi trần.

- Chi phí: đắt tiền hơn **Thinnet** và **UTP** nhưng lại rẻ tiền hơn **Thicknet** và cáp quang.

- Tốc độ: tốc độ lý thuyết 500Mbps, thực tế khoảng 155Mbps, với đường chạy 100m; tốc độ phổ biến 16Mbps (Token Ring).

- Độ suy dần: tín hiệu yếu dần nếu cáp càng dài, thông thường chiều dài cáp nên ngắn hơn 100m.

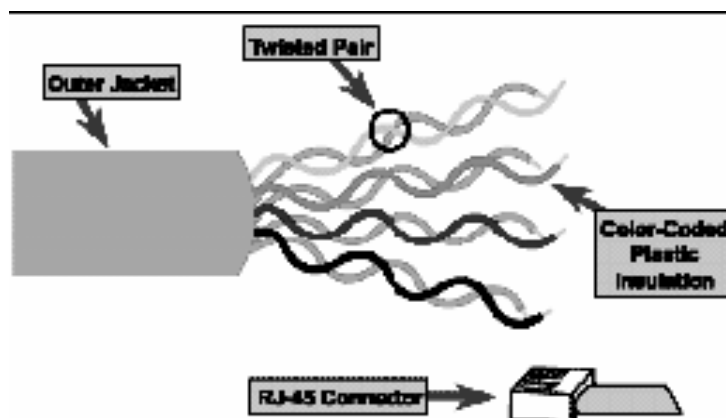
- Đầu nối: STP sử dụng đầu nối DIN (DB -9).



Hình 5.8 – Mô tả cáp STP.

Cáp xoắn đôi không có vỏ bọc chống nhiễu UTP (Unshielded Twisted- Pair).

Gồm nhiều cặp xoắn như cáp STP nhưng không có lớp vỏ đồng chống nhiễu. Cáp xoắn đôi trần sử dụng chuẩn 10BaseT hoặc 100BaseT. Do giá thành rẻ nên đã nhanh chóng trở thành loại cáp mạng cục bộ được ưu chuộng nhất. Độ dài tối đa của một đoạn cáp là 100 mét. Do không có vỏ bọc chống nhiễu nên cáp UTP dễ bị nhiễu khi đặt gần các thiết bị và cáp khác do đó thông thường dùng để đi dây trong nhà. Đầu nối dùng đầu RJ-45.



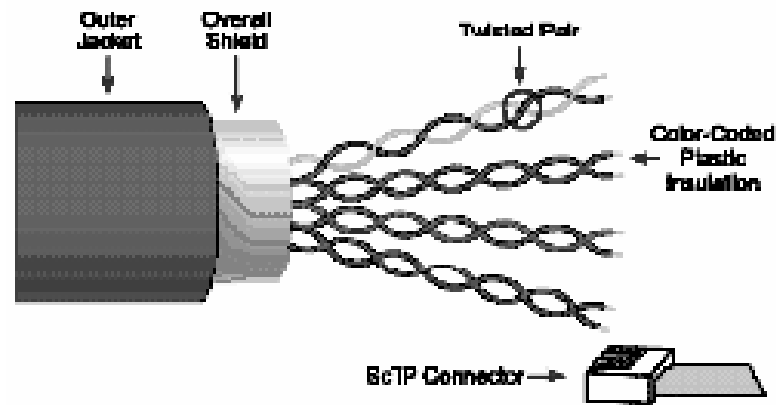
Hình 5.9 – Mô tả cáp UTP

Cáp UTP có năm loại:

- Loại 1: truyền âm thanh, tốc độ < 4Mbps.
- Loại 2: cáp này gồm bốn dây xoắn đôi, tốc độ 4Mbps.
- Loại 3: truyền dữ liệu với tốc độ lên đến 10 Mbps. Cáp này gồm bốn dây xoắn đôi với ba mắt xoắn trên mỗi foot (foot là đơn vị đo chiều dài, 1 foot = 0.3048 mét).
- Loại 4: truyền dữ liệu, bốn cặp xoắn đôi, tốc độ đạt được 16 Mbps.
- Loại 5: truyền dữ liệu, bốn cặp xoắn đôi, tốc độ 100Mbps.

Cáp xoắn có vỏ bọc ScTP-FTP (Screened Twisted-pair).

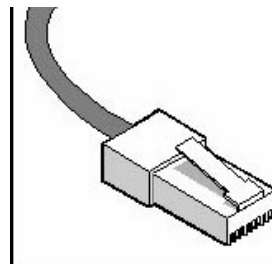
FTP là loại cáp lai tạo giữa cáp UTP và STP, nó hỗ trợ chiều dài tối đa 100m.



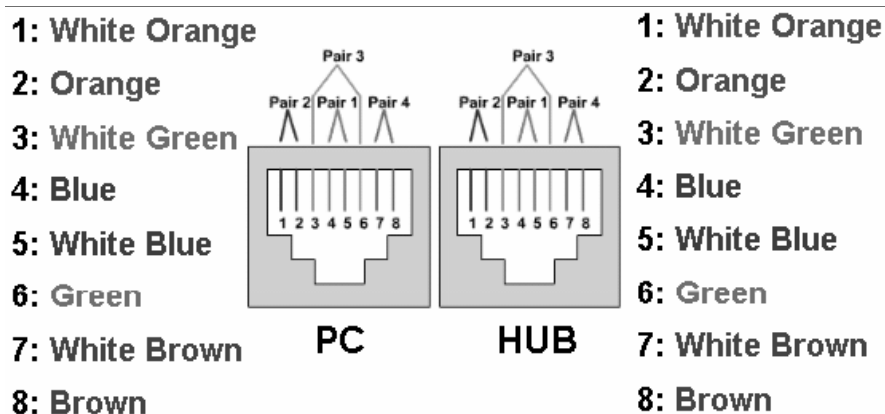
Hình 5.10 – Mô tả cáp FTP

Các kỹ thuật bấm cáp mạng.

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

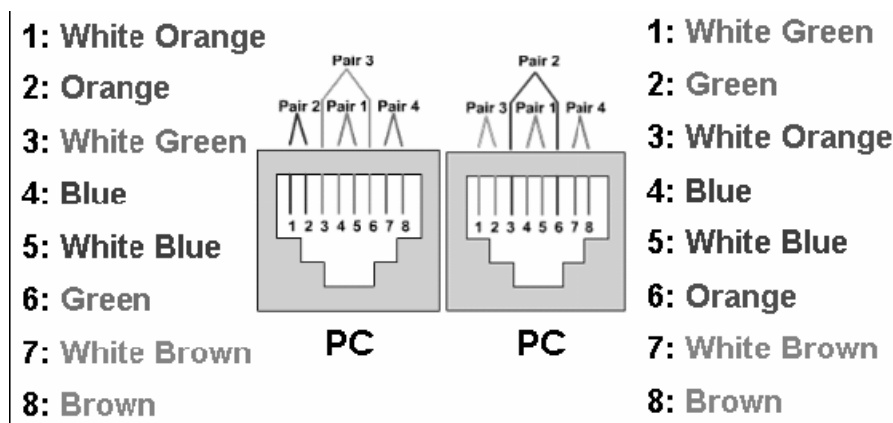


Hình 5.11 – Đầu RJ45.



Hình 5.12 – Cách đấu dây thẳng.

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

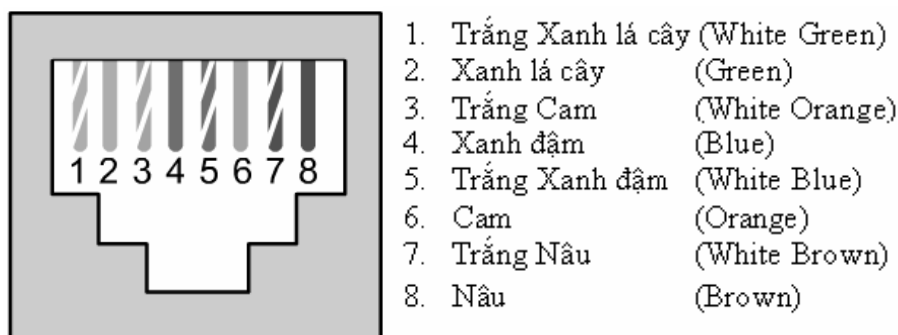


Hình 5.13 – Cách đấu dây chéo.

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

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

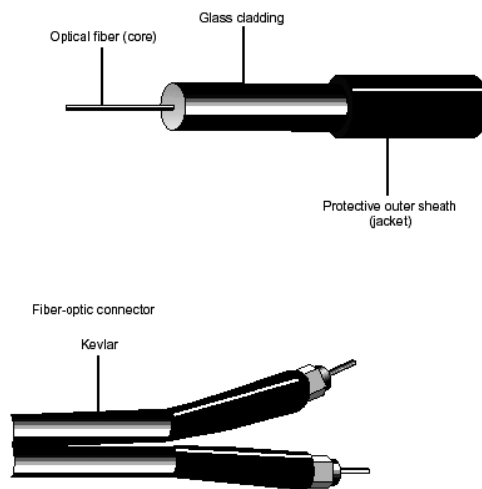
- Chuẩn T568-A (còn gọi là Chuẩn A):



- Chuẩn T568-B (còn gọi là Chuẩn B):



3. Cáp quang (Fiber-optic cable).

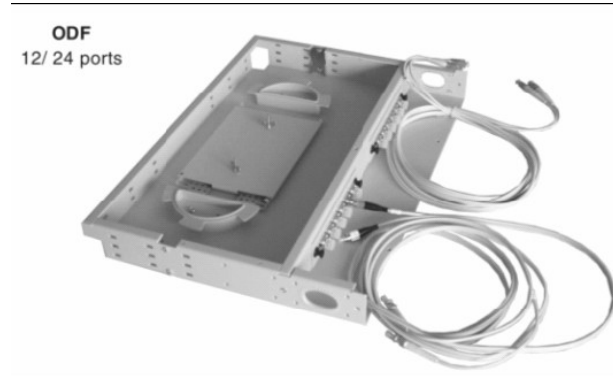


Hình 5.14 – Mô tả cáp quang.

Cáp quang có cấu tạo gồm dây dẫn trung tâm là sợi thủy tinh hoặc plastic đã được tinh chế nhằm cho phép truyền đi tối đa các tín hiệu ánh sáng. Sợi quang được tráng một lớp nhằm phản chiếu các tín hiệu. Cáp quang chỉ truyền sóng ánh sáng (không truyền tín hiệu điện) với băng thông rất cao nên không gặp các sự cố về nhiễu hay bị nghe trộm. Cáp dùng nguồn sáng laser, diode phát xạ ánh sáng. Cáp rất bền và độ suy giảm tín hiệu rất thấp nên đoạn cáp có thể dài đến vài km. Băng thông cho phép đến 2Gbps. Nhưng cáp quang có khuyết điểm là giá thành cao và khó lắp đặt. Các loại cáp quang:

- Loại lõi 8.3 micron, lớp lót 125 micron, chế độ đơn.
- Loại lõi 62.5 micron, lớp lót 125 micron, đa chế độ.
- Loại lõi 50 micron, lớp lót 125 micron, đa chế độ.
- Loại lõi 100 micron, lớp lót 140 micron, đa chế độ.

Hộp đấu nối cáp quang: do cáp quang không thể bẻ cong nên khi nối cáp quang vào các thiết bị khác chúng ta phải thông qua hộp đấu nối.



Hình 5.15 – Mô tả hộp đấu nối cáp quang.

Đầu nối cáp quang: đầu nối cáp quang rất đa dạng thông thường trên thị trường có các đầu nối như sau: **FT, ST, FC...**



Hình 5.16 – Một số loại đầu nối cáp quang.

III. ĐƯỜNG TRUYỀN VÔ TUYẾN.

1. Giới thiệu

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

- Cung cấp nối kết tạm thời với mạng cáp có sẵn.
- Những người liên tục di chuyển vẫn nối kết vào mạng dùng cáp.
- Lắp đặt đường truyền vô tuyến ở những nơi địa hình phức tạp không thể đi dây được.
- Phù hợp cho những nơi phục vụ nhiều kết nối cùng một lúc cho nhiều khách hàng. Ví dụ như: dùng đường vô tuyến cho phép khách hàng ở sân bay kết vào mạng để duyệt Internet.

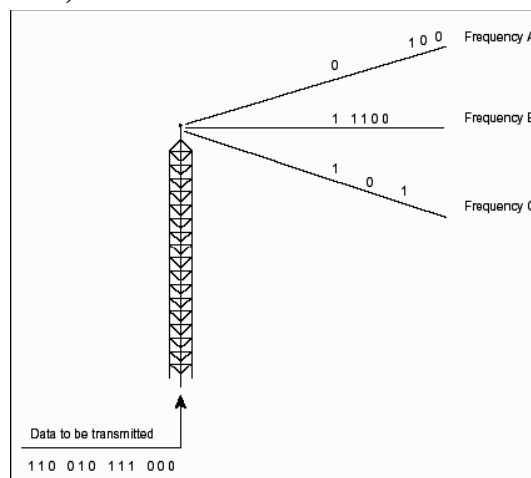
- Dùng cho những mạng có giới hạn rộng lớn vượt quá khả năng cho phép của cáp đồng và cáp quang.

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

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

- Tín hiệu không an toàn.
- Dễ bị nghe lén.
- Khi có vật cản thì tín hiệu suy yếu rất nhanh.
- Băng thông không cao.

2. Sóng vô tuyến (radio).

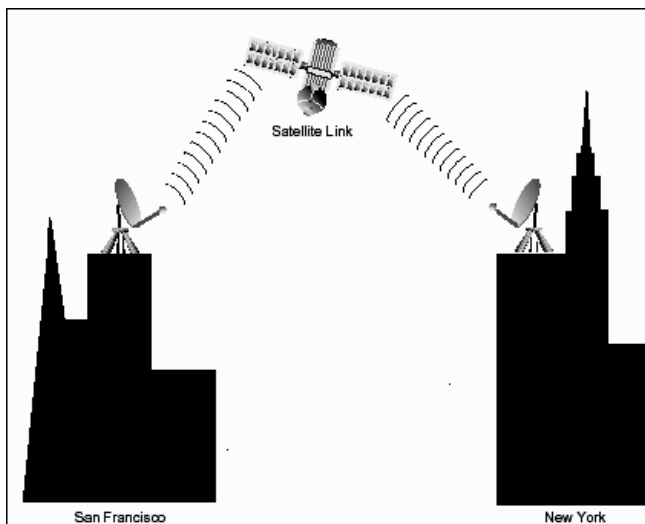


Hình 5.17 – Truyền dữ liệu qua sóng vô tuyến.

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

3. Sóng viba.

Truyền thông viba thường có hai dạng: truyền thông trên mặt đất và các nối kết với vệ tinh. Miền tần số của viba mặt đất khoảng 21-23 GHz, các kết nối vệ tinh khoảng 11-14 Mhz. Băng thông từ 1-10 MBps. Sự suy yếu tín hiệu tùy thuộc vào điều kiện thời tiết, công suất và tần số phát. Chúng dễ bị nghe trộm nên thường được mã hóa.



Hình 5.18 – Truyền dữ liệu thông qua vệ tinh.



Hình 5.19 – Truyền dữ liệu trực tiếp giữa hai thiết bị.

IV. CÁC THIẾT BỊ MẠNG.

1. Card mạng (NIC hay Adapter).

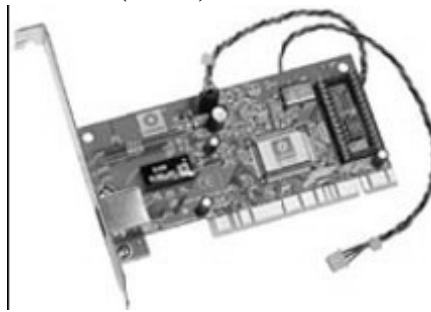
Card mạng là thiết bị nối kết giữa máy tính và cáp mạng. Chúng thường giao tiếp với máy tính qua các khe cắm như: **ISA**, **PCI** hay **USB**... Phần giao tiếp với cáp mạng thông thường theo các chuẩn như: **AUI**, **BNC**, **UTP**... Các chức năng chính của card mạng:

- Chuẩn bị dữ liệu đưa lên mạng: trước khi đưa lên mạng, dữ liệu phải được chuyển từ dạng byte, bit sang tín hiệu điện để có thể truyền trên cáp.

- Gửi dữ liệu đến máy tính khác.
- Kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp.

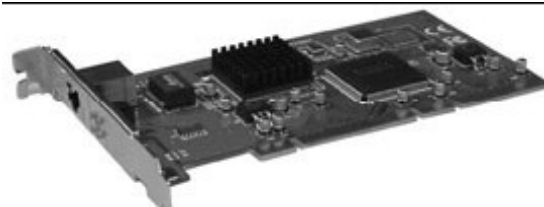
Địa chỉ **MAC (Media Access Control)**: mỗi card mạng có một địa chỉ riêng dùng để phân biệt card mạng này với card mạng khác trên mạng. Địa chỉ này do **IEEE – Viện Công nghệ Điện và Điện tử** – cấp cho các nhà sản xuất card mạng. Từ đó các nhà sản xuất gán cố định địa chỉ này vào chip của mỗi card mạng. Địa chỉ này gồm 6 byte (48 bit), có dạng **XXXXXX.XXXXXX**, 3 byte đầu là mã số của nhà sản xuất, 3 byte sau là số serial của các card mạng do hãng đó sản xuất. Địa chỉ này được ghi cố định vào **ROM** nên còn gọi là địa chỉ vật lý. Ví dụ địa chỉ vật lý của một card Intel có dạng như sau: 00A0C90C4B3F.

Hình dưới là card mạng RE100TX theo chuẩn Ethernet IEEE 802.3 và IEEE 802.3u. Nó hỗ trợ cả hai băng thông 10Mbps và 100Mbps theo chuẩn 10Base-T và 100Base-TX. Ngoài ra card này còn cung cấp các tính năng như **Wake On LAN, Port Trunking**, hỗ trợ cơ chế truyền **full duplex**. Card này cũng hỗ trợ hai cơ chế boot ROM 16 bit (RPL) và 32 bit (PXE).



Hình 5.20 – Card RE100TX.

Hình dưới là card FL1000T 10/100/1000Mbps Gigabit Adapter, nó là card mạng theo chuẩn **Gigabit** dùng đầu nối RJ45 truyền trên môi trường cáp UTP cat 5. Card này cung cấp đường truyền với băng thông lớn và tương thích với card PCI 64 và 32 bit đồng thời nó cũng hỗ trợ cả hai cơ chế truyền **full/half duplex** trên cả ba loại băng thông 10/100/1000 Mbps.



Hình 5.21 – Card FL1000T 10/100/1000Mbps **Gigabit**.

Hình dưới là card mạng không dây WL11A 11Mbps **Wireless PCMCIA LAN Card**, card này giao tiếp với máy theo chuẩn **PCMCIA** nên khi sử dụng cho PC chúng ta phải dùng thêm card chuyển đổi từ PCI sang **PCMCIA**. Card được thiết kế theo chuẩn IEEE802.11b ở dải tần 2.4GHz ISM, dùng cơ chế **CSMA/CA** để xử lý đụng độ, băng thông của card là 11Mbps, có thể mã hóa 64 và 128 bit.

Đặc biệt card này hỗ trợ cả hai kiến trúc kết nối mạng là **Infrastructure** và **AdHoc**.

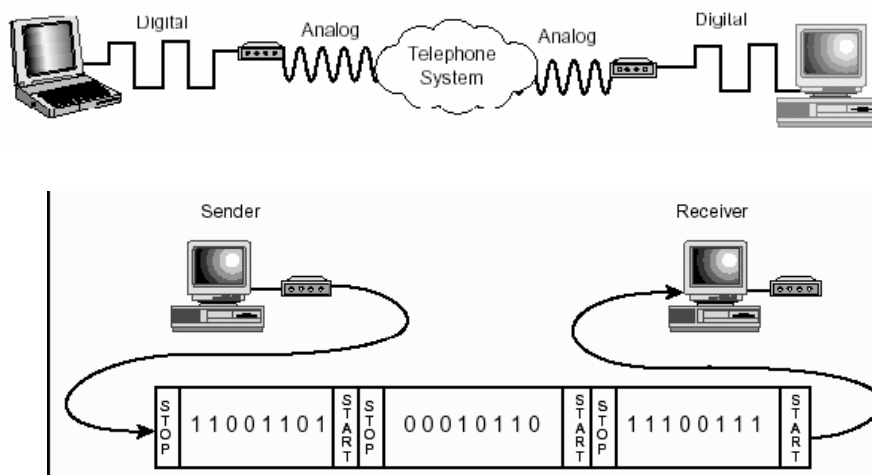


Hình 5.22 – Card WL11A.

2. Modem.

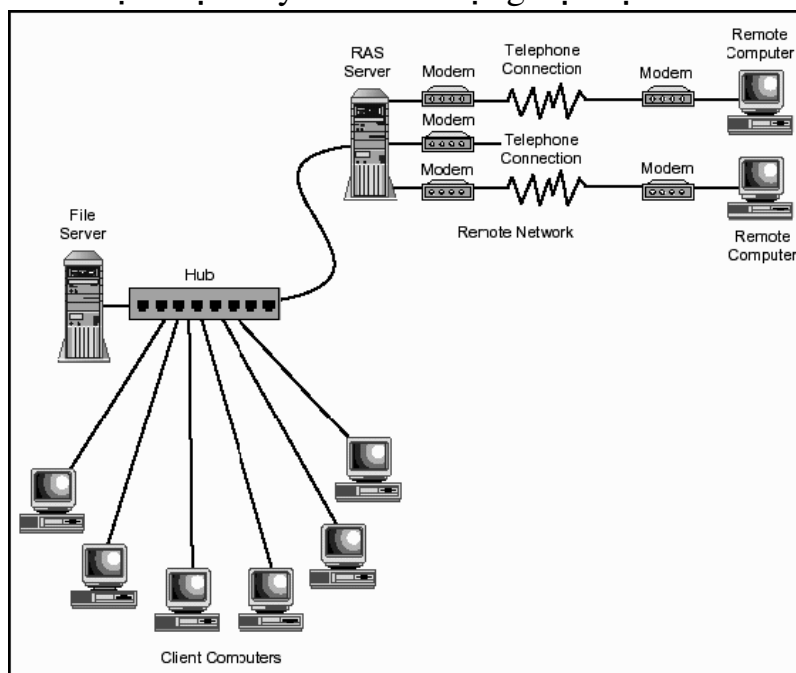
Là thiết bị dùng để nối hai máy tính hay hai thiết bị ở xa thông qua mạng điện thoại. **Modem** thường có hai loại: **internal** (là loại được gắn bên trong máy tính giao tiếp qua khe cắm ISA hoặc PCI), **external** (là loại thiết bị đặt bên ngoài CPU và giao tiếp với CPU thông qua cổng COM theo chuẩn RS-232). Cả hai loại trên đều có cổng giao tiếp RJ11 để nối với dây điện thoại.

Chức năng của **Modem** là chuyển đổi tín hiệu số (**digital**) thành tín hiệu tương tự (**analog**) để truyền dữ liệu trên dây điện thoại. Tại đầu nhận, **Modem** chuyển dữ liệu ngược lại từ dạng tín hiệu tương tự sang tín hiệu số để truyền vào máy tính. Thiết bị này giá tương đối thấp nhưng mang lại hiệu quả rất lớn. Nó giúp nối các mạng LAN ở xa với nhau thành các mạng WAN, giúp người dùng có thể hòa vào mạng nội bộ của công ty một cách dễ dàng dù người đó ở nơi nào.



Hình 5.24 – Mô hình truyền dữ liệu thông qua **Modem**.

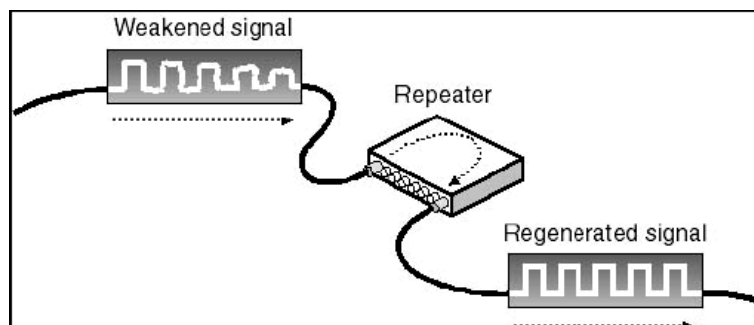
Remote Access Services (RAS): là một dịch vụ mềm trên một máy tính hoặc là một dịch vụ trên thiết bị phần cứng. Nó cho phép dùng **Modem** để nối kết hai mạng **LAN** với nhau hoặc một máy tính vào mạng nội bộ.



Hình 5.25 – Sử dụng **RAS** để liên lạc.

3. Repeater.

Là thiết bị dùng để khuếch đại tín hiệu trên các đoạn cáp dài. Khi truyền dữ liệu trên các đoạn cáp dài tín hiệu điện sẽ yếu đi, nếu chúng ta muốn mở rộng kích thước mạng thì chúng ta dùng thiết bị này để khuếch đại tín hiệu và truyền đi tiếp. Nhưng chúng ta chú ý rằng thiết bị này hoạt động ở lớp vật lý trong mô hình **OSI**, nó chỉ hiểu tín hiệu điện nên không lọc được dữ liệu ở bất kỳ dạng nào, và mỗi lần khuếch đại các tín hiệu điện yếu sẽ bị sai do đó nếu cứ tiếp tục dùng nhiều **Repeater** để khuếch đại và mở rộng kích thước mạng thì dữ liệu sẽ ngày càng sai lệch.



Hình 5.26 – Thiết bị **Repeater**.

4. Hub.

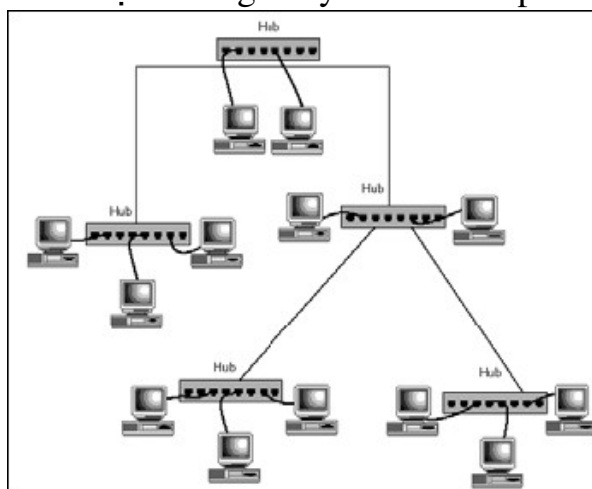
Là thiết bị giống như **Repeater** nhưng nhiều port hơn cho phép nhiều máy tính nối tập trung về thiết bị này. Các chức năng giống như **Repeater** dùng để khuếch đại tín hiệu điện và truyền đến tất cả các port còn lại đồng thời không lọc được dữ liệu. Thông thường **Hub** hoạt động ở lớp 1 (lớp vật lý). Toàn bộ **Hub** (hoặc **Repeater**) được xem là một **Collision Domain**.

Hub gồm có ba loại:

- **Passive Hub**: là thiết bị đầu nối cáp dùng để chuyển tiếp tín hiệu từ đoạn cáp này đến các đoạn cáp khác, không có linh kiện điện tử và nguồn riêng nên không khuếch đại và xử lý tín hiệu;

- **Active Hub**: là thiết bị đầu nối cáp dùng để chuyển tiếp tín hiệu từ đoạn cáp này đến các đoạn cáp khác với chất lượng cao hơn. Thiết bị này có linh kiện điện tử và nguồn điện riêng nên hoạt động như một repeater có nhiều cổng (**port**);

- **Intelligent Hub**: là một **active hub** có thêm các chức năng vượt trội như cho phép quản lý từ các máy tính, chuyển mạch (**switching**), cho phép tín hiệu điện chuyển đến đúng port cần nhận không chuyển đến các port không liên quan.



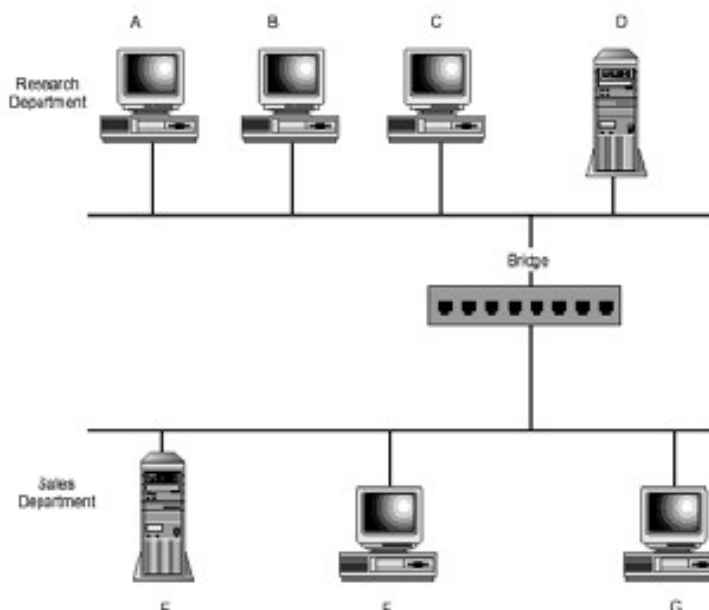
Hình 5.27 – Mô hình mạng sử dụng **Hub**.

5. Bridge (cầu nối).

Là thiết bị cho phép nối kết hai nhánh mạng, có chức năng chuyển có chọn lọc các gói tin đến nhánh mạng chứa máy nhận gói tin. Trong **Bridge** có bảng địa chỉ **MAC**, bảng địa chỉ này sẽ được dùng để quyết định đường đi của gói tin (cách thức truyền đi của một gói tin sẽ được nói rõ hơn ở trong phần trình bày về thiết bị **Switch**). Bảng địa chỉ này có thể được khởi tạo tự động hoặc phải cấu hình bằng tay. **Bridge** hoạt động ở lớp hai (lớp **Data link**) trong mô hình **OSI**.

Ưu điểm của **Bridge** là: cho phép mở rộng cùng một mạng logic với nhiều kiểu cáp khác nhau. Chia mạng thành nhiều phân đoạn khác nhau nhằm giảm lưu lượng trên mạng.

Khuyết điểm: chậm hơn **Repeater** vì phải xử lý các gói tin, chưa tìm được đường đi tối ưu trong trường hợp có nhiều đường đi. Việc xử lý gói tin dựa trên phần mềm.



Hình 5.28 – Mô hình mạng sử dụng **Bridge**.

6. Switch

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

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

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

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

- + Nếu địa chỉ đích đã có trong bảng **MAC**:

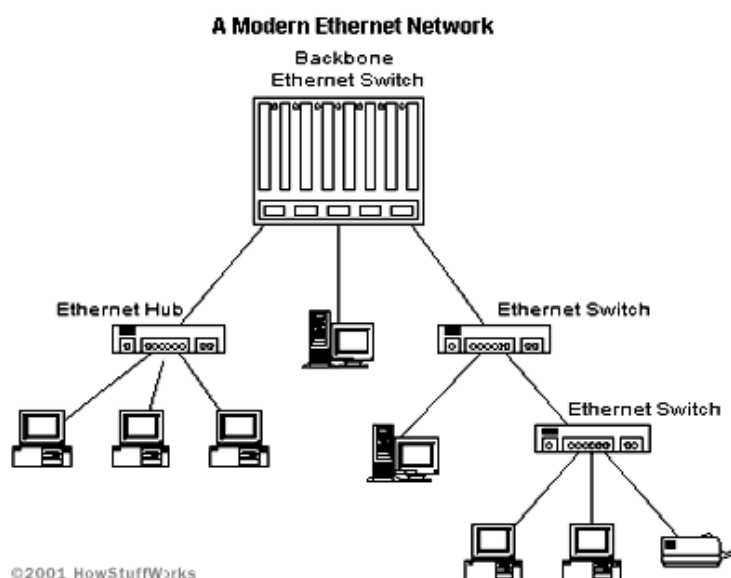
- Nếu port đích trùng với port nguồn thì **Switch** (hoặc **Bridge**) sẽ loại bỏ gói tin.

Nếu port đích khác với **port** nguồn thì gói tin sẽ được gửi ra **port** đích tương ứng.

Chú ý:

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

Do cách hoạt động của **Switch** (hoặc **Bridge**) như vậy, nên mỗi **Port** của **Switch** là một **Collision Domain**, và toàn bộ **Switch** được xem là một **Broadcast Domain** (khái niệm **Collision Domain** và **Broadcast Domain** sẽ được giới thiệu trong chương 5, phần “các công nghệ mạng LAN”).



Hình 5.29 – Mô hình mạng sử dụng **Switch**.

Ngoài các tính năng cơ sở, **Switch** còn các tính năng mở rộng như sau:

- Phương pháp chuyển gói tin (**Switching mode**): trong thiết bị của **Cisco** có thể sử dụng một trong ba loại sau:

+ **Store and Forward**: là tính năng lưu dữ liệu trong bộ đệm trước khi truyền sang các port khác để tránh đụng độ (**collision**), thông thường tốc độ truyền khoảng 148.800 pps. Với kỹ thuật này toàn bộ gói tin phải được nhận đủ trước khi **Switch** truyền frame này đi do đó độ trễ (**latency**) lệ thuộc vào chiều dài của frame.

+ **Cut Through**: **Switch** sẽ truyền gói tin ngay lập tức một khi nó biết được địa chỉ đích của gói tin. Kỹ thuật này sẽ có độ trễ thấp hơn so với kỹ thuật **Store and Forward** và độ trễ luôn là con số xác định, bất chấp chiều dài của gói tin.

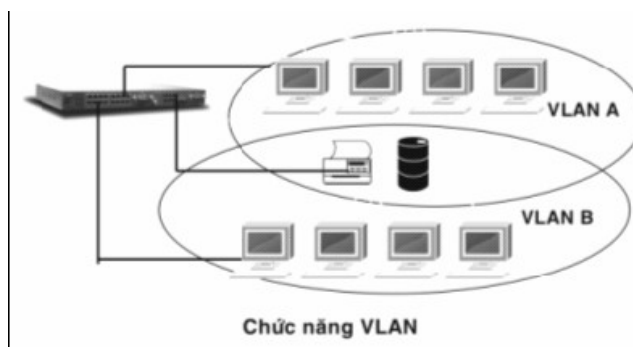
+ **Fragment Free**: thì **Switch** đọc 64 byte đầu tiên và sau đó bắt đầu truyền dữ liệu.

- **Trunking (MAC Base)**: ở một số thiết bị **Switch**, tính năng **Trunking** được hiểu là tính năng giúp tăng tốc độ truyền giữa hai **Switch**, nhưng chú ý là hai **Switch** phải cùng loại. Riêng trong thiết bị **Switch** của **Cisco**, **Trunking** được hiểu là đường truyền dùng để mang thông tin cho các **VLAN**.



Hình 5.30 – Mô tả cách dùng đường **Trunking**.

- **VLAN**: tạo các mạng ảo, nhằm đảm bảo tính bảo mật khi mở rộng mạng bằng cách nối các **Switch** với nhau. Mỗi **VLAN** có thể được xem là một **Broadcast Domain**, nên khi chia các mạng ảo giúp ta sẽ phân vùng miền **broadcast** nhằm cải tiến tốc độ và hiệu quả của hệ thống. Nói cách khác, **VLAN** là một nhóm logic các thiết bị hoặc người sử dụng. Nhóm logic này được chia dựa vào chức năng, ứng dụng, ... mà không phụ thuộc vào vị trí địa lý. Chỉ có các thiết bị trong cùng **VLAN** mới liên lạc được với nhau. Nếu muốn các **VLAN** có thể liên lạc được với nhau thì phải sử dụng **Router** để liên kết các **VLAN** lại.



Hình 5.31 – Mô tả cách sử dụng **VLAN**.

- **Spanning Tree**: tạo đường dự phòng, bình thường dữ liệu được truyền trên một cổng mạng số thứ tự thấp. Khi mất liên lạc thiết bị tự chuyển sang cổng khác, nhằm đảm bảo mạng hoạt động liên tục. **Spanning Tree** thực chất là hạn chế các đường dư thừa trên mạng.

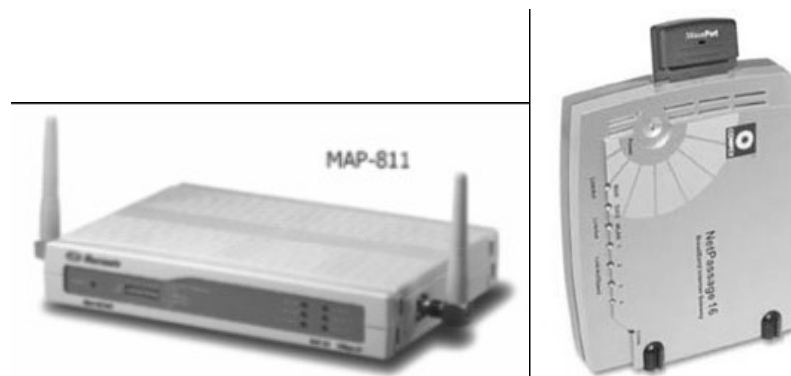
Hình dưới là **Switch Complex SRX2216** được thiết kế theo chuẩn IEEE 802.3, IEEE802.3u, **Switch** này thường dùng trong các giải pháp mạng vừa và nhỏ. Thiết bị này hỗ trợ 16 port RJ45 tốc độ 10/100Mbps, 12K **MAC Address**, 2K bộ đệm (**buffer**). Ngoài ra thiết bị này còn có những tính năng như: **Store and**

Forward, Spanning Tree, Port Trunking, Virtual LAN giúp chúng ta mở rộng mạng mà không sợ xảy ra đụng độ (**collision**).



Hình 5.31 - Switch Complex SRX2216.

7. Wireless Access Point.



Hình 5.32 – Thiết bị Wireless

Wireless Access Point là thiết bị kết nối mạng không dây được thiết kế theo chuẩn IEEE802.11b, cho phép nối **LAN to LAN**, dùng cơ chế **CSMA/CA** để giải quyết tranh chấp, dùng cả hai kiến trúc kết nối mạng là **Infrastructure** và **AdHoc**, mã hóa theo 64/128 Bit. Nó còn hỗ trợ tốc độ truyền không dây lên 11Mbps trên băng tần 2,4GHz ISM dùng công nghệ **radio DSSS (Direct Sequence Spread Spectrum)**



Hình 5.33 – Mạng sử dụng Wireless.

8. Router.

Là thiết bị dùng nối kết các mạng **logic** với nhau, kiểm soát và lọc các gói tin nên hạn chế được lưu lượng trên các mạng **logic** (thông qua cơ chế **Access-list**). Các **Router** dùng bảng định tuyến (**Routing table**) để lưu trữ thông tin về mạng dùng trong trường hợp tìm đường đi tối ưu cho các gói tin. Bảng định tuyến chứa các thông tin về đường đi, thông tin về ước lượng thời gian, khoảng cách...

Bảng này có thể cấu hình tĩnh hay tự động. **Router** hiểu được địa chỉ **logic IP** nên thông thường **Router** hoạt động ở lớp mạng (**network**) hoặc cao hơn. Người ta cũng có thể thực hiện **firewall** ở mức độ đơn giản trên **Router** thông qua tính năng **Accesslist** (tạo một danh sách truy cập hợp lệ), thực hiện việc ánh xạ địa chỉ thông qua tính năng **NAT** (chuyển đổi địa chỉ).

Khi một gói tin đến **Router**, **Router** sẽ thực hiện các việc kiểm tra địa chỉ **IP** đích của gói tin:

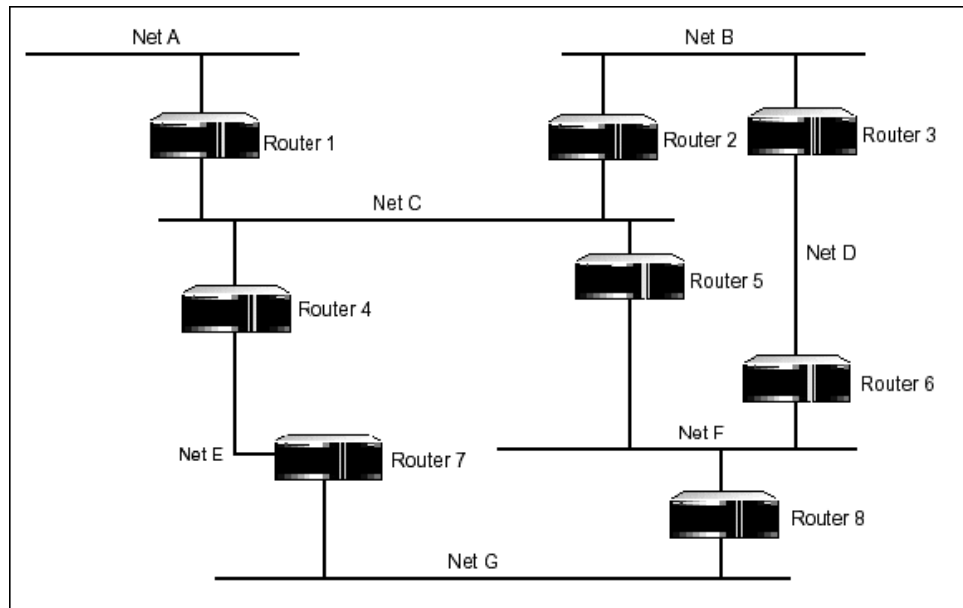
- Nếu địa chỉ mạng của **IP** đích này có trong bảng định tuyến của **Router**, **Router** sẽ gửi ra port tương ứng.

- Nếu địa chỉ mạng của **IP** đích này không có trong bảng định tuyến, **Router** sẽ kiểm tra xem trong bảng định tuyến của mình có khai báo **Default Gateway** hay không:

- + Nếu có khai báo **Default Gateway** thì gói tin sẽ được **Router** đưa đến **Default Gateway** tương ứng.

- + Nếu không có khai báo **Default Gateway** thì gói tin sẽ bị loại bỏ.

Chú ý: địa chỉ được xét ở đây là địa chỉ **IP**. Do cách hoạt động của **Router** như đã trình bày, nên mỗi **port** của **Router** là một **Broadcast Domain**.



Hình 5.34 – Mô hình mạng sử dụng **Router**.