CHƯƠNG 1
TỔNG QUAN VỀ MẠNG MÁY TÍNH

1.1 MỞ ĐẦU

Mạng máy tính phát sinh từ nhu cầu muốn chia sẻ, dùng chung tài nguyên và cho phép giao tiếp trực tuyến (online) cũng như các ứng dụng đa phương tiện trên mạng. Tài nguyên gồm có tài nguyên phần mềm (dữ liệu, chương trình ứng dụng,...) và tàinguyên phần cứng (máy in, máy quét, CD ROM,.). Giao tiếp trực tuyến bao gồm gửi và nhận thông điệp, thư điện tử. Các ứng dụng đa phương tiện có thể là phát thanh, truyền hình, điện thoại qua mạng, hội thảo trực tuyến, nghe nhạc và xem phim trực tuyến…

Trước khi mạng máy tính được sử dụng, người ta thường phải tự trang bị máy in, máy vẽ và các thiết bị ngoại vi khác cho riêng mình. Để có thể dùng chung máy in thì mọi người phải thay phiên nhau ngồi trước máy tính được nối với máy in. Khi được nối mạng thì tất cả mọi người ngồi tại các vị trí khác nhau đều có quyền sử dụng máy in đó.

Sự kết hợp của máy tính với các hệ thống truyền thông, đặc biệt là viễn thông đã tạo ra cuộc cách mạng trong vấn đề tổ chức khai thác và sử dụng hệ thống máy tính. Mô hình tập trung dựa trên máy tính lớn được thay thế mô hình các máy tính đơn lẻ được kết nối lại để cùng thực hiện công việc, hình thành môi trường làm việc nhiều người sử dụng phân tán, cho phép nâng cao hiệu quả khai thác tài nguyên chung từ những vị trí địa lý khác nhau. Các hệ thống như thế được gọi là mạng máy tính.

Mạng máy tính ngày nay đã trở thành một lĩnh vực nghiên cứu phát triển và ứng dụng cốt lõi của Công nghệ thông tin. Các lĩnh vực nghiên cứu phát triển và ứng dụng của mạng: kiến trúc mạng, nguyên lý thiết kế, cài đặt và các ứng dụng trên mạng.

1.2 CÁC KHÁI NIỆM CƠ BẢN

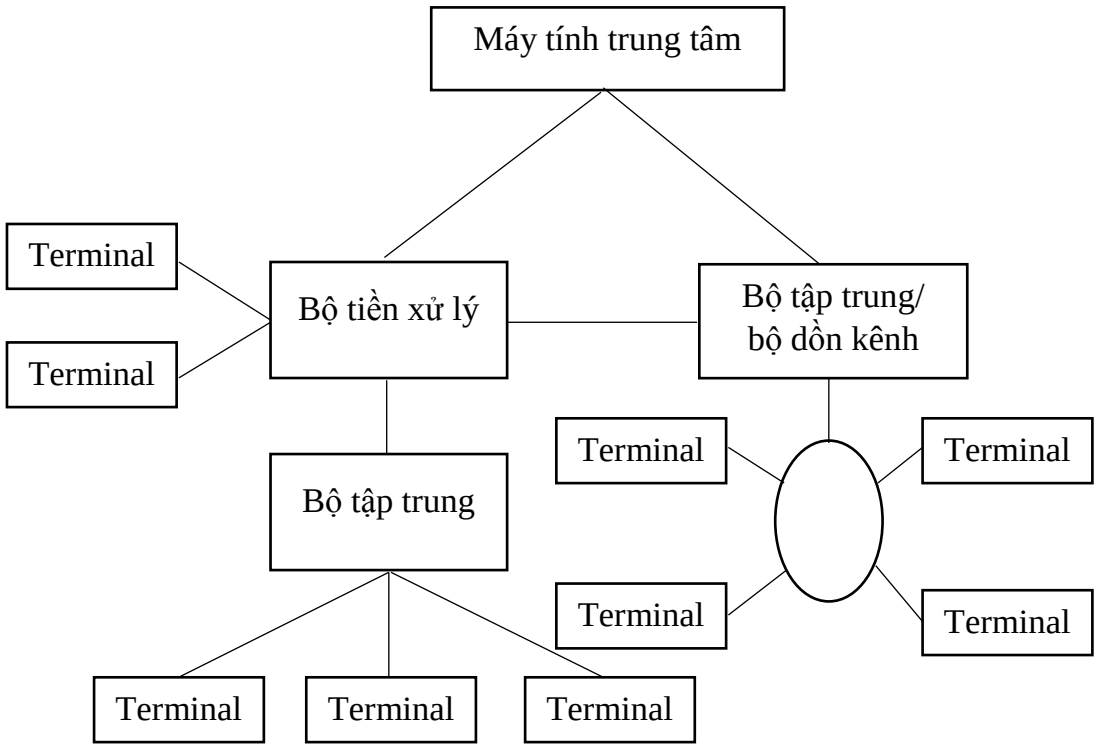
1.2.1 Lịch sử phát triển

Cuối những năm 60 đã xuất hiện các mạng xử lý gồm các trạm cuối (terminal) thụ động được nối vào một máy xử lý trung tâm. Máy tính trung tâm hầu như đảm nhiệm tất cả mọi việc từ xử lý thông tin, quản lý các thủ tục truyền dữ liệu, quản lý sự đồng bộ của các trạm cuối, quản lý các hàng đợi, xử lý các ngắt từ các trạm cuối,... Mô hình này bộc lộcác yếu điểm như: tốn quá nhiều vật liệu (đường truyền) để nối các trạm với trung tâm, máy tính trung tâm phải làm việc quá nhiều dẫn đến quá tải.

Để giảm nhẹ nhiệm vụ của máy tính trung tâm người ta gom các trạm cuối vào bộ gọi là bộ tập trung (hoặc bộ dồn kênh) trước khi chuyển về trung tâm. Các bộ này có chức năng tập trung các tín hiệu do trạm cuối gửi đến vào trên cùng một đường truyền. Sự khác nhau giữa hai thiết bị này thể hiện ở chỗ:

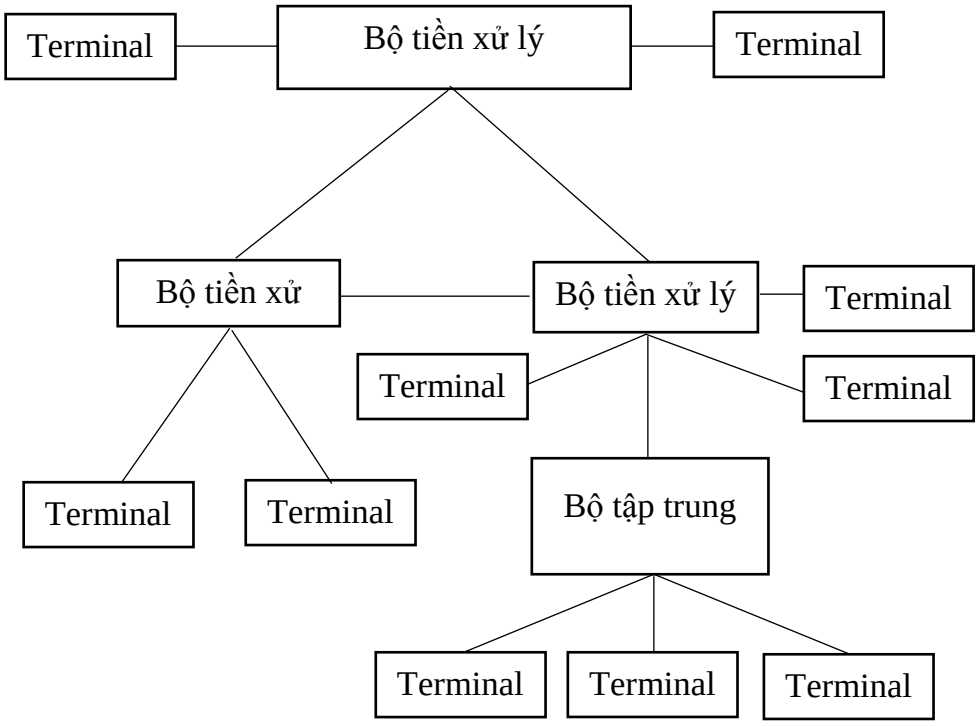
- Bộ dồn kênh (*multiplexor*): Có khả năng truyền song song các thông tin do trạm cuối gửi về trung tâm.
- Bộ tập trung (*concentrator*): Không có khả năng này, phải dùng bộ đệm để lưu trữ tạm thời dữ liệu.

Trong hệ thống này, mọi sự liên lạc giữa các trạm cuối với nhau phải đi qua máy tính trung tâm, không được nối trực tiếp với nhau. Hệ thống trên không được gọi là mạng máy tính mà chỉ được gọi là mạng xử lý.



Hình 1.1 Mạng xử lý với các bộ tiền xử lý

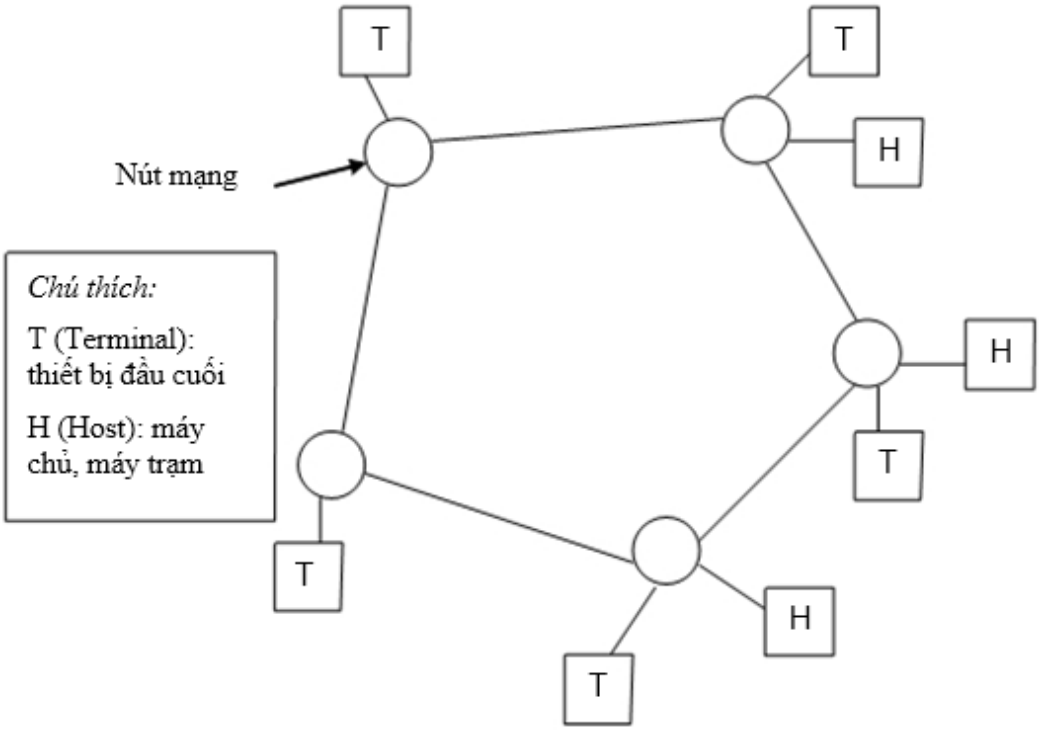
Từ cuối những năm 70, các máy tính được nối trực tiếp với nhau để tạo thành mạng máy tính nhằm phân tán tải của hệ thống và tăng độ tin cậy.



Hình 1.2 Mạng máy tính – nối trực tiếp các bộ tiền xử lý

Những năm 70 xuất hiện khái niệm mạng truyền thông (*communication network*), trong đó các thành phần chính của nó là các nút mạng (*Node*), được gọi là bộ chuyển mạch (*switching unit*) dùng để hướng thông tin tới đích.

Các nút mạng được nối với nhau bằng đường truyền gọi là khung của mạng. Các máy tính xử lý thông tin của người sử dụng (*host*) hoặc các trạm cuối (*terminal*) được nối trực tiếp vào các nút mạng để khi cần thì trao đổi thông tin qua mạng. Bản thân các nút mạng thường cũng là máy tính nên có thể đồng thời đóng cả vai trò máy của người sử dụng. Vì vậy chúng ta không phân biệt khái niệm mạng máy tính và mạng truyền thông.



Hình 1.3 Mạng truyền thông

Các máy tính được kết nối thành mạng nhằm đạt các mục đích sau:

- Chia sẻ các tài nguyên có giá trị cao (thiết bị, chương trình, dữ liệu,..) không phụ thuộc vào khoảng cách địa lý của tài nguyên và người sử dụng.
- Tăng độ tin cậy của hệ thống: do có khả năng thay thế khi xảy ra sự cố đối với một máy tính nào đó.

1.2.2 Mục đích và ứng dụng của mạng máy tính

1.2.2.1 Mục đích

Trong nhiều trường hợp, việc sử dụng mạng máy tính trong các cơ quan nhằm vào một số mục đích:

- *Mạng tạo khả năng dùng chung tài nguyên cho các người dùng*: Vấn đề là làm cho các tài nguyên trên mạng như chương trình, dữ liệu và thiết bị,…đặc biệt là các thiết bị đắt tiền, có sẵn dùng cho mọi người trên mạng mà không cần quan tâm đến vị trí thực của tài nguyên và người dùng.
- *Mạng cho phép nâng cao độ tin cậy:* Khi sử dụng mạng, có thể thực hiện một chương trình tại nhiều máy tính khác nhau, nhiều thiết bị có thể dùng chung. Điều

này làm tăng độ tin cậy trong công việc vì khi có máy tính hoặc thiết bị hỏng, công việc vẫn có thể tiếp tục với các máy tính hoặc thiết bị khác trên mạng trong khi chờ sửa chữa.

- *Tiết kiệm chi phí và thời gian:* Việc dùng chung các thiết bị ngoại vi cho phép giảm chi phí trang thiết bị tính trên số người dùng. Về phần mềm, nhiều nhà sản xuất phần mềm cung cấp cả những phiên bản cho nhiều người dùng với chi phí thấp hơn cho mỗi người dùng.

1.2.2.2 Các ứng dụng của mạng máy tính

Việc phát triển mạng máy tính đã tạo ra nhiều ứng dụng mới. Một số ứng dụng có ảnh hưởng quan trọng đến toàn xã hội: Khả năng truy xuất các chương trình và dữ liệu từ xa, khả năng thông tin liên lạc dễ dàng và hiệu quả, khả năng tìm kiếm thông tin nhanh chóng trên phạm vi toàn thế giới.

Định nghĩa ứng dụng mạng máy tính: Ứng dụng mạng là những ứng dụng mà trong khi chạy nó yêu cầu hệ thống lấy thông tin từ máy khác về.

- Truy nhập từ xa Telnet
- Truyền tệp (FTP)
- Gopher
- WAIS
- World Wide Web

1.2.3 Các yếu tố của mạng máy tính

1.2.3.1 Định nghĩa mạng máy tính

Mạng máy tính là tập hợp hai hay nhiều máy tính được kết nối với nhau bởi đường truyền theo một kiến trúc nào đó sao cho chúng có thể trao đổi dữ liệu qua lại với nhau dễ dàng.

Hình 1.4 Mô hình mạng cơ bản

Về cơ bản, một mạng máy tính là một số các máy tính được kết nối với nhau theo một cách nào đó. Khác với các trạm truyền hình chỉ gửi thông tin đi, các mạng máy tính luôn có hai chiều, sao cho khi máy tính PC1 gửi thông tin tới máy tính PC2 thì PC2 có thể trả lời lại PC1. Nói một cách khác, một số máy tính được kết nối với nhau và có thể trao đổi thông tin cho nhau gọi là mạng máy tính.

1.2.3.2 Đường truyền vật lý

Đường truyền vật lý dùng để chuyển các tín hiệu giữa các máy tính. Các tín hiệu đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (*on - off*). Tất cả các tín hiệu đó đều thuộc dạng sóng điện từ (trải từ tần số sóng radio, sóng ngắn, tia hồng

ngoại). Ứng với mỗi loại tần số của sóng điện tử có các đường truyền vật lý khác nhau để truyền tín hiệu.

Hiện nay có hai loại đường truyền:

- Đường truyền hữu tuyến gồm có:
  - ✓ Cáp đồng trục *(coaxial cable)*
  - ✓ Cáp đôi dây xoắn *(twisted – pair cable):* có 2 loại là STP và UTP.
  - ✓ Cáp sợi quang *(fiber optic cable)*
- Đường truyền vô tuyến gồm có:
  - ✓ Radio
  - ✓ Sóng cực ngắn *(viba hay microware)*
  - ✓ Tia hồng ngoại (fibered)

Liên quan đến đường truyền vật lý chúng ta có các khái niệm về Băng thông, tốc độ và thông lượng

- *Băng thông (còn gọi là dải thông - bandwidth)*: Băng thông là một khái niệm cực kỳ quan trọng trong các hệ thống truyền thông. Hai phương pháp xem xét băng thông có tầm quan trọng trong nghiên cứu các mạng là băng thông tương tự (*analog*) và băng thông số (*digital*).

Băng thông tương tự: là độ đo phạm vi tần số mà đường truyền có thể đáp ứng được trong một hệ thống điện tử dùng kỹ thuật tương tự. Đơn vị đo lường cho băng thông tương tự là Hz, hay số chu kỳ trên giây. Ví dụ, băng thông của cáp điện thoại là 400-4000Hz, có nghĩa là nó có thể truyền các tín hiệu với các tần số nằm trong phạm vi từ 400 đến 4000Hz.

Băng thông số: đo lường lượng thông tin tốiđa từ nơi này đến nơi khác trong một thời gian cho trước. Đơn vị cơ bản đo lường băng thông số là bít/giây (bps) và các bội của nó là Kilobit/giây (kbps), Megabit/giây (Mbps), Gigabit/giây (Gbps), Terabit/giây (Tbps)…

Băng thông của cáp truyền phụ thuộc vào độ dài cáp. Cáp càng dài thì băng thông càng giảm. Do vậy khi thiết kế mạng phải chỉ rõ độ dài chạy cáp tối đa, bởi vì ngoài giới hạn đó thì chất lượng truyền tín hiệu không còn được bảo đảm.

- *Thông lượng (throughput*): Là lượng thông tin thực sự được truyền qua trong một đơn vị thời gian. Cũng như băng thông, đơn vị của thông lượng là bps và các bội của nó: Kbps, Mbps, Gbps, Gbps, Tbps. Trong một mạng LAN băng thông có thể cho phép 100Mbps, nhưng điều này không có nghĩa là mỗi người dùng trên mạng đều có thể di chuyển thực sự 100 Megabit dữ liệu trong một giây. Điều này chỉ đúng trong những điều kiện vô cùng lý tưởng. Do nhiều lý do, thông lượng thường nhỏ hơn rất nhiều so với băng thông số tối đa của môi trường mạng.

- *Tốc độ (rate*): Tốc độ thường được tính bằng đơn vị bps,nghĩa là số bit truyền đi trong 1 giây. Ví dụ: Tốc độ trên đường truyền Ethernet là 10Mbps nghĩa là 10 triệu bit được truyền trong 1 giây.

- *Hiệu suất sử dụng đường truyền (utilization):* Đại lượng này đặc trưng cho hiệu suất phục vụ của đường truyền trong mạng. Nó được đo bằng tỷ lệ % giữa thông lượng và băng thông của đường truyền.

- *Độ trễ (delay):* Là thời gian cần thiết để truyền một gói tin từ nguồn đến đích. Độ trễ thường được đo bằng miligiây (ms), giây (s). Độ trễ phụ thuộc vào băng thông củamạng. Băng thông càng lớn thì độ trễ càng nhỏ.

- *Độ suy hao:*Là độ đo sự yếu đi của tín hiệu trên đường truyền. Nó cũng phụ thuộc vào độ dài cáp. Còn độ nhiễu từ gây ra bởi tiếng ồn điện từ bên ngoài làm ảnh hưởng đến tín hiệu trên đường truyền.

1.2.3.3 Kiến trúc mạng máy tính

Kiến trúc mạng máy tính thể hiện cách nối các máy tính với nhau ra sao và tập hợp các quy tắc, quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt.

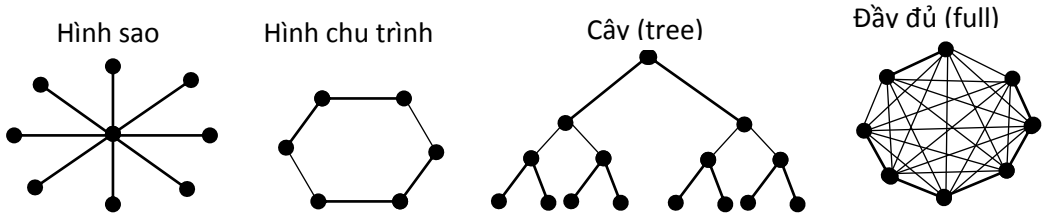
Cách nối các máy tính được gọi là hình trạng *(Topolopy)* của mạng hay còn gọi là Topo mạng. Còn tập hợp các quy tắc, quy ước truyền thông được gọi là giao thức *(Protocol)* của mạng. Topo và giao thức là hai khái niệm rất cơ bản của mạng máy tính, vì thế chúng sẽ được trình bày cụ thể hơn trong những phần sau.

- **Topo mạng**

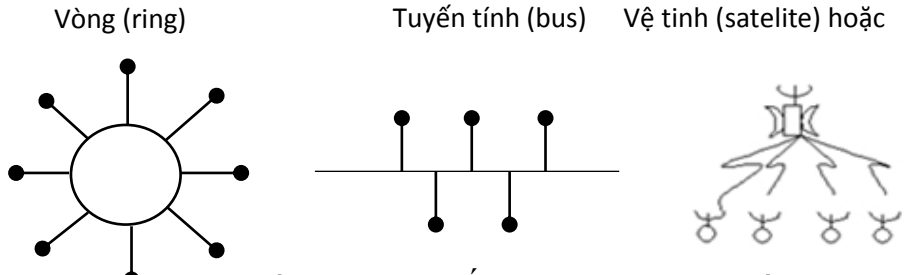
Có hai kiểu kết nối mạng chủ yếu là điểm - điểm *(point - to - point)* và quảng bá *(broadcast hay point - to - multipoint).*

Theo kiểu kết nối điểm - điểm, các đường truyền nối từng cặp nút với nhau và mỗi nút đều có trách nhiệm lưu trữ tạm thời sau đó chuyển tiếp dữ liệu đi tới đích. Do cách làm việc như thế nên mạng kiểu này còn được gọi là mạng lưu và chuyển tiếp *(store and forward)*. Nói chung các mạng diện rộng đều sử dụng nguyên tắc này. Hình 1.5 cho một số dạng topo của mạng loại này.

Theo kiểu quảng bá, tất cả các nút mạng dùng chung một đường truyền vật lý. Dữ liệu gửi đi từ một nút mạng có thể được tất cả các nút mạng còn lại tiếp nhận và chỉ cần chỉ ra địa chỉ đích của dữ liệu để mỗi nút kiểm tra xem có phải là gửi cho mình hay không. Hình 1.6 cho một số dạng topo của mạng loại này.



Hình 1.5 Một số topo mạng điểm – điểm



Hình 1.6 Một số topo mạng quảng bá

Trong các topo dạng vòng hoặc dạng tuyến tính cần có một cơ chế "trọng tài" để giải quyết xung đột khi nhiều nút muốn truyền tin cùng một lúc. Việc cấp phát đường truyền có thể là "động" hoặc "tĩnh". Cấp phát "tĩnh" thường dùng cơ chế quay vòng để phân chia đường truyền theo các khoảng thời gian định trước. Cấp phát "động" là cấp phát theo yêu cầu để hạn chế thời gian "chết" vô ích của đường truyền.

- **Giao thức mạng**

Việc trao đổi thông tin cho dù là đơn giản nhất, cũng đều phải tuân theo những quy tắc nhất định. Hai người nói chuyện với nhau muốn cho cuộc nói chuyện có kết quả thì ít nhất cả hai cũng phải ngầm định tuân theo quy tắc: khi người này nói thì người kia phải nghe và ngược lại. Việc truyền tín hiệu trên mạng cũng vậy, cần phải có những quy tắc, quy ước về nhiều mặt:

- ✓ Khuôn dạng của dữ liệu: cú pháp và ngữ nghĩa.
- ✓ Thủ tục gửi và nhận dữ liệu.
- ✓ Kiểm soát chất lượng truyền.
- ✓ Xử lý các lỗi, sự cố.

Tập hợp tất cả các quy tắc và quy ước trên gọi là giao thức mạng. Yêu cầu về xử lý và trao đổi thông tin của người sử dụng ngày càng cao thì giao thức mạng càng phức tạp.Các mạng có thể có giao thức khác nhau tuỳ thuộc vào sự lựa chọn của nhà thiết kế.

1.2.4 Phân loại mạng máy tính

Có nhiều cách để phân loại mạng tuỳ thuộc vào yếu tố chính được chọn làm chỉ tiêu để phân loại: khoảng cách địa lý, kỹ thuật chuyển mạch, kiến trúc của mạng

1.2.4.1 Theo khoảng cách địa lý

Nếu lấy khoảng cách địa lý làm yếu tố chính để phân loại thì mạng máy tính được phân thành 4 loại: mạng cục bộ*(LAN)*, mạng đô thị*(MAN)*, mạng diện rộng*(WAN)*, mạng toàn cầu*(GAN).*

a. ***Mạng cục bộ (Local Area Networks - LAN):*** cài đặt trong phạm vi tương đối hẹp (ví dụ như trong một tòa nhà, một cơ quan, một trường học,..), khoảng cách lớn nhất giữa các máy tính nối mạng là vài chục km trở lại.

b. ***Mạng đô thị (Metropolitan Area Networks - MAN):*** cài đặt trong phạm vi một đô thị, một trung tâm kinh tế xã hội, có bán kính nhỏ hơn 100 km.

c. ***Mạng diện rộng (Wide Area Networks - WAN):*** Phạm vi của mạng có thể vượt qua biên giới quốc gia và thậm chí cả lục địa.

d. ***Mạng toàn cầu (Global Area Networks - GAN):*** Phạm vi rộng khắp toàncầu. Mạng Internet là một ví dụ cho loại này.

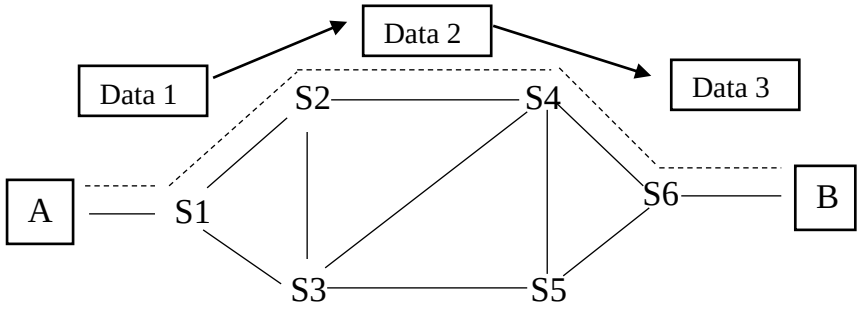
Chúng ta cũng cần lưu ý rằng: khoảng cách địa lý được dùng làm "mốc" chỉ mang tính tương đối. Cùng với sự phát triển của các công nghệ truyền dẫn và quản trị mạng thì những ranh giới đó ngày càng mờ nhạt đi.

1.2.4.2 Theo kỹ thuật chuyển mạch

Nếu lấy "kỹ thuật chuyển mạch" làm yếu tố chính để phân loại thì ta có 3 loại: mạng chuyển mạch kênh, mạng chuyển mạch thông báo và mạng chuyển mạch gói.

a. Mạng chuyển mạch kênh

Khi có hai thực thể cần trao đổi thông tin với nhau thì giữa chúng sẽ thiết lập một "kênh" cố định và được duy trì cho đến khi một trong hai bên ngắt liên lạc. Các dữ liệu chỉ được truyền theo con đường cố định đó.



Hình 1.7 Mạng chuyển mạch kênh

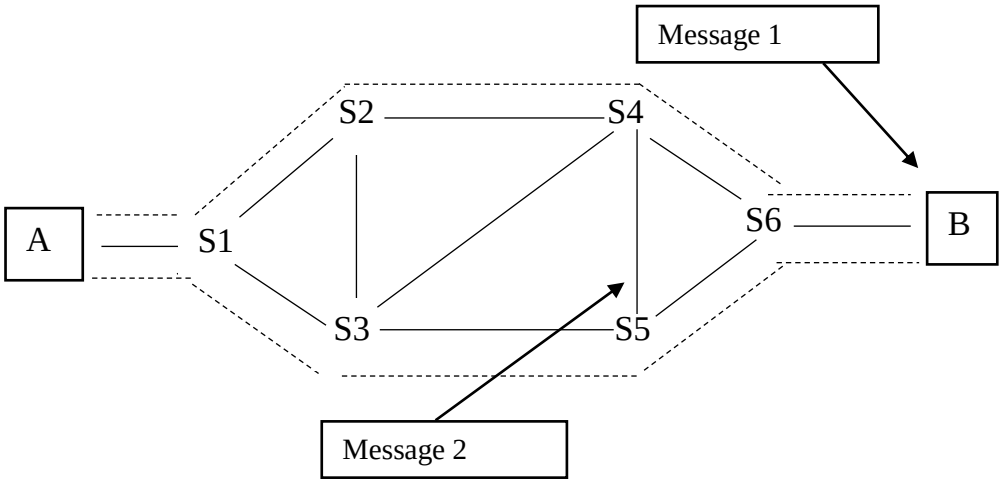
Nhược điểm:

- ✓ Tốn thời gian để thiết lập kênh cố định giữa hai thực thể.
- ✓ Hiệu suất sử dụng đường truyền thấp vì sẽ có lúc kênh bị bỏ không do cả hai bên đều hết thông tin cần truyền trong khi các thực thể khác không được phép sử dụng kênh truyền

b. Mạng chuyển mạch thông báo

Thông báo (message) là một đơn vị thông tin của người sử dụng có khuôn dạng được qui định trước. Mỗi thông báo đều có chứa vùng thông tin điều khiển trong đó chỉ định rõ đích đến của thông báo. Căn cứ vào thông tin này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp theo đường dẫn tới đích của nó.

Mỗi nút cần phải lưu trữ tạm thời để "đọc" thông tin điều khiển trên thông báo để sau đó chuyển tiếp thông báo đi. Tuỳ thuộc vào điều kiện của mạng, các thông báo khác nhau có thể truyền theo đường truyền khác nhau.



Hình 1.8. Mạng chuyển mạch thông báo

Ưu điểm so với mạng chuyển mạch kênh:

- ✓ Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được phân chia giữa nhiều thực thể.

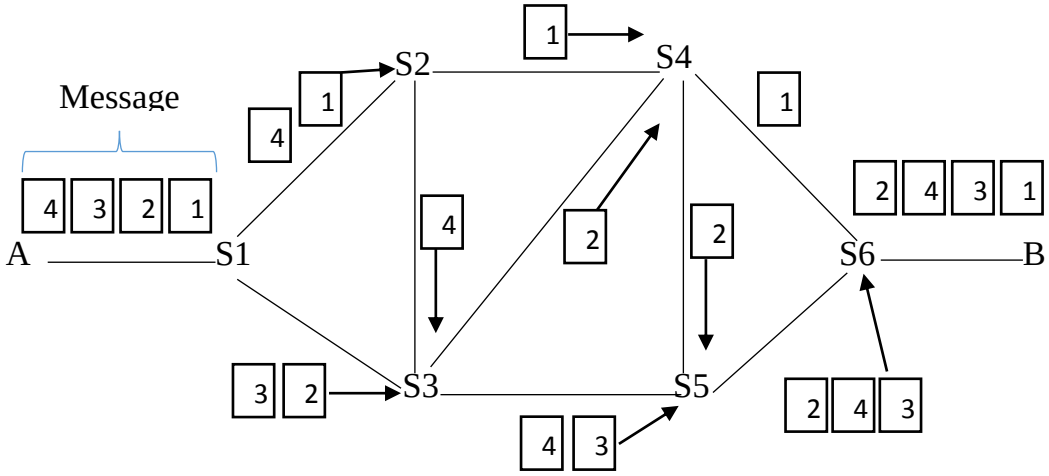
- ✓ Mỗi nút mạng có thể lưu trữ thông báo cho tới khi kênh truyền rỗi mới gửi thôngbáo đi, vì vậy giảm được tình trạng tắc nghẽn mạch.
- ✓ Có thể điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên cho thông báo
- ✓ Có thể tăng hiệu suất sử dụng dải thông bằng cách gán địa chỉ quảng bá để gửi thông báođồng thời tới nhiều đích.

Nhược điểm:

- ✓ Không hạn chế kích thước của thông báo, dẫn đến phí tổn lưu trữ tạm thời cao và ảnh hưởng tới thời gian đáp (response time), chất lượng truyền tin.
- ✓ Thích hợp cho các dịch vụ thư tín điện tử hơn là các áp dụng có tính thời gian thực vì tồn tại độ trễ do lưu trữ và xử lý thông tin điều khiển tại mỗi nút.

c) Mạng chuyển mạch gói

Mỗi thông báo được chia làm nhiều phần nhỏ hơn được gọi là các gói tin có khuôn dạng quy định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và đích (người nhận) của gói tin. Các gói tin của một thông báo có thể đi qua mạng tới đích bằng nhiều con đường khác nhau. Ở bên nhận, thứ tự nhận được có thể không đúng thứ tự được gửi đi.



Hình 1.9 Mạng chuyển mạch gói

So sánh mạng chuyển mạch thông báo và mạng chuyển mạch gói:

Các gói tin được giới hạn kích thước tối đa sao cho các nút mạng cóthể xử lý toàn bộ gói tin trong bộ nhớ mà không cần phải lưu trữ tạm thời trên đĩa. Vìthế mạng chuyển mạch gói truyền các gói tin qua mạng nhanh chóng và hiệu quả hơnso với mạng chuyển mạch thông báo. Nhưng vấn đề khó khăn của mạng loại này làviệc tập hợp các gói tin để tạo lại thông báo ban đầu của người sử dụng, đặc biệt trongtrường hợp các gói được truyền theo nhiều đường khác nhau. Cần phải cài đặt cơ chế"đánh dấu" gói tin và phục hồi gói tin bị thất lạc hoặc truyền bị lỗi cho các nút mạng.

Do có ưu điểm mềm dẻo và hiệu suất cao hơn nên hiện nay mạng chuyển mạch gói được sửdụng phổ biến hơn các mạng chuyển mạch thông báo. Việc tích hợp cả haikỹ thuật chuyểnmạch (kênh và gói) trong một mạng thống nhất (được gọi là mạng dịch vụ tích hợp số- *Intergrated Services Digital Networks*, viết tắt là ISDN) đang là một xu hướng phát triển của mạng ngày nay.

1.2.4.3Theo kiến trúc mạng

Người ta còn phân loại mạng theo kiến trúc mạng (topo và giao thức sử dụng). Các mạng thường hay được nhắc đến như: SNA của IBM, TCP/IP,...

1.2.5 Mạng toàn cầu Internet

Mạng toàn cầu là một tập hợp gồm hàng vạn mạng trên khắp thế giới. Mạng Internet bắt nguồn từ một thử nghiệm của Cục quản lý các dự án nghiên cứu tiên tiến *(Advanced Research Projects Agency - ARPA)* thuộc Bộ quốc phòng Mỹ đã kết nối thành công các mạng máy tính cho phép các trường đại học và các công ty tư nhân tham gia vào các dự án nghiên cứu..

Về cơ bản, Internet là một liên mạng máy tính giao tiếp dưới cùng một bộ giao thức TCP/IP *(Transmission Control Protocol/Internet Protocol)*. Giao thức này cho phép mọi máy tính trên mạng giao tiếp với nhau một cách thống nhất giống như một ngôn ngữ quốc tế mà mọi người sử dụng để giao tiếp với nhau hàng ngày.

Số lượng máy tính kết nối mạng và số lượng người truy cập vào mạng Internet trên toàn thế giới ngày càng tăng lên nhanh chóng, đặc biệt từ những năm 90 trở đi. Mạng Internet không chỉ cho phép chuyển tải thông tin nhanh chóng mà còn giúp cung cấp thông tin, nó cũng là diễn đàn và là thư viện toàn cầu đầu tiên.

1.3 HỆ ĐIỀU HÀNH MẠNG

1.3.1 Đặc điểm, quy định chức năng của một hệ điều hành mạng

Môi trường mạng có những đặc điểm riêng, khác với môi trường chỉ dùng máy tính cá nhân (PC), thể hiện ở các đặc trưng sau:

- Trước hết đó là môi trường nhiều người dùng. Đặc điểm này dẫn đến các nhu cầu liên lạc giữa những người sử dụng, nhu cầu bảo vệ dữ liệu và nói chung là bảo vệ tính riêng tư của người sử dụng.
- Mạng còn là môi trường đa nhiệm, có nhiều công việc thực hiện trên mạng. Đặc điểm này sẽ phát sinh các nhu cầu chia sẻ tài nguyên, nhu cầu liên lạc giữa các tiến trình như trao đổi dữ liệu, đồng bộ hoá.
- Là môi trường phân tán, tài nguyên (thông tin, thiết bị) nằm ở các vị trí khác nhau, chỉ kết nối thông qua các đường truyền vật lý. Điều này phát sinh các nhu cầu chia sẻ tài nguyên trên toàn mạng nhưng sự phân tán cần được trong suốt để nó không gây khó khăn cho người sử dụng.
- Có nhiều quan niệm cũng như các giải pháp mạng khác nhau. Điều đó nảy sinh nhu cầu giao tiếp giữa các mạng khác nhau.
- Làm việc trên môi trường mạng chắc chắn sẽ phức tạp hơn môi trường máy đơn lẻ. Vì thế rất cần có các tiện ích giúp cho việc sử dụng và quản trị mạng dễ dàng và hiệu quả.
- Tất cả các nhu cầu trên phải được tính tới trong hệ điều hành mạng.

1.3.2 Các tiếp cận thiết kế và cài đặt

Để thiết kế và cài đặt một hệ điều hành mạng có hai cách tiếp cận khác nhau:
(1) Tôn trọng tính độc lập của các hệ điều hành cục bộ đã có trên các máy tính của mạng. Khi đó hệ điều hành mạng được cài đặt như một tập các chương trình tiện ích

chạy trên các máy khác nhau của mạng. Giải pháp này tuy không được "đẹp" nhưng dễ cài đặt và không vô hiệu hóa được các phần mềm đã có.

(2) Bỏ qua các hệ điều hành đã có trên các máy và cài đặt mới hoàn toàn một hệ điều hành thuần nhất trên toàn mạng, gọi là hệ điều hành phân tán. Giải pháp này tốt hơn về phương diện hệ thống so với giải pháp trên, nhưng bù lại độ phức tạp trong công việc thì lớn hơn rất nhiều. Mặt khác, việc tôn trọng tính độc lập và chấp nhận sự tồn tại của các sản phẩm hệ thống đã có là một điểm hấp dẫn của các tiếp cận thứ nhất. Bởi vậy tùy theo điều kiện cụ thể mà ta áp dụng giải pháp nào cho phù hợp. Sau đây ta xem xét cụ thể hơn về từng giải pháp nói trên.

Hệ điều hành theo giải pháp (1)

Tư tưởng chủ đạo của giải pháp này là cung cấp cho mỗi người sử dụng mọi tiến trình đồng nhất mà ta gọilà Agent làm nhiệm vụ cung cấp một giao diện đồng nhất và tất cả các hệ thống cục bộ đãcó Agent quản lý một cơ sở dữ liệu chứa các thông tin về các hệ thống cục bộ và chươngtrình dữ liệu của người sử dụng trong trường hợp đơn giản nhất Agent chỉ hoạt động nhưmột bộ xử lý lệnh, dịch các lệnh của người sử dụng thành ngôn ngữ lệnh của hệ thốngcục bộ rồi gửi chúng để thực hiện trước khi mỗi chương trình thực hiện, Agent phải đảmbảo rằng tất cả các tập cần thiết đề sử dụng. Việc cài đặt mạng như vậy sẽ chống lại haicông việc chính: thiết kế ngôn ngữ lệnh của mạng và cài đặt Agent.

Cách tiếp nhận này đơn giản và không gây ảnh hưởng đến hệ thống cục bộ đã có sẵn.Thậm chí các hệ thống cục bộ không cần thiết đến sự tồn tại của mạng. Nhưng giải pháp này chỉ có thể khả thi khi mà tất cả các tập tin cần thiết đều biết trước để Agent có thể gửi chúng tới một hệ thống cục bộ trước khi chương trình bắt đầu hoạt động. Ngoài ra rất khó thực hiện các tương tác vào ra mà chương trình lại không biết tới sự tồn tại của mạng. Một giải pháp tổng quát hơn nhằm bỏ tiến trình đang chạy lại bằng cách tóm tắt tất cả các lời gọi hệ thống *(System Call)* của nó để chúng có thể thực hiện trong bối cảnh của hệ thống quản lý tệp của mạng *(NetWork file System).*

Hệ điều hành theo giải pháp (2)

Trong trường hợp này người ta gọi là hệ điều hành phân tán và có thể được thiết kế một trong hai mô hình: Mô hình tiến trình hoặc mô hình đối tượng.

Trong mô hình tiến trình mỗi tài nguyên (tập, đĩa, thiết bị ngoại vi,…) được quản lý theo một tiến trình nào đó và hệ điều hành mạng điều khiển sự tương tác giữa các tiến trình đó. Các dịch vụ của hệ điều hành mạng tập trung truyền thông như quản lý tệp, lên lịch cho bộ xử lý, điều khiển terminal,... được quản lý bởi các Server đặc biệt có khả năng tiếp nhận các yêu cầu thực hiện dịch vụ tương ứng trong nhiều trường hợp các Server có thể chạy như tiến trình của người sử dụng thông thường.

Trong mô hình đối tượng, thế giới bao gồm các đối tượng khác nhau, mỗi đối tượngcó một kiểu (type), một biểu diễn và một tập các thao tác có thể thực hiện trên nó. Đểthực hiện một thao tác trên một đối tượng, chẳng hạn đọc một tệp tin trên một tiến trìnhngười sử dụng phải có "giấy phép" đối với đối tượng. Nhiệm vụ cơ bản của hệ điều hànhđây là quản lý các giấy phép và cấp phát các "giấy phép" đó cho các tiến trình để thực hiện cho các thao tác cần thiết. Trong một hệ tập trung, bản thân hệ điều hành nằm giữ các "giấy phép" bên trong để ngăn ngừa những người sử dụng cố ý giả mạo chúng. Trong một hệ phân tán các "giấy phép" được luân chuyển theo một cách

nào đó để mỗi tiến trình đều có cơ hội nhận được "giấy phép" và sao cho người sử dụng không thể tự tạo ra được chúng.

Việc thiết kế hệ điều hành phân tán theo mô hình đối tượng là một hướng đi rấttriển vọng và tồn tại nhiều vấn đề cần giải quyết trọn vẹn hơn. Còn đối với tiến trình thìchúng ta có thể thấy rõ nhiệm vụ then chốt chính là xây dựng cơ chế liên lạc giữa các tiếntrình *(Interprocess Communication - IPC).* Để làm điều đó người ta sử dụng một tronghai cách: dùng lời gọi hàm *(Function/procedure Calls)* hoặc chuyển thông báo *(messagepassing).*

Khi các lời gọi hàm hoặc thủ tục được dùng làm cơ chế IPC, hệ thống đầy đủ baogồm tệp và các hàm (hoặc thủ tục) được viết tắt theo ngôn ngữ nào đó. Mã của các hàmnào được phân tán cho các bộ vi xử lý. Để thực hiện việc truyền thông giữa các máy, mộthàm trên máy này có thể gọi một hàm trên máy khác. Ngữ nghĩa của các lời gọi hàm đâycũng giống như đối với các lời gọi hàm thông thường: hàm gọi bị treo cho đến khi hàmgọi được kết thúc, tham số được truyền từ hàm gọi cho đến hàm được gọi, còn kết quảđược chuyển theo chiều ngược lại. Cách tiếp cận này dẫn đến một hệ điều hành được viết như một chương trình lớn, ưu điểm là chặt chẽ và nhất quán, tuy nhiên thiếu mềm dẻo.

Nếu dùng phương pháp chuyển thông báo của cơ chế IPC thì các tiến trình sẽ liên tục vớinhau bằng cách chuyển thông báo. Mã của các tiến trình được tách biệt và có thể viết bằng các ngôn ngữ khác. Cách tiếp cận này đòi hỏi nhiều vấn đề hơn cách tiếp cận gọi hàm, chẳng hạn vấn đề địa chỉ hóa thiết lập các liên kết ảo, cắt, hợp thông báo, kiểm soát luồng dữ liệu truyền thông báo *(broad casting).*

1.3.3 Các kiểu hệ điều hành mạng

1.3.3.1Kiểu ngang hàng (peer-to-peer)

Mọi trạm đều có quyền bình đẳng như nhau và đều có thể cung cấp tài nguyên cho các trạm khác. Các tài nguyên cung cấp được có thể là tập tin (tương ứng với thiết bị là đĩa), máy in. Nói chung trong các mạng ngang hàng không có việc biến một máy tính thành một trạm làm việc của một máy tính khác. Trong mạng ngang hàng, thông thường các máy sử dụng chung một hệ điều hành.

Win 95, NT Workstation, Lanstic Novell Lite, Win XP, Win 7, Win 8,… là các hệ điều hành mạng ngang hàng.

Các đặc điểm của mạng ngang hàng:

- Thích hợp với các mạng cục bộ quy mô nhỏ, đơn lẻ, các giao thức riêng lẻ, mức độ thấp và giá thành rẻ.
- Các mạng ngang hàng được thiết kế chủ yếu cho các mạng nội bộ vừa và nhỏ và sẽ hỗ trợ tốt các mạng dùng một nền và một giao thức. Các mạng trên nhiều nền, nhiều giao thức sẽ thích hợp hơn với hệ điều hành có máy chủ dịch vụ.
- Người dùng được phép chia sẻ file và tài nguyên nằm trên máy của họ và truy nhập đến các tài nguyên được chia sẻ trên máy người khác nhưng không có nguồn quản lý tập trung.
- Vì mạng ngang hàng không cần máy cụ thể làm máy chủ. Chúng thường là một phần của hệ điều hành nền hay là phần bổ sung cho hệ điều hành và thường rẻ hơn so với các hệ điều hành dựa trên máy chủ.

- Trong một mạng ngang hàng, tất cả các máy tính được coi là bình đẳng, bởi vì chúng có cùng khả năng sử dụng các tài nguyên có sẵn trên mạng.

Những thuận lợi:

- Chi phí ban đầu ít - không cần máy chủ chuyên dụng.
- Cài đặt - một hệ điều hành có sẵn (ví dụ Win XP, 7, 8) có thể chỉ cần cấu hình lại để hoạt động ngang hàng.

Những bất lợi:

- Không quản lý tập trung được.
- Bảo mật kém.
- Có thể tốn rất nhiều thời gian để bảo trì.

1.3.3.2 Kiểu hệ điều hành mạng có máy chủ *(server based network)*

Trong hệ điều hành kiểu này, có một số máy có vai trò cung cấp dịch vụ cho máy khác gọi là máy chủ (đúng hơn phải gọi là máy cung cấp dịch vụ - mà khi đó thì phải xem là máy "tớ").

Các dịch vụ có nhiều loại, từ dịch vụ tệp (cho phép sử dụng tệp trên máy chủ), dịch vụ in (do một máy chủ điều khiển những máy in chung của mạng) tới các dịch vụ như thư tín, WEB, DNS,...

Trong mạng có máy chủ, hệ điều hành trên máy chủ và máy trạm có thể khác nhau. Ngay trong trường hợp máy chủ và máy trạm sử dụng cùng một hệ điều hành thì chức năng của bản trên máy chủ cũng có thể khác với chức năng cài đặt trên máy trạm.

Sau đây là một số hệ điều hành có dùng máy chủ: Novell Netware 4.1 Microsoft NT V4.0, Winddow Server, OS/2 LAN Server.

Đặc điểm của các hệ điều hành có máy chủ:

- Hệ điều hành cho các mạng an toàn, hiệu suất cao, chạy trên nhiều nền khác nhau (kể cả phần cứng, hệ điều hành và giao thức mạng)
- Một máy chủ là một máy tính trong mạng được chia sẻ bởi nhiều người dùng, như các máy dịch vụ file, máy dịch vụ in, máy dịch vụ truyền tin. Nói cách khác, nó được thiết kế để cung cấp một dịch vụ cụ thể, khác với các hệ máy tính nhiều người dùng, tập trung và đa mục đích mặc dù máy dịch vụ file kết hợp với các hệ thống như hệ điều hành mạng Novell's NetWare 3.xx hay 4.xx, Windows Server thường hoạt động theo cách đó.
- Kiểm soát quyền sử dụng trên toàn mạng tại máy chủ.
- Cung cấp các dịch vụ thư mục trên toàn mạng.
- Các giải pháp dựa trên máy chủ được coi là sự quản trị mạng tập trung và thường là máy quản lý mạng nội bộ chuyên dụng.
- Bản thân máy chủ có thể chỉ là máy chủ chuyên dụng như Novell Netware 4.1, máy này không thể hoạt động như một máy trạm. Cũng có những hệ điều hành mà máy chủ NT cũng có thể được sử dụng như một máy trạm.

1.3.3.3 Mô hình khách/chủ*(Client/Server)*

Đầu thập niên 60, việc sử dụng máy tính thực hiện theo mô hình tập trung. Các trạm thực sự chỉ làm việc giao tiếp còn việc xử lý thực sự tiến hành ở một máy tính nào đó. Như vậy với mô hình này hoàn toàn không có xử lý cộng tác. Một phát triển tiếp theo là mô hình xử lý chủ tớ (master/slaver) với việc một máy xử lý và chuyển giao một số công việc cho các máy cấp thấp hơn, hoàn toàn không có việc máy cấp thấp hơn liên lạc hoặc giao việc theo chiều ngược lại. Như vậy quá trình cộng tác chỉ là một chiều.

Một bước đột phá trong mô hình tính toán cộng tác là mô hình chia sẻ thiết bị (shared device) theo đó một máy có thể cho máy khác sử dụng thiết bị của mình (chủ yếu là đĩa và máy in). Hệ điều hành mạng theo kiểu ngang hàng hay có sử dụng máy chủ dịch vụ đều có thể dùng cho mô hình này. Tuy nhiên chỉ ở mức này thôi thì chính CPU chưa bị chia sẻ nghĩa là chưa có sự phân tán trong xử lý mà chủ yếu là phân tán thông tin. Ngay cả việc sử dụng máy in từ xa cũng không mang ý nghĩa của xử lý phân tán vì thực chất chỉ là gửi nội dung in tới hàng đợi của một máy in do một máy tính nào đó quản lý mà thôi. Máy chủ cung cấp dịch vụ in không tạo ra giá trị mới cho công việc của máy uỷ thác dịch vụ in.

Trong những năm gần đây đã xuất hiện mô hình khách chủ trong đó một số máychủ đóng vai trò cung ứng dịch vụ theo yêu cầu của các máy trạm. Máy trạm trong mô hình này gọi là máy khách (client) là nơi gửi các yêu cầu xử lý về cho máy chủ. Máy chủ(server) xử lý và gửi kết quả về máy khách. Máy khách có thể tiếp tục xử lý các kết quả này phục vụ cho cộng việc. Như vậy máy khách chịu trách nhiệm chủ yếu về giao diện và chỉ đảm nhận một phần xử lý. Trong mô hình khách/chủ xử lý thực sự phân tán.

Ta nói đến mô hình khách chủ chứ không nói đến hệ điều hành khách chủ vì trên thực tế mô hình khách chủ yêu cầu phải có một hệ điều hành dựa trên máy chủ dù máy chủ này ở trong mạng cục bộ hay máy chủ cung cấp dịch vụ từ một mạng khác. Hầu hết các ứng dụng trên Internet là ứng dụng khách chủ sử dụng từ xa.

Lưu ý rằng các tiến trình khách và chủ đôi khi có thể thực hiện trên cùng một máytính.

- Client process và server process có thể hoạt động trên cùng một bộ xử lý, trên các bộ sử lý khác nhau ở cùng một máy (các bộ xử lý song song) hoặc trên các bộ xử lý khác nhau trên các máy khác nhau (xử lý phân tán).
- Một điều quan trọng cần nhận thấy là cả hệ điều hành ngang hàng và hệ điều hành dựa trên máy chủ đều có thể thỏa mãn mô hình khách/chủ. Trên thực tế, hầu hết các hệ điều hành hiện đại đều cung cấp ít nhất một vài chức năng khách-chủ.

Hệ điều hành khách/chủ

Các hệ điều hành cho cấu trúc khách/chủ bao gồm: Sun Solaris NFS, UnixWare NFS, Novell Netware và Windows NT Server.

- Hệ điều hành khách/chủ cho phép mạng tập trung các chức năng và các ứng dụng tại một hay nhiều máy dịch vụ file chuyên dụng. Theo cách này, chúng có thể hoạt động như trường hợp đặc biệt của hệ điều hành dựa trên máy chủ.
- Các máy dịch vụ file trở thành trung tâm của hệ thống, cung cấp sự truy cập tới các tài nguyên và cung cấp sự bảo mật. Các máy trạm riêng lẻ (máy khách) được truy nhập tới các tài nguyên có sẵn trên máy dịch vụ file.

- OS cung cấp cơ chế tích hợp tất cả các bộ phận của mạng và cho phép nhiều người dùng đồng thời chia sẻ cùng một tài nguyên bất kể vị trí vật lý.
- Các hệ điều hành ngang hàng cũng có thể hoạt động như hệ điều hành khách/chủ như vớiUnix/NFS và Windows 95.

Các điểm thuận lợi của một mạng khách/chủ:

- ✓ Cho phép cả điều khiển tập trung và không tập trung: Các tài nguyên và bảo mật dữ liệu có thể được điều khiển qua một máy chủ chuyên dụng hay rải rác trên toàn mạng.
- ✓ Chống quá tải mạng.
- ✓ Cho phép sử dụng các máy, các mạng chạy trên các nền khác nhau.
- ✓ Đảm bảo toàn vẹn dữ liệu.
- ✓ Giảm chi phí phát triển hệ thống.

1.3.4 Các chức năng của một hệ điều hành mạng

Sau đây là các chức năng cụ thể mà một hệ điều hành mạng.

- Cung cấp phương tiện liên lạc giữa các tiến trình, giữa những người sử dụng và giữa các tài nguyên nói chung của toàn mạng. Có thể kể đến các khía cạnh sau:
  - ✓ Chuyển dữ liệu giữa các tiến trình
  - ✓ Đồng bộ hoá các tiến trình
  - ✓ Cung cấp phương tiện liên lạc giữa người sử dụng. Ở mức thấp có thể là tạo, luuchuyển và hiển thị các thông báo nóng trực tuyến, ở mức độ cao có thể là nhắn tin (paging) hoặc thư tín điện tử (Email)
- Hỗ trợ cho các hệ điều hành của máy trạm, cho phép truy nhập tới máy chủ từ các máy trạm. Các hệ điều hành mạng hiện đại đều cung cấp các hỗ trợ cho các hệ điều hành khác nhau chạy trên các máy trạm khách. Sau đây là một số ví dụ minh hoạ vấn đề này:

Các hệ điều hành UNIX cung cấp các chương trình chạy trên DOS có tên là NFS*(Network File System)* khởi động trên DOS để các máy PC có thể sử dụng hệ thống tệp của các máy chủ UNIX.

Một số hệ điều hành như Windows NT và Windows 95 cung cấp hỗ trợ cho các dịch vụ thư mục Novell *(NDS)* cho phép chúng truy nhập trực tiếp tới tài nguyên trên máy chủ Novell Netware.

- Dịch vụ định tuyến và cổng nối: cho phép truyền thông giữa các giao thức mạng khác nhau. Ví dụ một máy chạy trên Novell NetWare với giao thức IPX/SPX không thể chạy trực tiếp các ứng dụng trên TCP/IP như một số ứng dụng Internet. Tuy vậy nếu có các modun chuyển đổi giao thức biến các gói tin IPX/SPX thành gói tin TCP/IP khi cần gửi từ mạng Netware ra ngoài và ngược lại thì một máy chạy Netware có thể giao tiếp được với Internet. Kiến trúc của Netware có ODI *(Open Datalink Interface)* là phần để chuyển đổi, chồng (bao gói) các giao thức khác nhau.
- Dịch vụ danh mục và tên *(Name /Directory Services):*
  - ✓ Để có thể khai thác tốt tài nguyên trên mạng, người sử dụng cần "nhìn thấy" một cách dễ dàng các tên tài nguyên (thiết bị, tệp) của toàn mạng một cách

tổng thể. Vì thế một dịch vụ cung cấp danh mục tài nguyên là vô cùng quan trọng.

- ✓ Đương nhiên việc người sử dụng nhìn thấy các tài nguyên nào còn phụ thuộc vào thẩm quyền của người đó. Mỗi khi vào mạng, khi người sử dụng đã được mạng nhận diện, họ có thể nhìn thấy những tài nguyên được phép sử dụng.
- ✓ Trong NOVELL dịch vụ đó chính là NDS *(Netware Directory Services)*. Trong Windows NT hay Windows95 đó chính là chức năng browser mà ta thấy được cài đặt trong explorer. Trong UNIX với lệnh mount ta có thể kết nối tên tài nguyên của một hệ thống con vào hệ thống tài nguyên chung.

- Bảo mật: Chức năng này đảm bảo việc kiểm soát các quyền truy cập mạng, quyền sử dụng tài nguyên của mạng. Các phương pháp được áp dụng bao gồm:
  - ✓ Dùng các dịch vụ đĩa để điều khiển bảo mật:
  - ✓ Chia ổ đĩa cứng của máy chủ thành các phần được gọi là volume hay partition sau đó gán volume được phép cho người dùng
  - ✓ Định các thẩm quyền trên tập tin và thư mục. Có nhiều loại thẩm quyền. It nhất thì các thẩm quyền được đọc, được ghi và được thực hiện được áp dụng cho đa số các hệ điều hành mạng. Một số hệ điều hành quy định thẩm quyền khá chi tiết như quyền được xoá, quyềnđược sao chép, quyền xem thư mục, quyền tạo thư mục. Các quyền này lại được xem xét cho đến từng nhóm đối tượng như cá nhân, nhóm là việc hay tất cả mọi người.
  - ✓ Thẩm quyền vào mạng hay thực hiện một số dịch vụ được nhận diện qua tên người sử dụng và mật khẩu.
  - ✓ Mã hoá các gói tin trên mạng.
  - ✓ Một số hệ điều hành còn cho phép mã hoá phần cứng để kiểm soát việc sử dụng thiết bị.
- Cung cấp phương tiện chia sẻ tài nguyên. Những tài nguyên trên mạng có thể cho phép nhiều người được sử dụng. Đáng kể nhất là đĩa (thực chất là tệp và thư mục) và máy in (thực chất là máy tính quản lý hàng đợi của máy in). hệ điều hành M phải có các công cụ cho phép tạo ra các tài nguyên có thể chia sẻ được. Các tài nguyên chia sẻ được phải là các tài nguyên độc lập với mọi ứng dụng. Chính vì vậy nó phải được cung cấp các trình điều khiển (driver) phù hợp với mạng. Máy in, modem...là các tài nguyên như vậy.

Trên mạng cũng cần có các công cụ can thiệp vào hoạt động của các tài nguyên mạng Ví dụ: đình chỉ một tiến trình truy nhập mạng từ xa, thay đổi thứ tự hàng đợi trên máy in mạng...

- Tạo tính trong suốt để người sử dụng không nhìn thấy khó khăn trong khi sử dụng các tài nguyên mạng cũng như tài nguyên tại chỗ. Chính dịch vụ thư mục và tên nói trên là một ví dụ về chức năng này. Trong Windows 95/NT người ta có thể duyệt thư mục trên toàn mạng không có gì khác với việc duyệt thư mục trong đĩa cục bộ
- Sao lưu dự phòng: Đối với bất kỳ hệ thống nào, chạy trên môi trường nào, vấn đề sao lưu dự phòng cũng quan trọng để có thể hồi phục thông tin của hệ thống sau một sự cố gây mất dữ liệu. Tuy nhiên trong môi trường mạng thì việc sao lưu có thể

thực hiện được việc sao lưu một cách tự động qua mạng. Chính vì thế các các hệ điều hành mạng đều cung cấp công cụ sao lưu như một chức năng cơ bản.

Trên Novell cho phép soi gương *(mirroring)* các ổ đĩa mà ta có thể đặt trong khi cài đặt hệ thống. Novell có cả một dịch vụ tên là SMS *(Storage Management Services)* cung cấp các công cụ sao chép, hồi phục không chỉ dữ liệu của NSD mà cả dữ liệu của hệ thống ví dụ NDS. NT có chức năng replicate không những đối với đĩa mà còn ở mức thư mục và định kỳ. Điều đó rất cần thiết không chỉ trên mạng cục bộ mà ngay cả trên mạng rộng.

1.4 KẾT NỐI LIÊN MẠNG

1.4.1 Cách tiếp cận

Liên mạng (Internetwork) là một tập hợp của nhiều mạng riêng lẻ được nối kết lại bởi các thiết bị nối mạng trung gian và chúng vận hành như chỉ là một mạng lớn. Để kếtnối các mạng đang tồn tại lại với nhau, người ta thường xuất phát từ một trong hai quan điểm sau:

1) Xem mỗi nút của mạng con như là một hệ thống mở
2) Xem mỗi mạng con như là một hệ thống mở.

Quan điểm 1 cho phép mỗi nút của mạng con có truyền thông trực tiếp với một nút của một mạng con bất kỳ khác. Như vậy toàn bộ các mạng con cũng sẽ là nút một mạng lớn hơn và tuân thủ một kiến trúc chung.

Trong khi đó với quan điểm 2, hai nút thuộc hai mạng con khác nhau thì không thể "bắttay" trực tiếp với nhau được mà phải thông qua một phần tử trung gian, gọi là giao diệnkết nối đặt giữa hai mạng con đó. Có nghĩa là cũng hình thành một mạng lớn hơngồm các giao diện kết nối và các máy tính (host) được nối với nhau bởi các mạng con đó.

Tương ứng với hai quan điểm đó có hai chiến lược kết nối mạng khác nhau. Mộtchiến lược (tương ứng với quan điểm 1) tìm cách xây dựng các chuẩn chung cho các mạng (các chuẩn của ISO, CCITT theo quan điểm này). Một chiến lược khác (tươngứng với quan điểm 2) cố gắng xây dựng các giao diện kết nối để tôn trọng tính độc lập của các các mạng hiện có. Rõ ràng sự hội tụ về một chuẩn chung là một điều lý tưởng, nhưng rõ ràng là không thể ngay tức khắc loại bỏ hàng vạn mạng đang tồn tại trên thế giới được, mà phải tìm cách tận dụng chúng. Trên thị trường hiện nay có rất nhiều các sản phẩmgiao diện cho phép chuyển đổi giữa các mạng khác nhau, đó là một minh chứng sốngđộng cho sức sống của quan điểm 2.

1.4.2 Giao diện nối kết

Mạng nối kết là một mạng gồm có các nút mạng là các giao diện nối kết *(Gateway)* được nối lại với nhau nhờ các đường truyền đặc biệt là các mạng con *(Subnet).*

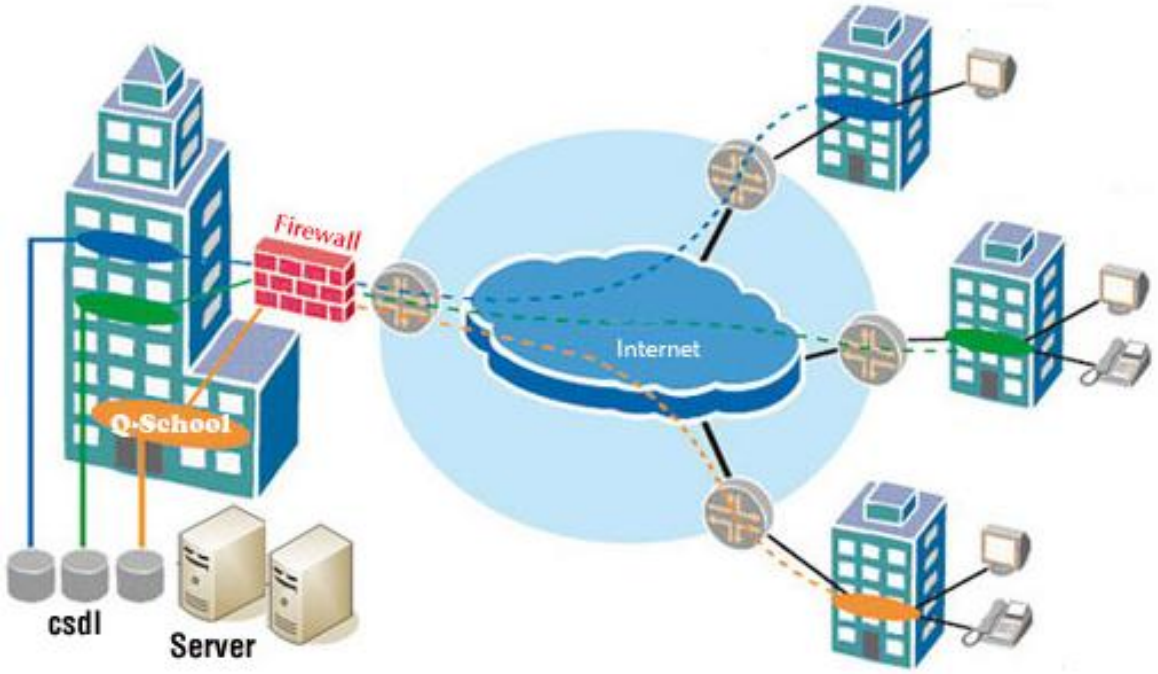
Một giao diện nối kết có thể thực hiện nối "tay đôi", "tay ba", hoặc "nhiều tay" tùy thuộc vào người thiết kế. Ngoài ra, giao diện nối kết có thể là một thiết bị (máy tính) độc lập nhưng cũng có thể được cài đặt ghép vào một nút của một mạng con nào đó.

Tùy thuộc vào chức năng cụ thể mà giao diện nối kết có những tên gọi riêng như là Brige, Router, Gateway.

1.4.3 Một số thuật ngữ thông dụng

INTERNET

Internet là một hệ thống mạng của các mạng máy tính được nối kết với nhau qua hệ thống viễn thông trên phạm vi toàn thế giới nhằm trao đổi thông tin.



Hình 1.10 Hệ thống mạng máy tính

Các chủ thể tham gia hoạt động Internet

- Bậc cơ sở: Người sử dụng internet
- Bậc trung chuyển: Cung cấp dịch vụ internet (Internet Service Provider – ISP)
- Bậc trên cùng: Cung cấp kết nối mạng internet (Internet Access Provide – IAP/IXP)
- Kết nối chuyên dùng:

  Kết nối trực tuyến (online), 24/24

  Dùng đường thuê (leased line)

  Sử dụng ở trường học, viện nghiên cứu,…

  Đáng tin cậy, chi phí cao
- Kết nối tạm thời: Là những kết nối thông qua line điện thoại, rẻ tiền(ADSL)

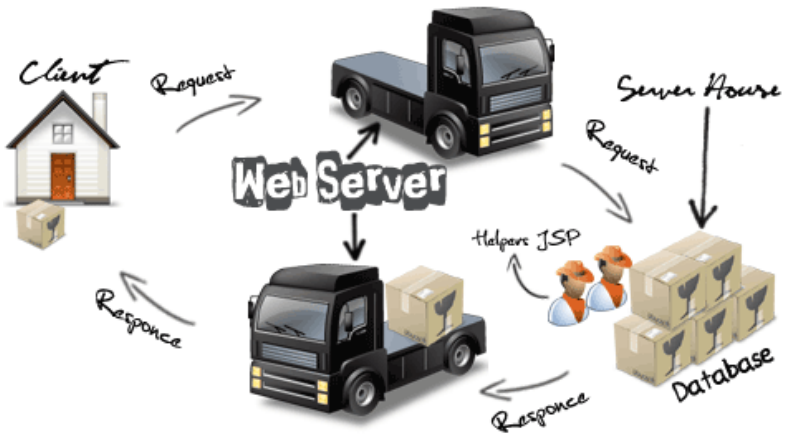
PROTOCOL

Giao thức (Protocol):

- Quy tắc các thành phần liên lạc nhau
- Cần quan tâm:

  Định dạng hay thứ tự của message trao đổi

  Hành động khi nhận message



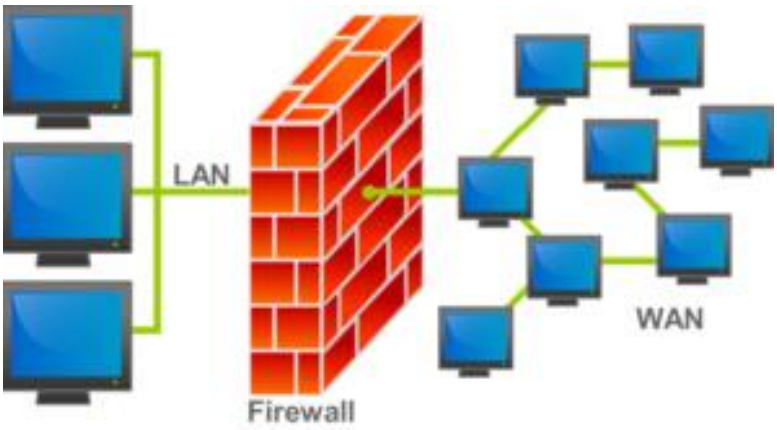
Hình 1.11 Quá trình trao đổi dữ liệu

ISP

Là chữ viết tắt của "Internet Service Provider" (Nhà cung cấp dịch vụ Internet).

TƯỜNG LỬA - FIREWALL

Tường lửa là một thiết bị phần cứng và/hoặc một phần mềm hoạt động trong một môi trường máy tính nối mạng để ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh của cá nhân hay tổ chức, việc này tương tự với hoạt động của các bứctường ngăn lửa trong các tòa nhà. Tường lửa còn được gọi là Thiết bị bảo vệ biên giới (*Border Protection Device - BPD*) hay bộ lọc gói tin (*packet filter*)



Hình 1.12 Kết nối giữa LAN và WAN thông qua tường lửa

TỔNG KẾT CHƯƠNG

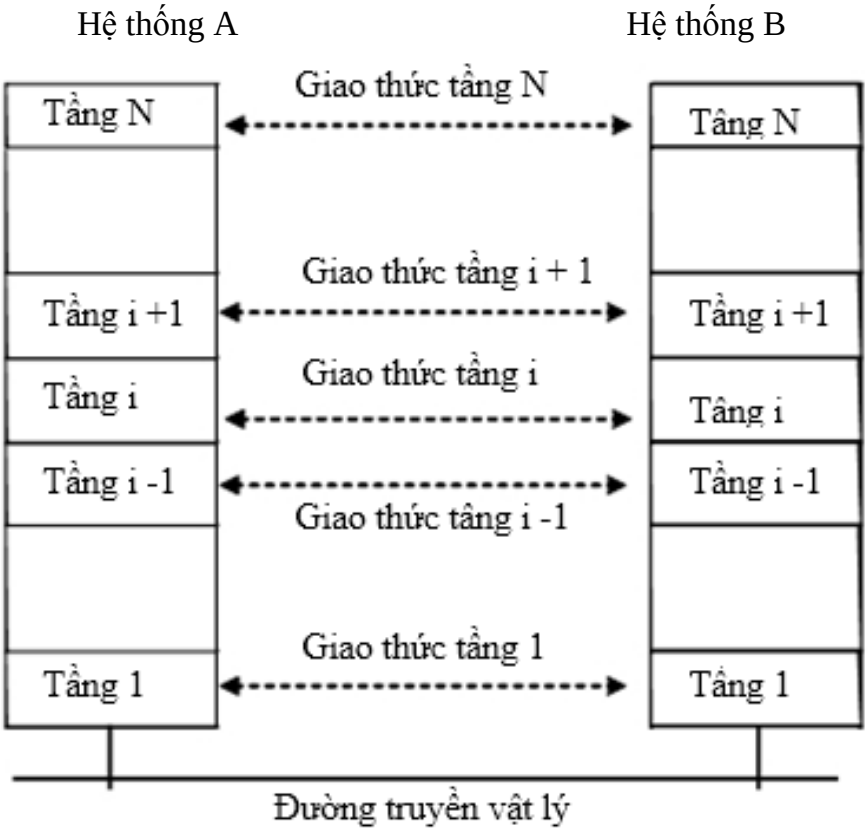
Các điểm quan trọng bạn cần nắm được trong chương này:

1. Mục đích và ứng dụng của mạng máy tính.
2. Định nghĩa mạng máy tính là gì? Kiến trúc và phân loại mạng máy tính?
3. Đặc điểm của hệ điều hành mạng và phân loại.
4. Chức năng của các hệ điều hành mạng.
5. Giao diện kết nối liên mạng và các thuật ngữ thông dụng.

CHƯƠNG 2
KIẾN TRÚC PHÂN TẦNG VÀ MÔ HÌNH OSI

2.1 KIẾN TRÚC PHÂN TẦNG

Để giảm độ phức tạp của việc thiết kế và cài đặt mạng, hầu hết các máy tính đều được phân tích thiết kế theo quan điểm phân tầng. Mỗi hệ thống thành phần của mạng được xem như một cấu trúc đa tầng, trong đó mỗi tầng được xây dựng trên tầng trước nó. Số lượng các tầng cũng như tên và chức năng của mỗi tầng tuỳ thuộc vào nhà thiết kế. Trong hầu hết các mạng, mục đích của mỗi tầng là để cung cấp một số dịch vụ nhất định cho tầng cao hơn. Mỗi tầng khi sử dụng không cần quan tâm đến các thao tác chi tiết mà các dịch vụ đó phải thực hiện.



Hình 2.1 Minh họa kiến trúc phân tầng tổng quát

Nguyên tắc của kiến trúc mạng phân tầng:

- Mỗi hệ thống trong một mạng đều có cấu trúc tầng như nhau (số lượng tầng, chức năng của mỗi tầng).
- Dữ liệu không được truyền trực tiếp từ tầng i của hệ thống này sang tầng thứ i của hệ thống kia (ngoại trừ đối với tầng thấp nhất). Bên gửi dữ liệu cùng với các thông tin điều khiển chuyển đến tầng ngay dưới nó và cứ thế cho đến tầng thấp nhất. Bên dưới tầng này là đường truyền vật lý, ở đấy sự truyền tin mới thực sự diễn ra. Đối với bên nhận thì các thông tin được chuyển từ tầng dưới lên trên cho tới tầng i của hệ thống nhận.

- Giữa hai hệ thống kết nối chỉ ở tầng thấp nhất mới có liên kết vật lý còn ở tầng cao hơn chỉ là liên kết logic hay liên kết ảo được đưa vào để hình thức hóa các hoạt động của mạng, thuận tiện cho việc thiết kế và cài đặt các phần mềm truyền thông.

Các vấn đề cần phải giải quyết khi thiết kế các tầng

- *Cơ chế nối, tách:* mỗi một tầng cần có một cơ chế để thiết lập kết nối và có một cơ chế để kết thúc kết nối khi mà sự kết nối là không cần thiết nữa.
- *Các quy tắc truyền dữ liệu:* Trong các hệ thống khác nhau dữ liệu có thể truyền theo một số cách khác nhau: Truyền một hướng *(simplex), t*ruyền hai hướng đồng thời *(full-duplex), t*ruyền theo cả hai hướng luân phiên *(half-duplex)*
- *Kiểm soát lỗi:* Đường truyền vật lý nói chung là không hoàn hảo, cần phải thoả thuận dùng một loại mã để phát hiện, kiểm tra lỗi và sửa lỗi. Phía nhận phải có khả năng thông báo cho bên gửi biết các gói tin nào đã thu đúng, gói tin nào phát lại.
- *Độ dài bản tin:* Không phải mọi quá trình đều chấp nhận độ dài gói tin là tuỳ ý, cần phải có cơ chế để chia bản tin thành các gói tin đủ nhỏ.
- *Thứ tự các gói tin:* Các kênh truyền có thể giữ không đúng thứ tự các gói tin, do đó cần có cơ chế để bên thu ghép đúng thứ tự ban đầu.
- *Tốc độ phát và thu dữ liệu*: Bên phát có tốc độ cao có thể làm "lụt" bên thu có tốc độ thấp. Cần phải có cơ chế để bên thu báo cho bên phát biết tình trạng đó để điều khiển lưu lượng hợp lý.

2.2 CÁC TỔ CHỨC THỰC HIỆN VIỆC CHUẨN HÓA MẠNG MÁY TÍNH

Một số tổ chức có vai trò quan trọng trong việc chuẩn hóa mạng máy tính:

- ISO *(International Organization For Standardization)*: là tổ chức tiêu chuẩn hóa quốc tế hoạt động dưới sự bảo trợ của Liên hợp quốc. Thành viên của ISO là các cơ quan tiêu chuẩn hóa của các quốc gia.
- CCITT *(Commite Consultatif International pour Telegraphe et Telephone)* là tổ chức tư vấn quốc tế về điện tín và điện thoại cũng hoạt động dưới sự bảo trợ của Liên hợp quốc. Thành viên của CCITT là các cơ quan bưu chính viễn thông của các quốc gia hoặc tư nhân.

Ngoài ra còn có một số cơ quan khác như ECMA (*Eoripean Computer Manuafactures Association* – Tổ chức chế tạo máy tính của Châu Âu), ANSI (*Ameracan National Standards Institute* – Viện tiêu chuẩn quốc gia của Mỹ), IEEE (*Institute of Electrical and Electronics Engineers* – Viện công nghệ điện và điện tử),… Đặc biệt IEEE là tổ chức tiên phong và chủ đạo đối với việc chuẩn hóa mạng cục bộ.

2.3 MỘT SỐ KHÁI NIỆM CƠ BẢN

2.3.1 Tầng (layer)

Mọi quá trình trao đổi thông tin giữa hai đối tượng đều thực hiện qua nhiều bước, các bước này độc lập tương đối với nhau.

Thông tin được trao đổi giữa hai đối tượng A, B qua 3 bước:

- ✓ Phát tin: Thông tin chuyển từ tầng cao => tầng thấp
- ✓ Nhận tin: Thông tin chuyển từ tầng thấp => tầng cao

- ✓ Quá trình trao đổi thông tin trực tiếp qua đường truyền vật lý (thực hiện ở tầng cuối cùng)

2.3.2 Giao diện, dịch vụ, đơn vị dữ liệu

- Mối quan hệ giữa hai tầng kề nhau gọi là giao diện

- Mối quan hệ giữa hai tầng đồng mức của hai hệ thống khác nhau gọi là giao thức

- Thực thể (entity): là thành phần tích cực trong mỗi tầng, nó có thể là một tiến trìnhtrong hệ đa xử lý hay là một trình con các thực thể trong cùng 1 tầng ở các hệ thốngkhác nhau (gọi là thực thể ngang hàng hay thực thể đồng mức). Mỗi thực thể có thể truyền thông lên tầng trên hoặc tầng dưới nó thông qua một giao diện (interface). Giao diện gồm một hoặc nhiều điểm truy nhập dịch vụ (Service Access Point - SAP). Tại các điểm truy nhập dịch vụ tầng trên chỉ có thể sử dụng dịch vụ do tầng dưới cung cấp. Thực thể được chia làm hai loại (thực thể cung cấp dịch vụ và sử dụng dịch vụ)

- ✓ Thực thể cung cấp dịch vụ *(service provide)*: Các thực thể ở tầng N cung cấp dịch vụ cho tầng N +1.
- ✓ Thực thể sử dụng dịch vụ *(service user)*: Các thực thể ở tầng N sử dụng dịch vụ do tầng N - 1 cung cấp.

- Đơn vị dữ liệu sử dụng giao thức *(Protocol Data Unit - PDU)*

- Đơn vị dữ liệu dịch vụ *(Service Data Unit - SDU)*

- Thông tin điều khiển *(Protocol Control Information - PCI)*

Một đơn vị dữ liệu mà 1 thực thể ở tầng N của hệ thống A gửi sang thực thể ở tầng N ở một hệ thống B không bằng đường truyền trực tiếp mà phải truyền xuống dưới để truyền bằng tầng thấp nhất thông qua đường truyền vật lý.

- ✓ Dữ liệu ở tầng N-1 nhận được do tầng N truyền xuống gọi là SDU.
- ✓ Phần thông tin điều khiển của mỗi tầng gọi là PCI.
- ✓ Ở tầng N-1 phần thông tin điều khiển PCI thêm vào đầu của SDU tạo thành PDU. Nếu SDU quá dài thì cắt nhỏ thành nhiều đoạn, mỗi đoạn bổ sung phần PCI, tạo thành nhiều PDU.

Bên hệ thống nhận trình tự diễn ra theo chiều ngược lại. Qua mỗi tầng PCI tương ứng sẽ được phân tích và cắt bỏ khỏi PDU trước khi gửi lên tầng trên.

2.4 THUẬT NGỮ OSI

Thực thể (entity): là một phần tử hoạt động trong một tầng của hệ thống. Mỗi tầng có một hoặc nhiều thực thể. Thực thể của tầng N cài đặt các chức năng của tầng N và giao thức truyền thông với các thực thể tầng N trên các hệ thống khác.

Thực thể có thể là một thực thể phần mềm như một tiến trình (process) hay một thực thể phần cứng như một chíp I/O thông minh...

Người cung cấp dịch vụ: Người sử dụng dịch vụ (Service Provider – Service User) Các thực thể ở tầng N cài đặt một dịch vụ được dùng bởi tầng N+1. Tầng N được gọi là nguoi2 cung cấp dịch vụ và tầng N+1 được gọi là người sử dụng dịch vụ. Tầng N có thể dùng các dịch vụ tầng N-1 để cung cấp dịch vụ của nó.

Điểm truy nhập dịch vụ (SAP: Service Access Point): Mỗi thực thể truyền thông với các thực thể tầng trên và dưới nó qua các giao diện (Interface). Mỗi giao diện có

nhiều điểm truy nhập dịch vụ, mỗi điểm truy nhập có một địa chỉ đơn nhất. Điểm truy nhập của tầng N là nơi tầng N+1 có thể truy nhập dịch vụ được cung cấp bởi tầng N.

Đơn vị dữ liệu giao thức (PDU: Protocol Data Unit)

Khi truyền thông, thực thể của lớp N có thể phân mảnh dữ liệu cần truyền ra làm nhiều phần, mỗi phần được thêm vào một thông tin điều khiển, được gọi là tiêu đề (Header) để tạo thành một PDU của tầng N. Ví dụ gói tin là một PDU của tầng mạng.

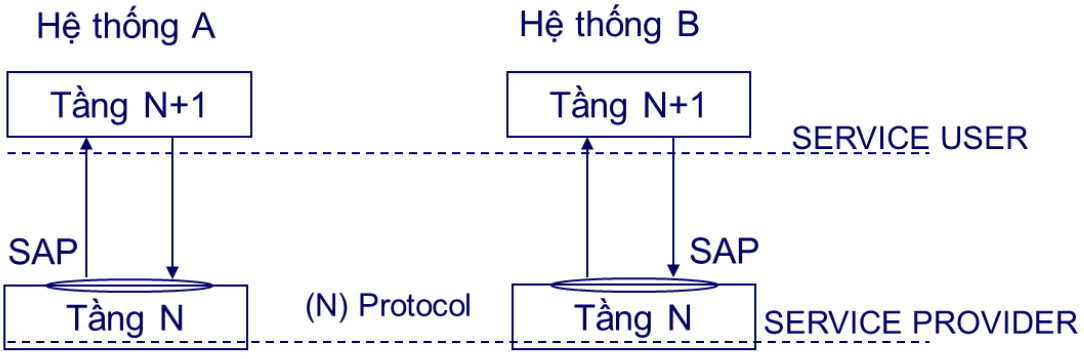
Các dịch vụ thường được xác định bằng tập hợp một số hàm nguyên thủy (primitive) dùng cho phép một người dịch vụ có thể gọi chúng để truy nhập dịch vụ.

Trong mô hình OSI, các hàm nguyên thủy được chia làm 4 nhóm:

Request (Yêu cầu)	Là hàm nguyên thủy mà người sử dụng dịch vụ dùng để gọi một chức năng.
Indication (Chỉ báo)	Là hàm nguyên thủy mà người cung cấp dịch vụ dùng để gọi một chức năng hoặc chỉ báo một chức năng đã được gọi tại SAP.
Response (Trả lời)	Là hàm nguyên thủy mà người sử dụng dịch vụ dùng để hoàn tất một chức năng đã được gọi từ trước bởi một hàm nguyên thủy chỉ báo ở SAP đó.
Confirm (Xác nhận)	Là hàm nguyên thủy mà người cung cấp dịch vụ dùng để thông tin về một yêu cầu mà người sử dụng dịch vụ đã gọi trước đó.

Trong sơ đồ bên dưới là qui trình thực hiện một giao thức giữa hai hệ thống A và B:

- Tầng (N+1) của A gửi xuống tầng (N) kề dưới nó một hàm Request.
- Tầng (N) của A cấu tạo một đơn vị dữ liệu để gửi yêu cầu đó sang tầng (N) của B theo giao thức tầng N đã xác định.
- Nhận được yêu cầu, tầng (N) của B chỉ báo lên tầng (N+1) kề trên nó bằng hàm Indication



Hình 2.2 Sơ đồ nguyên lý hoạt động của các hàm nguyên thủy

- Tầng (N+1) của B trả lời bằng hàm Response gửi xuống tầng (N) kề dưới nó.
- Tầng (N) của B cấu tạo một đơn vị dữ liệu để gửi trả lời đó trở về tầng (N) của A theo giao thức tầng N đã xác định.
- Nhận được trả lời, tầng (N) của A xác nhận với tầng (N+1) kề trên nó bằng hàm Confirm, kết thúc một giao tác giữa 2 hệ thống.

Dãy các sự kiện trên gọi là kiểu hội thoại có xác nhận (confirmed dialogue) do người sử dụng dịch vụ sẽ được xác nhận (từ người cung cấp dịch vụ) rằng yêu cầu đã được chấp nhận.

Lưu ý: Các hàm nguyên thủy đều được gọi đến (hoặc gửi đi) từ một điểm truy nhập dịch vụ (SAP).

Trong thực tế loại dịch vụ connect luôn luôn là có xác nhận, còn các loại dịch vụ DATA là không xác nhận hoặc có xác nhận

STT	Hàm nguyên thủy	Ý nghĩa
1	CONNECT.Request	Yêu cầu thiết lập liên kết
2	CONNECT.Indication	Báo cho thực thể bị gọi
3	CONNECT.Response	Đồng ý hay không đồng ý
4	CONNECT.Confirm	Xác nhận với bên gọi việc kết nối có được chấp nhận hay không
5	DATA.Request	Bên gọi yêu cầu truyền dữ liệu
6	DATA.Indication	Báo cho bên nhân biết là dữ liệu sẽ đến
7	DISCONNECT.Request	Yêu cầu hủy bỏ liên kết
8	DISCONNECT.Indication	Báo cho bên nhận

Ví dụ:

1. CONNECT.Request	A quay số điện thoại của B
2. CONNECT.Indication	Chuông reo
3. CONNECT.Response	B nhấc máy
4. CONNECT.Confirm	Chuông ngừng reo
5. DATA.Request	A nói chuyện với B
6. DATA.Indication	B nghe thấy A nói
7. DATA.Response	B trả lời A
8. DATA.Confirm	A nghe thấy B trả lời
9. DISCONNECT.Request	A cúp máy
10. DISCONNECT.Indication	B nghe thấy A cúp máy

2.5 PHƯƠNG THỨC HOẠT ĐỘNG

Ở mỗi tầng trong mô hình OSI có hai loại dịch vụ: dịch vụ định hướng liên kết *(connection - oriented service)* và dịch vụ không định hướng liên kết *(connectionless service).*

- *Dịch vụ định hướng liên kết:* là dịch vụ theo mô hình điện thoại, trước khi truyền dữ liệu cần thiết lập một liên kết logic giữa các thực thể đồng mức.
- *Dịch vụ không liên kết:* không cần phải thiết lập liên kết logic và một đơn vị dữ liệu được truyền là độc lập với các đơn vị dữ liệu trước hoặc sau nó. Loại dịch vụ

này theo mô hình bưu điện: mỗi bản tin hay mỗi bức thư cần có một địa chỉ cụ thể bên nhận.

Trong phương pháp liên kết quá trình truyền thông gồm có 3 giai đoạn:

- *Thiết lập liên kết (logic):* hai thực thể đồng mức ở hai hệ thống sẽ thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn truyền sau (thể hiện bằng hàm CONNECT).
- *Truyền dữ liệu:* dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu,...) để tăng độ tin cậy và hiệu quả của việc truyền dữ liệu (hàm DATA).
- *Huỷ bỏ liên kết (logic):* giải phóng các tài nguyên hệ thống đã được cấp phát cho liên kết để dùng cho các liên kết khác (hàm DISCONNECT).

Trong mỗi loại dịch vụ được đặc trưng bằng chất lượng dịch vụ. Có dịch vụ đòi hỏi bên nhận tin gửi thông báo xác nhận khi đó độ tin cậy được bảo đảm.

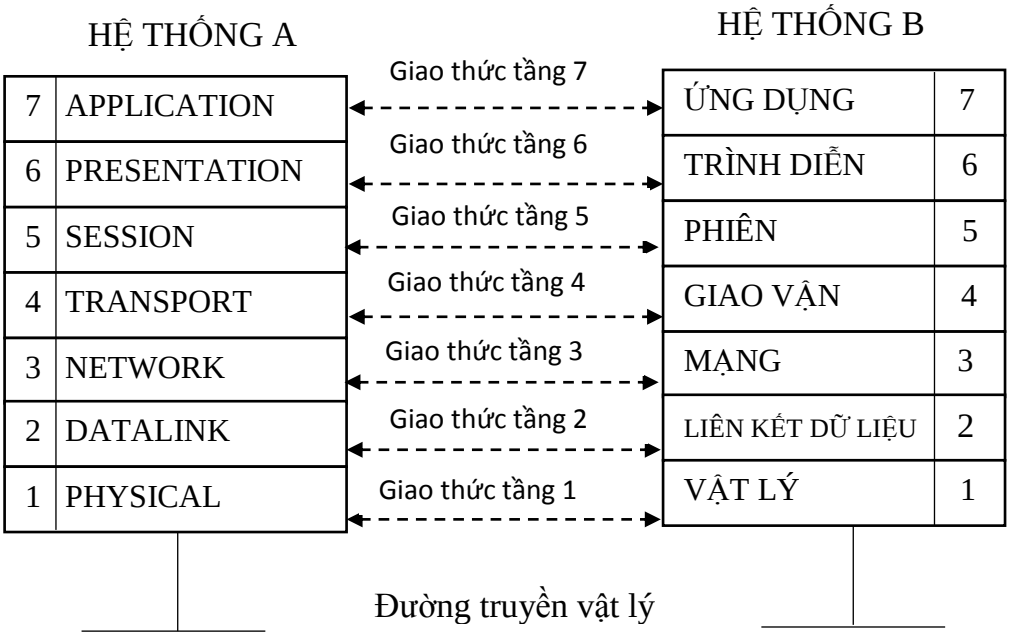
Có những ứng dụng không chấp nhận sự chậm trễ do phải xác nhận sự truyền tin (VD hệ thống truyền tin). Nhưng có nhiều ứng dụng như thư tín điện tử người gửi chỉ cần có một dịch vụ với độ tin cậy cao, chấp nhận sự chậm trễ.

2.6 MÔ HÌNH OSI

2.6.1 Giới thiệu

Khi thiết kế các nhà thiết kế tự do lựa chọn kiến trúc mạng riêng của mình. Từ đó dẫn đến tình trạng không tương thích giữa các mạng: phương pháp truy nhập đường truyền khác nhau, sử dụng họ giao thức khác nhau,... Sự không tương thích đó làm cho người sử dụng các mạng khác nhau không thể trao đổi thông tin với nhau được. Sự thúc bách của khách hàng khiến cho các nhà sản xuất và những nhà nghiên cứu, thông qua tổ chức chuẩn hoá quốc tế và quốc gia để tìm ra một giải pháp chung dẫn đến sự hội tụ của các sản phẩm mạng. Trên cơ sở đó những nhà thiết kế và các nghiên cứu lấy đó làm khung chuẩn cho sản phẩm của mình.

Vì lý do đó, năm1977, Tổchức tiêu chuẩn hoá quốc tế *(International Organization for Standardization - ISO)* đã lập ra một tiểu ban nhằm đưa ra một khung chuẩn như thế. Kết quả là vào năm 1984 ISO đã xây dựng mô hình 7 tầng gọi là mô hình tham chiếu cho việc nối kết các hệ thống mở *(Reference Model for Open Systems Interconnection - OSI Reference Model)* gọi tắt là mô hình OSI. Mô hình này được dùng làm cơ sở để nối kết các hệ thống mở phục vụ cho các ứng dụng phân tán. Mọi hệ thống tuân theo mô hình tham chiếu OSI đều có thể truyền thông tin với nhau.



Hình 2.2 Mô hình OSI 7 tầng

2.6.2 Vai trò, chức năng và đặc điểm của các tầng trong mô hình OSI

2.6.2.1 Tầng vật lý (physical)

a) Vai trò và chức năng của tầng vật lý

Theo định nghĩa của ISO, tầng vật lý cung cấp phương tiện truyền tin (điện, cơ), chức năng, thủ tục để kích hoạt, duy trì và hủy bỏ các liên kết vật lý giữa các hệ thống.

Trong đó, thuộc tính điện liên quan đến sự biểu diễn các bít (các mức tín hiệu) và tốc độ truyền các bit, thuộc tính cơ liên quan đến các tính chất vật lý của giao diện vật lý với một đường truyền (kích thước, cấu hình). Thuộc tính chức năng chỉ ra các chức năng được thực hiện bởi các phần tử của giao diện vật lý một hệ thống và đường truyền vật lý và thuộc tính thủ tục liên quan đến các giao thức điều khiển việc truyền các xâu bit qua đường vật lý.

Nhiệm vụ của tầng vật lý là chuyển các bit từ máy này đến máy kia. Tốc độ truyền tin phụ thuộc vào môi trường truyền tin. Tín hiệu truyền có thể ở dạng tương tự (analog) hoặc dạng số *(digital).* Hướng phát triển hiện nay:

- Truyền tin bằng cáp quang, bằng vệ tinh
- Hệ thống nối nhanh *(Fast – Connect)*, hệ thống chuyển mạch gói
- Mạng thông tin số đa dịch vụ *(Intergrated Services Digital Network)*

b) Môi trường truyền tin

- ***Phương tiện truyền***

Mục đích lắp đặt cáp là bảo đảm dung lượng (tốc độ) cần thiết cho các nhu cầu truyền thông trong mạng, hệ thống cáp cần phải ổn định. Để đạt được mục tiêu này, người quản trị mạng cần phải cân đối 4 yếu tố sau:

- Tốc độ truyền lớn nhất của hệ thống cáp hiện hành, khả năng nâng cấp.
- Nhu cầu về tốc độ truyền thông trong vòng 5 – 10 năm tới là bao nhiêu.

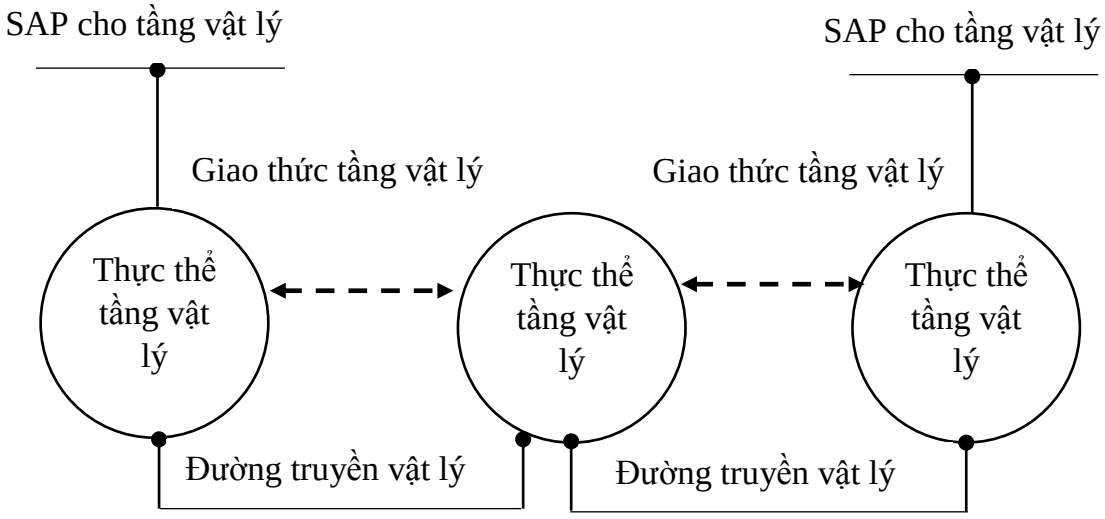
- Chọn trong số những loại cáp đang có trên thị trường.
- Chi phí để lắp đặt thêm cáp dự phòng.

Việc kết nối vật lý một máy tính vào mạng được thực hiện bằng cách cắm một card giao tiếp NIC *(Network Interface Card)* vào khe cắm máy tính và nối với cáp mạng. Sau khi kết nối đã hoàn tất, quản lý việc truyền tin giữa các trạm trên mạng tùy thuộc vào phần mềm mạng.

NIC sẽ chuyển gói tín hiệu vào mạng LAN, gói tín hiệu được truyền đi như một dòng các bit dữ liệu thể hiện bằng các biến thiên tín hiệu điện. Có hai kỹ thuật truyền tín hiệu đã được mã hóa lên mạng: Truyền ở dải tần gốc *(baseband)* và truyền ở dải tầng rộng *(broadband)*.

Khác với các tầng khác, tầng vật lý là không có gói tin riêng và do vậy không có phần đầu (header) chứa thông tin điều khiển, dữ liệu được truyền đi theo dòng bit.

a) Môi trường thực



b) Môi trường Logic

Hình 2.3 Quan hệ của tầng vật lý với môi trường thực

Trong hình 2.3 a): A và B là hai hệ thống mở được nối với nhau bằng một đoạn cáp đồng trục và một đoạn cáp quang. Modem C để chuyển đổi tín hiệu từ tín hiệu số sang tín hiệu tương tự để truyền trên cáp đồng, và modem D lại chuyển đổi tín hiệu từ tín hiệu tương tự sang tín hiệu số. Transducer E chuyển đổi từ xung điện thành xung ánh sáng để truyền qua các quang. Cuối cùng Transducer F chuyển đổi thành xung điện để đi vào B.

Hình 2.3 b) là môi trường logic của tầng vật lý. Ở đây, một thực thể vật lý là một cấu trúc logic giao diện với đường truyền vật lý. Các thực thể đó có mặt trong các hệthống A, B và cũng có thể có thực thể vật lý ở giao diện giữa D và E. Thực thể trung

gian này là một bộ chuyển tiếp hoạt đọng ở tầng vật lý giao diện với các đường truyền vậy lý khác nhau.

Một giao thức tầng vật lý giữa các thực thể vật lý để quy định phương thức truyền (đồng bộ, dị bộ) và tốc độ truyền,.. Điều mong muốn là giao thức đó phải độc lập tối đa với đường truyền vật lý để cho một hệ thống có thể giao diện với nhiều đường truyền khác nhau. Do vậy, các chuẩn vật lý sẽ phải bao gồm không chỉ các thực thể mà còn cả đặc tả của giao diện với đường truyền.

- ***Các thông số cơ bản của môi trường truyền tin***

Độ suy giảm:

Tín hiệu trên đường dây bị suy giảm trong quá trình truyền tin. Để khắc phục ta dùng các bộ khuyếch đại. Độ suy giảm được tính bằng đơn vị decibel. Nếu điện thế ban đầu là V_i và sau đó giảm xuống V_2 thì số decibel của bộ suy giảm được định nghĩa như sau:

$$S(decibel) = 20\ log_{10}\frac{V_1}{V_2}$$

Độ nhiễu:

Điện từ trường trong môi trường truyền tin gây nhiễu cho các tín hiệu mang thông tin. Để khắc phục ta dùng các bộ lọc nhiễu (filters). Để đặc trưng độ nhiễu trên đường dây, ta dùng tỉ số tần số tín hiệu/tạp âm (Signal/Noise – S/N):

$$SN(decibel) = 10\ log_{10}\frac{S}{N}\ (S: Signall\ N: Noise)$$

Tốc độ truyền:

$$C = B\ log_2\left(1 + \frac{S}{N}\right) bit/s$$

Trong đó B là độ rộng dản tần tính bằng Hz. C là tốc độ tính bằng bit/giây (b/s). Nếu mạng điện thoại có dải tần 3000Hz, tỉ số S/N = 20 db thì đốc độ truyền cực đại là:

$$\frac{S}{N} = 10\ log_{10}\frac{S}{N} = 20 \rightarrow \frac{S}{N} = 100$$

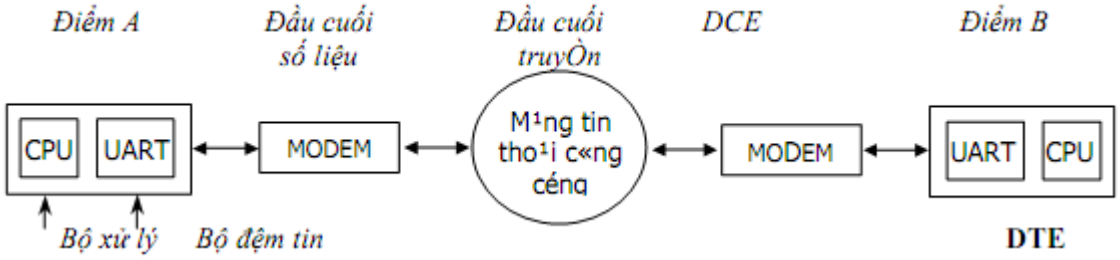
$$C = B\ log_2\left(1 + \frac{S}{N}\right) = 3000\ x\ log2\ (1 + 100) = 19963\ b/s$$

Các tín hiệu trên kênh truyền có thể là tín hiệu tương tự hay tín hiệu số và tương tự sẽ tạo thành kênh tương tự hoặc kênh số.

c) Các chuẩn cho giao diện vật lý

- ***Modem:***

Modem là bộ điều chế và giải điều chế biến đổi các tín hiệu số thành các tín hiệu tương tự và ngược lại trên mạng điện thoại.



Hình 2.4 Sơ đồ truyền tin giữa hai điểm A và B

Tín hiệu số từ máy tính đến modem và được modem biến đổi thành tín hiệu tương tự để có thể đi qua mạng điện thoại. Tín hiệu này đến modem ở điểm B được biến đổi ngược lại thành tín hiệu số đưa vào máy tính ở điểm B.

Các kỹ thuật điều chế cơ bản là điều chế biên độ AM, điều chế tần số FM, điều chế pha PM.

Các phương thức truyền dữ liệu giữa hai điểm có thể là: Một chiều đơn (simplex), hai chiều luân phiên (half – dumplex), hai chiều đầy đủ (duplex).

- ***DTE và DCE:***

Trước khi vào phần này chúng ta làm quen với hai thuật ngữ mới đó là DTE, DCE.

DTE *(đầu cuối số liệu – Data Terminal Equipment)* là một thuật ngữ chung để chỉ các máy của người sử dụng cuối (end-user), có thể là máy tính hoặc một trạm cuối (terrminal). Tất cả các ứng dụng của người dùng đều nằm ở DTE. Mục đích của việc nối mạng chính là để nối các DTE lại với nhau để chia sẻ tài nguyên, lưu trữ thông tin chung và trao đổi dữ liệu.

DCE *(đầu cuối truyền – Data Communication Qquipment)* là thuật ngữ chung chỉ các thiết bị làm nhiệm vụ kết nối các DTE với đường truyền. DCE có thể được cài đặt ngay bên trong DTE hoặc đứng riêng như một thiết bị độc lập. Chức năng chủ yếu của nó là chuyển đổi tín hiệu biểu diễn dữ liệu của người dùng thành tín hiệu chấp nhận được bởi đường truyền và ngược lại.DCE có thể là Modem, Transducer, Multiplexing...

Trong hình 2.4 ở trên, các hệ thống mở A, B chính là các DTE, còn các Modem C, D và Tranducer E, F đóng vai trò là các DCE.

Đa số các trường hợp kết nối mạng máy tính sử dụng cùng một kiểu giao diện vật lý để thuận tiện cho việc truyền thông trực tiếp giữa các sản phẩm khác loại, khỏi phải thực hiện việc chuyển đổi rắc rối. Các đặc tả về hoạt động của các DTE và DCE được đưa ra bởi nhiều tổ chức chuẩn hóa như CCITT, EIA và IEEE. ISO cũng đã công bố các đặc tả về các đầu nối cơ học kết nối giữa các DCE và DTE.

Việc truyền dữ liệu chủ yếu được thực hiện thông qua mạng điện thoại, bởi thế các tổ chức trên đã đưa ra nhiều khuyến nghị về vấn đề này. Các khuyến nghị loại V và loại X của CCITT là một ví dụ điển hình. Chúng là các đặc tả ở tầng vật lý được sử dụng phổ biến nhất trên thế giới, đặc biệt là ở Tây Âu. Bên cạnh đó các chuẩn thuộc họ RS- (nay đã đổi thành EIA-) của EIA cũng đã được sử dụng rất phổ biến, đặc biệt là ở Bắc Mỹ. Dưới đây ta sẽ xem xét một số chuẩn thông dụng nhất.

- ***Chuẩn RS-232C:***

Đầu những năm 50, chuẩn RS0232 *(Recommended Standard 232C của EIA)* được phát triển để truyền tin giữa các thiết bị đầu cuối dữ liệu. Chuẩn này hiện nay đang được sử dụng, nó chính là các cổng COM1, COM2 trên các máy PC.

+ Phần cơ học: là một bộ có 25 chân, độ rộng tính ở giữa là 47,05mm ± 13, hàng trên đánh số 1 ÷ 13 (trái qua phải) hàng dưới là 14 ÷ 25 (trái qua phải).

+ Phần điện: gồm qui ước logic 1< -3V và logic 0 > +3V.

Tốc độ truyền cho phép 20 kbps qua dây cáp 15m (thường là 9,6 kbps).

Từ năm 1987, RS-232-C đã được sửa đổi và đặt tên lại là EIA-232-D. Ngoài ra còn có một số chuẩn mở rộng khác như RS-422-A, RS-423-A, RS-449, các khuyến

nghị loại X của CCITT như X21,.. Mặc dù RS-232-C vẫn là chuẩn thông dụng nhất cho giao diện DTE/DCE nhưng các chuẩn mới này được áp dụng phổ biến hiện nay.

Đối với các máy tính, thông thường người ta sử dụng hai cổng COM1, COM2 để kết nối trực tiếp. Cổng COM1 có địa chỉ vào/ra là 3F8_3FF hex và ngắt là IRQ4, cổng COM2 có địa chỉ vào/ra là 2F8_2FF hex và ngắt là IRQ3. Các chân cắm của hai cổng cũng được chuẩn hóa để tiện lợi hơn cho việc sử dụng.

2.6.2.2 Tầng liên kết dữ liệu (Data Link)

a) Vai trò và chức năng của tầng liên kết dữ liệu

Tầng liên kết dữ liệu cung cấp các phương tiện để truyền thông tin qua liên kết vật lý đảm bảo tin cậy thông qua các cơ chế đồng bộ hóa, kiểm soát lỗi và kiểm soát luồng dữ liệu.

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

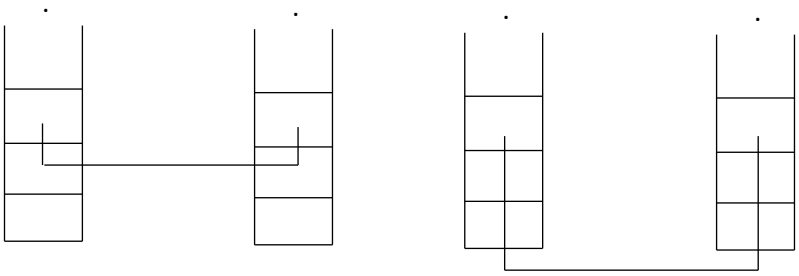
Tầng liên kết dữ liệu cũng cung cấp cách phát hiện và sửa lỗi cơ bản để đảm bảo cho dữ liệu nhận được giống hoàn toàn với dữ liệu gửi đi. Nếu một gói tin có lỗi không sửa được, tầng liên kết dữ liệu phải chỉ ra được cách thông báo cho nơi gửi biết gói tin đó có lỗi để nó gửi lại.

Thông thường, tầng LKDL có liên quan đến nhiễu của tín hiệu của các phương tiệntruyền vật lý, cho dù là truyền qua dây đồng, cáp quang hay truyền thông qua sóng ngắn. Nhiễu là một vấn đề rất thông thường và có thể do rất nhiều nguồn khác nhau, trong đó có cả nhiễu của các tia vũ trụ, nhiễu do tạp âm của khí quyển và từ các nguồn khác nhau.

b) Các vấn đề của tầng liên kết dữ liệu:

- ***Cung cấp dịch vụ cho tầng mạng***

Tầng 2 chuyển dữ liệu từ mức 3 ở máy nguồn tới mức 3 ở máy nhận.



Đường số liệu ảo (Virtual Communication) *Đường số liệu thực (Actual Communication)*

Hình 2.5 Đường truyền dữ liệu trong tầng LKDL

Các dịch vụ tầng 2 có thể là:

- Dịch vụ không nối kết, không báo nhận *(Unacknowledged Connectionless Service)*
- Dịch vụ không nối kết, có báo nhận *(Acknowledged Connectionless Service)*

- Dịch vụ có nối kết *(Connection Oriented Service)*

Dịch vụ kết nối có hướng có 3 giai đoạn: kết nối, truyền số liệu, tách bỏ liên kết (kết thúc): CONNECT, DATA, DISCONNECT. Truyền tin giữa 2 tầng kề nhau dùng các hàm dịch vụ nguyên thủy (Request, Indication, Response và Confirm).

Dịch vụ không kết nối được thực hiện bằng 1 bước duy nhất là truyền tin, không cần thiết lập liên kết logic. Các đơn vị truyền dữ liệu độc lập nhau.

- ***Khung tin – nhận biết gói tin:***

Để cung cấp dịch vụ cho tầng mạng, tầng LKDL phải dùng dịch vụ được cung cấp từ tầng vật lý. Tầng vật lý tiếp nhận dòng bit và giao cho nơi nhận. Dòng bit này có thể có lỗi. Tầng LKDL sẽ kiểm tra và nếu cần sẽ sửa lỗi.

Tầng LKDL tách dòng bít thành các khung tin (frame) và tính thông số kiểm tra tổng (checksum) cho mỗi khung tin cậy, nếu kết quả khác với checksum chứa trong khung tin, nghĩa là có lỗi và khi đó lỗi sẽ được thông báo cho nơi gửi.

Muốn tách các khung tin, có thể chèn các đoạn phân cách vào giữa các khung tin, giống như khoảng trống giữa các từ trong văn bản. Nhưng điều này khó thực hiện nên người ta thường dùng các phương pháp sau:

- Đếm số ký tự: Hiện nay ít được dùng, vì từ đếm cũng bị lỗi khi truyền.
- Dùng ký tự bắt đầu (STX) và kết thúc (ETX) với ký tự đệm (DLE).
- Dùng các cờ (flags) đánh dấu bắt đầu và kết thúc với các bít đệm.

- ***Kiểm tra lỗi:***

Các cách để kiểm tra lỗi trong quá trình truyền:

- Dùng thông số trả lời có biên nhận (ACK) hoặc không biên nhận (NAK) để biết đã nhận đúng bản tin hay phải phát lại.
- Dùng bộ định thời gian, nếu quá thời gian quy định không có trả lời nghĩa là bản tin chưa nhận được.
- Dùng phương pháp đánh số thứ tự các khung tin (frame) được gửi đi.

Quá trình kiểm tra lỗi đồng thời với quản lý thời gian và số thứ tự của các khung tin nhằm bảo đảm mỗi khung tin chỉ nhận được một lần duy nhất. Đây là chức năng quan trọng của tầng LKDL.

- ***Điều khiển luồng dữ liệu:***

Trong quá trình truyền dữ liệu, nếu tốc độ bên phát nhanh hơn bên thu thì xảy ra hiện tượng mất tin do không nhận kịp. Vì vậy cần phải điều khiển luồng truyền (flow control) để quá trình thu phát được phối hợp nhịp nhàng và đồng bộ với nhau.

Các giao thức phải chứa các quy tắc xác định rõ khi nào gởi có thể phát các khung tin kế tiếp.

- ***Quản lý liên kết:***

Một chức năng khác của tầng LKDL là quản lý các kết nối như tách, nối, đánh số khung tin, bắt đầu lại khi lỗi, quản lý các thiết bị đầu cuối thứ cấp hoặc sơ cấp bằng khung tin thăm dò (poll).

- ***Nén dữ liệu khi truyền:***

Nén dữ liệu là một vấn đề quan trọng trong việc truyền dữ liệu. Về cơ bản, nén dữ liệu là ép chúng lại để đỡ tốn chỗ khi lưu trữ trên đĩa và đỡ tốn thời gian khi truyền trên đường truyền. Thực tế, các dữ liệu số chứa nhiều đoạn lặp đi lặp lại, nén dữ liệu sẽ thay thế các thông tin lặp lại bằng một ký hiệu hoặc một đoạn mã để rút ngắn độ dài của tập tin. Các kỹ thuật nén dữ liệu gồm:

- *Null compression:* Thay thế một dãy các dấu cách bằng một mã nén và một giá trị số lượng các dấu cách.
- *Run-length compression:* Mở rộng kỹ thuật trên bằng cách nén bất kỳ một dãy nào có từ 4 ký tự lặp. Các ký tự này được thay thế bằng một mã nén, là một trong các ký tự này và một giá trị bằng đúng số lần lặp.
- *Keyword encoding:* Tạo ra một bảng mã cho các từ hoặc các cặp ký tự thường xuyên xuất hiện và thay thế.
- *Phương pháp thống kê Huffman:* Kỹ thuật nén này giả thiết rằng sự phân bố các ký tự trong dữ liệu là không đồng nhất. Tức là có một số ký tự xuất hiện nhiều hơn các ký tự khác. Ký tự nào càng xuất hiện nhiều thì càng ít tốn bít để mã hóa nó. Một bảng được tạo ra để ghi lại lược đồ mã hóa và bảng này có thể chuyển cho Modem nhận để nó biến đổi trở lại các ký tự đã mã hóa.

Ngoài ra còn một thuật toán nén nữa được gọi là nén ngẫu nhiên. Thuật toán này được sử dụng trong một chuẩn nén dữ liệu V.24bits.

c) Phát hiện và hiệu chỉnh lỗi

Trong khi truyền đi một byte trong hệ thống máy tính thì khả năng xảy ra một lỗi do hỏng hóc ở phần nào đó hoặc do nhiễu gây nên là khá lớn. Các kênh vào ra thường xảy ra nhiều lỗi, đặc biệt là khi truyền số liệu. Quá trình sửa lỗi thường khó hơn rất nhiều so với phát hiện lỗi. Có thể chia phương pháp xử lý lỗi ra làm hai nhóm:

- Phát hiện và thông báo cho bên phát biết để phát lại tin.
- Phát hiện lỗi và tự sửa.

Một số phương pháp xử lý lỗi:

- Phương pháp bit chẵn lẻ *(Parity)*
- Tính theo đa thức chuẩn
- Mã sửa sai

d) Thủ tục liên kết dữ liệu cơ bản

Để truyền tin có độ tin cậy cao ta dùng dịch vụ liên kết *(Connection Oriented Services)*

Ví dụ: Máy A gửi số liệu cho máy B, khi tầng 2 đã được kết nối, số liệu từ tầng 3 máy A chuyển xuống tầng 2 nhờ chương trình con "*FromNetworkLayer*". Tầng 2 bổ sung phần đầu thông tin điều khiển và tính cờ kiểm tra tổng (FCS).

Khung tin (Frame)	Đầu tin (Header)	Thông tin (Information)	FCS

Khung tin được phát sang tầng 2 máy B nhờ chương trình con ToPhysicalLayer.

Máy B đợi tin bằng chương trình con Procedure CallWait (Event). Khi khung tin tới bên nhận, máy B tính cờ kiểm tra tổng, nếu không đúng cờ sẽ báo event =

CksumErr, nếu khung tin đúng nó báo even = FrameArrival và thu nhận khung tin từ tầng vật lý nhờ chương trình con FromPhysicalLayer.

Sau đó đầu tin chứa các thông tin điều khiển (Header) sẽ được kiểm tra và nếu tất cả đều đúng cả, phần số liệu được chuyển lên tầng 3 nhờ chương trình con ToNetworkLayer.

- Giao thức đơn công với kênh không lỗi và không chờ: Trong giao thức này do tin chỉ truyền theo một hướng, đường kênh không có lỗi nên số liệu luôn sẵn sàng không phải chờ.
- Giao thức đơn công với kênh không lỗi và phải chờ: Bên thu bộ nhớ hạn chế và?? tốc độ vật lý hữu hạn, do đó bên phát phải chờ.

e) Các giao thức của tầng liên kết dữ liệu

Cũng giống như tầng vật lý, có rất nhiều giao thức được xây dựng cho tầng này, gọi chung là các giao thức liên kết dữ liệu (Data Link Protcol- DLP). Các DLP được phân chia thành hai loại: đồng bộ và dị bộ. Trong đó, loại đồng bộ lại được chia thành 2 nhóm là hướng ký tự và hướng bit.

- Giao thức dị bộ (*asynchronous DLP*):

Các DLP dị bộ sử dụng phương thức truyền dị bộ, tức là không cần có sự đồng bộ liên tục giữa người gửi và người nhận, nó cho phép một đơn vị dữ liệu được truyền đi bất kỳ lúc nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó. Ở giao thức loại này, các bít đặc biệt START và STOP được dùng để tách các xâu bit biểu diễn các ký tự trong dòng dữ liệu được truyền đi. Các giao thức loại này thường được dùng trong các máy điện báo hoặc các máy tính trạm cuối tốc độ thấp. Phần lớn các máy PC sử dụng phương thức truyền dị bộ vì tính đơn giản của nó.

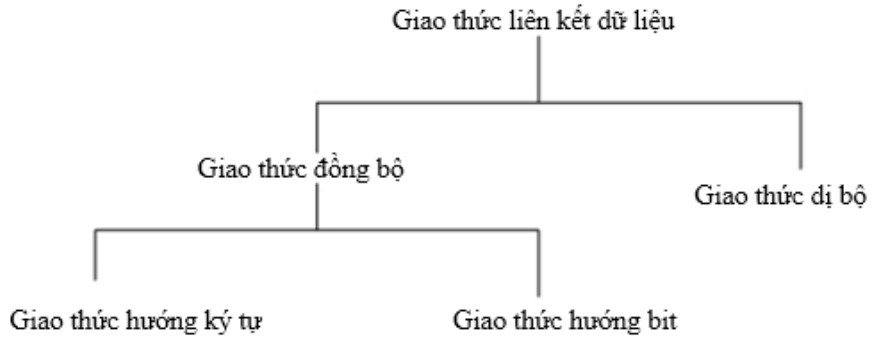
- Giao thức đồng bộ (*synchronous DLP*):

Chèn các ký tự điều khiển hoặc các cờ giữa các dữ liệu của người sử dụng để báo cho bên nhận. Có hai nhóm giao thức đồng bộ:

- ✓ Đồng bộ hướng ký tự (*character – oriented*)
- ✓ Đồng bộ hướng bit (*bit – oriented*)

Các hệ thống truyền thông đòi hỏi hai mức đồng bộ hóa:

- ✓ Mức vật lý: để giữ đồng bộ giữa các đồng hồ người gửi và người nhận.
- ✓ Mức LKDL: để phân biệt dữ liệu của người sử dụng với các cờ và các vùng thông tin điều khiển khác.



Hình 2.6 Phân loại các giao thức liên kết dữ liệu

Sau đây ta xét hai loại giao thức đồng bộ là giao thức truyền tin đồng bộ nhị phân BSC *(Binary Synchronous Control)* và giao thức điều khiển liên kết dữ liệu mức cao HDLC *(Highlevel Data Link Control)*.

Giao thức BSC/Basic mode

Đây là giao thức hướng ký tự (COP)

- *Tập ký tự điều khiển:*

ENQ *(Enquire)*: Yêu cầu trả lời từ một trạm xa.

ACK *(Acknowledgement)*: Thông báo tiếp nhận tốt thông tin.

NAK *(Negative Acknowledgement)*: Thông báo tiếp nhận không tốt thông tin.

STX *(Start of Text)*: Kết thúc phần Header và bắt đầu phần dữ liệu.

ETX *(End of Text)*: Kết thúc phần dữ liệu.

ETB *(End of Transmission Block):* Kết thúc đoạn tin (khối dữ liệu).

SOH *(Start of Heading):* Bắt đầu phần Header của bản tin.

EOT *(End of Transmission):* Kết thúc quá trình truyền tin và giải phóng liên kết.

DLE (Data Link Escape): Để thay đổi ý nghĩa của các ký tự điều khiển truyền tin khác.

SYN *(Synchronous Idle):* Ký tự đồng bộ bản tin để duy trì sự đồng bộ giữa hai bên.

- *Khuôn dạng tổng quát bản tin của giao thức BSC*

SYN	SYN	SOH	Header	STX	TIN Số ký tự (độ rộng 5 – 6 bit)	ETX/ETB	CRC

Nơi nhận	Number seg	Control	Biên nhận

Để thông suốt bản tin, có thể dùng thêm các byte đệm:

SYN	SYN		DLE	DLE		DLE	ETX/ETB	CRC

Khi phát nếu ký tự phát trùng với DLE thì chèn thêm DLE. Khi thu, DLE chèn thêm sẽ được khử bỏ.

- *Các thủ tục chính của BSC/Basic Mode*

Mời truyền tin:

Giả sử trạm A muốn mời trạm B truyền tin, A sẽ gửi lệnh sau tới B:

EOT	B	ENQ

Trong đó: B là địa chỉ của trạm được mời truyền tin,EOT để chuyển liên kết sang trạng thái điều khiển.

Khi B nhận được lệnh này, có thể xảy ra hai trường hợp:

- Nếu có tin để truyền thì trạm B sẽ cấu tạo một đơn vị dữ liệu và gửi cho A.
- Nếu không có tin để gửi, B sẽ gửi EOT để trả lời.

Ở phía A, sau khi gửi lệnh đi quá một thời gian xác định trước mà không nhận được trả lời của B, hoặc là nhận được trả lời sai thì A sẽ chuyển sang trạng thái "phục hồi". Trạng thái này sẽ được nói đến ngay sau đây.

Mời nhận tin:

Giả sử trạm A muốn mời trạm B nhận tin, A sẽ gửi lệnh tương tự như trên tới B:

EOT	B	ENQ

Ở đây EOT có thể vắng mặt.

Khi B nhận được lệnh này, nếu B sẵn sàng nhận tin thì trạm B sẽ gửi ACK về A, ngược lại nó sẽ gửi NAK.

Phía A, sau khi gửi lệnh đi quá một thời gian xác định trước mà không nhận được trả lời của B hoặc nhận được trả lời sai thì A sẽ chuyển sang trạng thái "phục hồi".

Yêu cầu trả lời

Khi một trạm cậần trạm khác trả lời một yêu cầu nào đó đã gửi đi trước, nó chỉ cần gửi lệnh ENQ cho trạm kia.

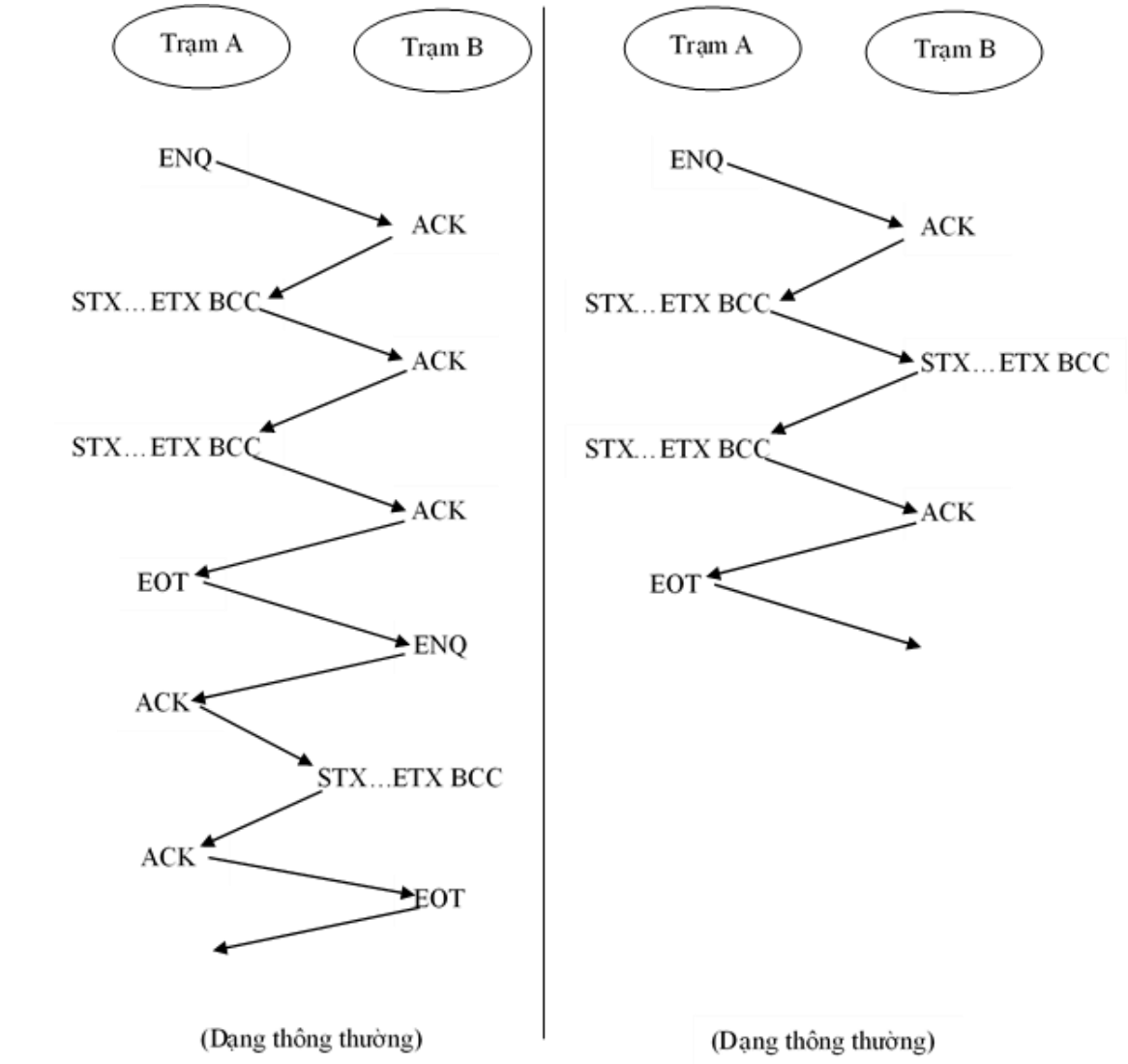
Ngừng truyền tin (tạm thời): gửi lệnh EOT

Giải phóng liên kết: gửi lệnh DLE EOT

Trạng thái phục hồi: Khi một trạm nào đó đi vào trạm thái phục hồi nó sẽ thực hiện một trong các hành động sau:

- ✓ Lặp lại lệnh đã gửi n lần (n là một số nguyên chọn trước)
- ✓ Gửi "yêu cầu trả lời" n lần
- ✓ Kết thúc truyền bằng cách gửi lệnh EOT

Để thấy rõ hơn phương thức trao đổi thông tin của giao thức BSC/Basic Mode ta dùng sơ đồ minh họa ở hình 2.7 dưới đây, trong đó có hai trường hợp: thông thường và hội thoại.



Hình 2.7 Sơ đồ minh họa hoạt động của giao thức BSC/Basic Mode

Giao thức HDLC

HDLC là giao thức hướng bit *(Bit Oriented Protocol – BOP)* có các phần tử của giao thức (đơn vị dữ liệu, thủ tục) được xây dựng từ các cấu trúc nhị phân (xâu bit) và khi nhận dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

Đây là giao thức có vị trí quan trọng nhất, được ISO phát triển để sử dụng trong cả hai trường hợp: điểm - điểm và điểm - nhiều điểm, cho phép truyền thông hai chiều đồng thời.

- *Khuôn dạng tổng quát bản tin của giao thức HDLC*

← Hướng truyền

8 bit 8 bit 128 – 2014 bytes

Flag 01111110	HEADER		INFORMATION Số các bit	FCS (16 bit)	Flag 01111110
	Address	Control			

Trong đó:

Flag(01111110): là cờ duùng để nhận biết điểm bắt đầu và kết thúc bản tin.

Để tránh sự xuất hiện của mã cờ trong nội dung của bản tin, người ta cài đặt cơ chế "cứng" có các chức năng sau:

- ✓ Khi truyền tin cứ sau năm bit 1 liên tiếp thì theêm 1 bit 0 để không nhầm với Flag:01101111111110010

  01101111**0**11110010

  ↑ bít chèn thêm (khi thu thì bit này được khử bỏ)

- ✓ Khi nhận tin, nếu phát hiện có bit 0 sau 5 bit 1 liên tiếp thì tự động loại bỏ bit 0 đó đi.

Address: Vùng chứa địa chỉ trạm đích của khung tin.

Information: Vùng ghi thông tin truyền đi, có kích thước không xác định.

FCS *(Frame Check Sequense):* Vùng để ghi mã kiểm soát lỗi (checksum) cho nội dung khung tin, dung phương pháp CRC với đa thức sinh là:

$$CRS\text{-}CCITT = x^{16} + x^{12} + x^5 + 1$$

Control: Vùng định danh cho các loại khung tin khác nhau của HDLC, có ba dạng:

- ✓ Dạng I: Hiệu lực truyền tin – *Information*
- ✓ Dạng S: Hiệu lực điều hành sự nối – *Supervisor*
- ✓ Dạng N: Chức năng phụ của điều hành nối – *Unnumbered*

➢ *Phương thức trao đổi thông tin:*

Giao thức HDLC có 3 phương thức trao đổi thông tin chínhứng với mỗi phương thức có các giao thức khung tin tương ứng là SNRM, SARM, SABM:

Phương thức trả lời chuẩn SNRM (Set Normal Response Mode): Được sử dụng trong trường hợp cấu hình không cân bằng, một trạm điều khiển chung (master), các trạm còn lại (slave) chỉ có thể truyền tin khi trạm chủ cho phép.

Phương thức trả lời dị bộ SARM (Set Asynchromous Response Mode): Cũng được sử dụng trong trường hợp cấu hình không cân bằng như trường hợp trên, nhưng các trạm slave được phép truyền tin mà không cần sự cho phép của trạm master. Phương thức này được sử dụng trong trường hợp điểm – điểm với liên kết hai chiều, cho phép trạm slave gửi các gói tin (frame) không đồng bộ với trạm master.

Phương thức trả lời dị bộ cân bằng SABM (Set Asynchronous Balanced Mode): Sử dụng trong trường hợp điểm – điểm, liên kết 2 chiều. Trong đó các trạm đều có vai trò tương đương.

➢ *Các giao thức dẫn xuất của HDLC*

- ✓ LAP *(Link Access Procerdure):* tương ứng với phương thức trả lời dị bộ (ARM)
- ✓ LAPB *(Link Access Protocol Balanced):* tương ứng với phương thức trả lời dị bộ cân bằng (ABM), được duùng hầu hết trong các mạng truyền dữ liệu công cộng X25.
- ✓ LAP-D *(Link Access Procedure, D Channel):* được xây dựng từ LAP-B và được dùng như giao thức liên kết dữ liệu cho các mạng ISDN

- ✓ SDLC, ADCCP.

➢ So sánh BOP và COP

- ✓ BOP nhận lần lượt từng bit một, do đó mềm dẻo, dễ dàng tương thích với các hệ khác nhau.
- ✓ BOP có overhead (phụ trội), số bit bổ sung và số tín hiệu điều khiển ít do đó có tốc độ cao.
- ✓ Thủ tục điều khiển trên bit nhị phân đảm bảo không phụ thuộc mã dùng. Cách giải quyết này mềm dẻo và cho phép giaải quyết vô số yêu cầu khác.
- ✓ Thủ tục HDLC được coi là chuẩn quốc tế và sẽ thống trị trong thời gian tới, nó thích ứng với các hệ thống phức tạp. Đối với các thiết bị ít phức tạp có thể dùng HDLC đơn giản hóa để đảm bảo sự tương thích với HDLC và sự phát triển mở rộng hệ thống sau này.

2.6.2.3 Tầng mạng (Network)

a) Vai trò và chức năng của tầng mạng

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

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

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

Ngoài 2 chức năng quan trọng nói trên, tầng mạng cũng thực hiện một số chức năng khác, đó là: thiết lập, duy trì và giải phóng các liên kết logic (cho tầng mạng), kiểm soát lỗi, kiểm soát luồng dữ liệu, dồn/tách kênh, cắt/hợp dữ liệu,..

b) Các vấn đề của tầng mạng

➢ ***Định địa chỉ cho tầng mạng***

Tầng mạng sử dụng các kiểu địa chỉ bổ sung sau:

- Địa chỉ mạng logic *(Logical Network Address)*: định tuyến các gói tin theo các mạng cụ thể trên liên mạng. Dùng để định danh một mạng cụ thể trên liên mạng dưới dạng một nguồn hay đích của một gói tin.

- Địa chỉ dịch vụ *(Service Address)*: định tuyến các gói tin theo các tiến trình cụ thể đang chạy trên thiết bị đích, dùng định danh một giao thức hay tiến trình trên máy tính là nguồn hay đích của một gói tin.
- Địa chỉ mạng vật lý (MAC): định danh một thiết bị cụ thể dưới dạng một nguồn hay đích của một khung.

Địa chỉ vật lý của máy trạm:

Mỗi thiết bị trên một mạng có một địa chỉ vật lý duy nhất để giao tiếp với các thiết bị khác, còn gọi là địa chỉ phần cứng. Trên tất cả các mạng hiện nay, mỗi địa chỉ xuất hiện một lần duy nhất (nghĩa là mỗi thiết bị chỉ có một địa chỉ duy nhất). Đối với phần cứng, địa chỉ thường được mã hóa trong thiết bị card mạng *(Network Interface Card)*, có thể được đặt bằng chuyển mạch hoặc bằng phần mềm. Trong mô hình OSI thì địa chỉ này được đặt ở tầng vật lý.

Độ dài của địa chỉ vật lý phụ thuộc vào từng mạng, chẳng hạn với mạng Ethernet và một số mạng khác thì địa chỉ vật lý dài 48 bit. Để trao đổi thông tin thì cần có địa chỉ của nơi gửi và địa chỉ của nơi nhận.

Hiện nay IEEE đang đảm nhiệm việc ấn định địa chỉ vật lý tổng thể *(Universal Physical Address)* cho các subnet. Đối với mỗi subnetwork, IEEE ấn định một phần địa chỉ đồng nhất đối với tất cả các subnetwork gọi là OUI (*Organization Unique Identifier)* phần này có độ dài là 24 bit, cho phép IEEE ấn định phần địa chỉ 24 bit còn lại theo yêu cầu.

- ***Dịch vụ cung cấp cho tầng giao vận***
  - ✓ Các dịch vụ phải độc lập với công nghệ được dùng trong mạng.
  - ✓ Tầng giao vận phải độc lập với công nghệ được dùng trong mạng.
  - ✓ Các địa chỉ mạng phải thống nhất để tầng giao vận có thể dùng cả mạng LAN và WAN.

Có 2 loại dịch vụ:

- ✓ Dịch vụ truyền tin có liên kết.
- ✓ Dịch vụ truyền tin không liên kết

Sự khác nhau giữa 2 dịch vụ:

Vấn đề	Dịch vụ có liên kết	Dịch vụ không liên kết
Khởi động kênh	Cần thiết	Không
Địa chỉ đích	Chỉ cần lúc khởi động	Cần ở mọi gói tin
Thứ tự gói tin	Được đảm bảo	Không đảm bảo
Kiểm soát lỗi	Ở tầng mạng	Ở tầng giao vận
Điều khiển thông lượng	Ở tầng mạng	Ở tầng giao vận
Thỏa thuận tham số	Có	Không
Nhận dạng liên kết	Có	Không

Các hàm cơ bản của dịch vụ liên kết tầng mạng:

N-CONNECT.Request (callce, caller, acks wanted, exp wanted, qos, user data)
N-CONNECT.Indication (callce, caller, acks wanted, exp wanted, qos, user data)
N-CONNECT.Response (response acks wanted, exp wanted, qos, user data)
N-CONNECT.Configmation (response acks wanted, exp wanted, qos, user data)
N-DISCONNECT.Request (orginator, reason, user data, responding address)
N-DISCONNECT.Indication (orginator, reason, user data, responding address)
N-DATA.Request (user data)
N-DATA.Indication (user data)
N-DATA-ACKNOWLEDGED.Request ()
N-DATA-ACKNOWLEDGED.Indication ()
N-EXPEDITED-DATA.Request (user data)
N-EXPEDITED-DATA.Indication (user data)
N-RESET.Request (originator, reson)
N-RESET.Inditcation (originator, reson)
N-RESET.Response ()
N-RESET.Confirm ()

Các hàm cơ bản của dịch vụ không liên kết tầng mạng:

N-UNITDATA.Request (source address, destination addres, qos, user_data)
N-UNITDATA.Indication (source address, destination address, qos, user_data)
N-FACILITY.Request (qos)
N-FACILITY.Indication (destination adress, qos, reason)
N-FACILITY.Indication (destination adress, qos, reason)

Hàm N-FACILITY,request cho phép người sử dụng dịch vụ mạng biết tỷ lệ phần trăm gói tin đang được chuyển vận.

Hàm N-REPORT.Indication cho phép tầng mạng thông báo với người sử dụng dịch vụ mạng

- ***Tổ chức các kênh truyền tin trong tầng mạng***

Có hai loại kênh truyền tin hoạt động trong mạng:

- *Kênh ảo (virtual circuit)*

Tương đương kênh điện thoại trong tầng vật lý sử dụng trong mạng có liên kết. Kênh được thiết lập cho mỗi liên kết. Mỗi khi đã được thiết lập thì các gói tin được chuyển đi tương tự trong mạng điện thoại cho đến khi liên kết bị hủy bỏ.

- ✓ Mỗi nút mạng chứa một kênh ảo, với cửa vào cho một kênh ảo.
- ✓ Khi một liên kết được khởi động, một kênh ảo chưa dùng sẽ được chọn.
- ✓ Nút chọn kênh ảo chứa đường dẫn đến trạm tiếp theo và có số thấp nhất.

Khi gói tin khởi động đến nút đích, nút chọn kênh ảo có số thấp nhất thay thế số trong gói tin và chuyển vào trạm đích. Số kênh ảo nối với trạm đích có thể khác số kênh ảo mà trạm nguồn sử dụng.

- *Mạng Datagram*

Tương tự với điện báo sử dụng trong mạng không liên kết. Trong mạng này, không có tuyến đường nào được thiết lập. Các gói tin có thể đi theo nhiều đường khác

nhau mà không nhất thiết theo một trình tự xác định. Thông tin vào là địa chỉ đích, thông tin ra là nút mạng phải tới.

Mạng Datagram phức tạp về điều khiển nhưng nếu kênh hỏng thì dễ dàng đi theo kênh khác. Do đó có thể giải quyết được vấn đề tắc nghẽn trong dữ liệu.

Các đặc trưng của mạng Datagram và mạng kênh ảo:

Vấn đề	Mạng Datagram	Mạng kênh ảo
Khởi động kênh	Không	Cần thiết
Địa chỉ (đ/c) hóa	Gói tin phải có đ/c nguồn đ/c đích	Gói tin chỉ cần số của kênh ảo
Thông tin tìm đường	Không cần bất cứ thông tin nào	Mỗi kênh ảo cần một vùng trong bảng
Tìm đường	Mỗi gói tin tìm đường độc lập. Phải tìm đường mỗi khi có gói tin tới nút mạng	Được thiết lập khi khởi động kênh ảo mới. Liên kết sẽ được duy trì cho cả phiên
Điều khiển	Chỉ mất gói tin ở trong nút hỏng	Kênh ảo đi qua nút hỏng sẽ bị hủy
Hỏng nút	Khó khắc phục	Dễ khắc phục hơn
Độ phức tạp	Trong tầng giao vận	Trong tầng mạng
Thích hợp	Các dịch vụ liên kết và không liên kết	Các dịch vụ liên kết

- ***Tìm đường đi trong mạng***
  - *Tổng quan*

Chức năng quan trọng nhất của tầng mạng là dẫn đường cho các gói tin từ trạm nguồn tới trạm đích. Thuật toán tìm đường đi là qui trình để quyết định chọn đường ra khỏi nút mạng nhằm gởi gói tin đi tiếp tới nút khác.

Yêu cầu của thuật toán tìm đường:

- ✓ Chính xác, ổn định, đơn giản và tối ưu.
- ✓ Thuật toán tìm đường phải có khả năng cập nhật lại cấu hình và đường vận chuyển để không phải khởi động lại mạng khi có một nút hỏng hoặc phải ngừng hoạt động của các máy ở trạm.

Các thuật toán phải chia thành 2 nhóm chính:

- ✓ Nhóm không thích nghi *(non adaptive)*: việc chọn đường không dựa vào việc đánh giá tình trạng giao thông và cấu hình trong thời gian thực.
- ✓ Nhóm thích nghi *(adaptive):* việc tìm đường phải thích nghi với tình trạng giao thông hiện tại.

Sơ đồ mạng được biểu diễn dưới dạng đồ thị, mỗi nút của đồ thị là một nút mạng, cung của đồ thị biểu diễn đường truyền nối giữa hai nút. Việc chọn đường giữa hai nút mạng là tìm đường ngắn nhất giữa chúng.

Mỗi cung được gán một nhãn cho biết thời gian trung bình phải đợi và thời gian truyền một gói tin chuẩn. Thời gian này được thử mỗi giờ hay mỗi ngày một lần. Đườngđi ngắn nhất là đường đi có ít bước chuyển tiếp qua nút nhất và có số đo độ dài nhỏ nhất vàmất ít thời gian.

Có nhiều thuật toán để tìm đường ngắn nhất giữa 2 điểm, ví dụ thuật toán Dijkstra (1959). Ta xây dựng đồ thị cho các nút mạng và tìm khoảng cách giữa các nút mạng.

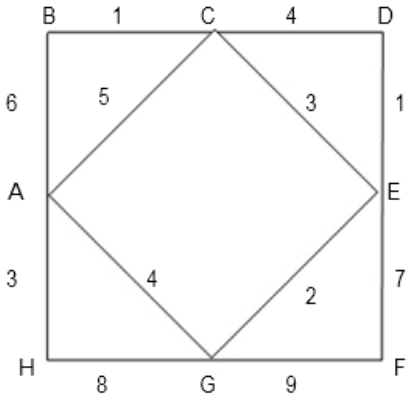
- *Giải thuật Dijkstra.*

Bài toán đặt ra là: tìm đường đi có "độ dài" (một đại lượng được dùng để làm thước đoví dụ độ trễ, cước phí truyền tin) cực tiểu, từ một nút (nguồn) cho trước đến mỗi nút còn lại của mạng (đích). Ở đây ta coi mạng như là một đồ thị có hướng G(V,E), V là tập đỉnh với n đỉnh tương ứng với n nút mạng, E là tập cung của đồ thị. Ma trận trọng số là a[u,v], u,v ∈ V.

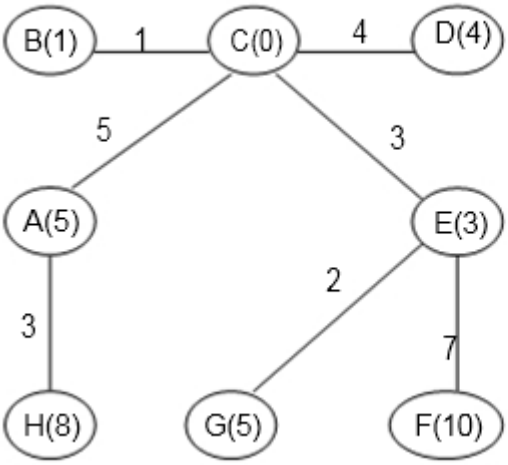
Thuật toán được xây dựng dựa trên cơ sở gán cho các đỉnh các nhãn tạm thời. Nhãn của mỗi đỉnh cho biết cận của độ dài đường đi ngắn nhất từ s đến nó. Các nhãn này sẽ được biến đổi theo một thủ tục lặp, mà ở mỗi bước lặp có một nhãn tạm thời trở thành nhãn cố định. Nếu nhãn của một đỉnh nào đó trở thành một nhãn cố định thì nó sẽ cho ta không phải là cận trên mà là độ dài của đường đi ngắn nhất từ đỉnh s đến nó. Thuật toán được mô tả cụ thể như sau:

```
Procedure Dijstra;
(* Đầu vào:
        Đồ thị có hướng G=(V,E) với n đỉnh,
        s ∈ V là đỉnh xuất phát, a[u,v], u,v ∈V là ma trận trọng số; Giả thiết:
a[u,v]≥0, u,v ∈V.
Đầu ra:
        Khoảng cách từ đỉnh s đến tất cả các đỉnh còn lại d[v], v ∈V.
        Trước[v],v ∈V, ghi nhận đỉnh đi trước v trong đường đi ngắn nhất từ s đến v *)
        Begin
                (* Khởi tạo *)
                for v ∈V do
                begin
                        d[v]:=a[s,v];
                        Truoc[v]:=s;
                end;
            d[s]:=0; T:=V\ {s} ; (* T là tập các đỉnh cá nhãn tạm thời *)
            (* Bước lặp *)
            while T <>  θ  do
            begin
                tìm đỉnh u ∈T thoả mãn d[u]=min {d[z]: z ∈T} ; T:=T\ {u} ;
                (* Cố định nhãn của đỉnh u*)
                For v ∈T do
                If d[v]>d[u]+a[u,v] then
                        Begin
                                d[v]:=d[u]+a[u,v]; Truoc[v]:=u;
                        End;
            end;
        End;
```

Ví dụ: Tìm đường đi ngắn nhất từ C đến các đỉnh còn lại của đồ thị ở hình dưới đây.



Từ đó ta thiết kế được "câychọn đường" và bảng chọn đường như các hình vẽ sau:

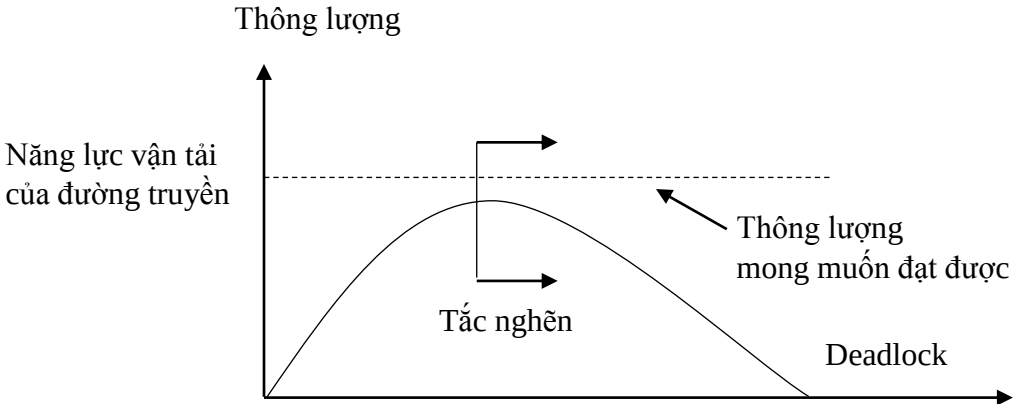


Đích	Nút kế tiếp
A	A
B	B
D	D
E	E
F	E
G	E
H	A

- *Tắc nghẽn trong mạng*

Các khái niệm

- ✓ Hiện tượng tắc nghẽn *(congestion):* lưu lượng đến mạng tăng lên, thông lượng vận chuyển của mạng lại giảm đi.
- ✓ Deadlock: tình trạng tắc nghẽn trầm trọng đến mức mạng bị nghẹt hoàn toàn, thông lượng vận chuyển của mạng tụt xuống bằng không.



Nguyên nhân dẫn đến tắc nghẽn:

- ✓ Lưu lượng đi đến trên nhiều lối vào đều cần cùng một đường đi ra.

- ✓ Tốc độ xử lý tại các router chậm.
- ✓ Các đường truyền có bandwidth thấp, dẫn đến hiện tượng thắt cổ chai.

Biểu hiện của tắc nghẽn: Thời gian khứ hồi (RTT) tăng cao bất thường

Các biện pháp khắc phục:

- ✓ Cung cấp đủ bộ đệm ở đầu vào và ra của các đường truyền.
- ✓ Quản lý bộ đệm hợp lý, có thể loại bỏ sớm (RED).
- ✓ Hạn chế lưu lượng đến ngay ở đầu vào của toàn bộ hệ thống.
- ✓ Điều khiển lưu lượng.

➢ *Kết nối liên mạng*

Nhu cầu trao đổi thông tin và phân chia các tài nguyên dùng chung đòi hỏi hoạt động truyền thông không chỉ ở phạm vi cục bộ mà ở cả khuôn khổ quốc gia và quốc tế. Từ đó dẫn đến sự nối kết các mạng viễn thông tin học được đặt ở các vị trí địa lý khác nhau và chịu sự quản lý của các tổ chức hoặc quốc gia khác nhau.

Sự kết nối mạng *(Network Interconnection)* giống như ghép nối đơn lẻ nhưng phức tạp hơn nhiều do tính chất không thuần nhất của các mạng con được kết nối. Chúng có thể có kiến trúc khác nhau bao gồm các máy tính nút mạng. Đường truyền khác nhau, chiến lược quản lý khác nhau.

Người ta thường xem xét các vấn đề sau để kết nối các mạng còn lại với nhau:

- Xem mỗi nút mạng con nhu là các hệ thống mở: mỗi nút mạng con có thể truyền thông trực tiếp với một nút mạng con khác bất kỳ. Như thế yêu cầu phải xây dựng một chuẩn chung cho các mạng.
- Xem mỗi mạng như là một hệ thống mở: hai nút thuộc hai mạng con không bắt tay trực tiếp với nhau mà phải thông qua một phần tử trung gian gọi là giao diện kết nối *(interconnection interface)*đặt giữa hai mạng con đó.

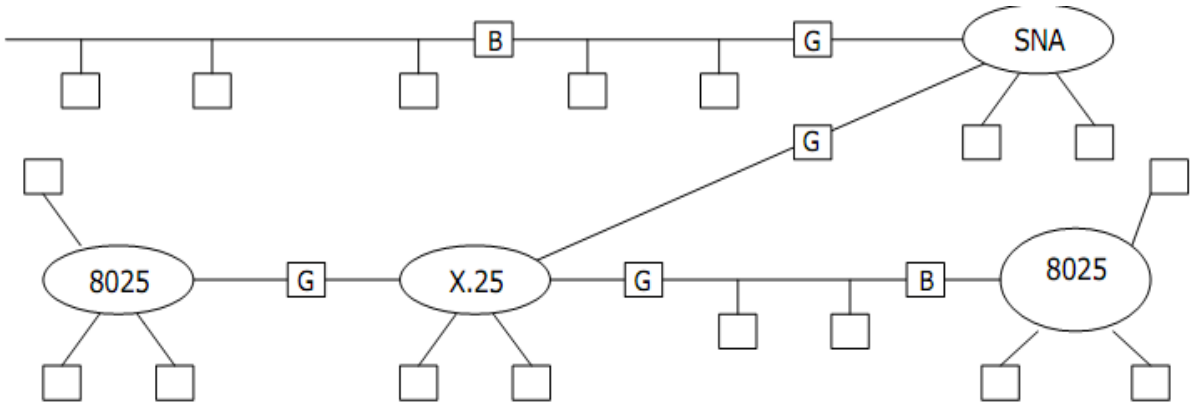
Chức năng của giao diện kết nối phụ thuộc vào sự khác biệt kiến trúc của mạng con: sự khác biệt càng lớn thì chức năng của giao diện càng phức tạp.

Có thể có các kết nối mạng như sau:

- LAN – LAN: Nối các mạng cục bộ.
- LAN – WAN: Nối các mạng cục bộ với mạng đường dài.
- WAN – WAN: Nối các mạng đường dài.
- LAN – WAN – LAN: Nối một mạng đường dài với mạng cục bộ.

Nếu máy nguồn và máy đích không ở cùng một mạng phải tìm đườngtừ mạng này sang mạng khác. Nếu trạm nguồn và đích không ở hai mạng liền kề thì giải quyết tìm đường qua nhiều trạm.

Các mạng khác nhau có các giao thức khác nhau, dẫn đến khác nhau về dạng khuôn của gói tin, điều khiển dòng dữ liệu và quy tắc xác nhận.



Hình 2.8 Kết nối liên mạng

➢ *Giao thức liên mạng IP*

Giao thức IP *(Internet Protocol)* hoạt động ở tầng mạng, cung cấp dịch vụ dữ liệu không liên kết cho nhiều giao thức liên kết dữ liệu khác. Đơn vị dữ liệu dùng trong giao thức IP được gọi là *datagram*, hay còn gọi là khung tin IP.

Chức năng của giao thức IP:

- ✓ Định nghĩa gói tin Datagram là đơn vị dữ liệu cơ bản của việc truyền tin trên mạng Internet.
- ✓ Xác định mô hình đánh địa chỉ cho các khung tin và quản lý các quá trình trao đổi, xử lý các khung tin này.
- ✓ Chọn đường cho các datagram trên mạng.
- ✓ Cung cấp cơ chế trên gói tin trên mạng hiệu quả nhất.
- ✓ Phân đoạn và tổng hợp các gói tin.

Tính chất của giao thức IP:

- ✓ Hoạt động theo phương thức không kết nối: IP không chuyển các thông tin điều khiển trước khi truyền dữ liệu.
- ✓ Không tin cậy: Giao thức IP không có khả năng phát hiện và khắc phục lỗi, không quan tâm đến vấn đề dữ liệu có được nhận một cách chính xác hay không. Do đó, các gói dữ liệu có thể bị thất lạc, bị trùng lắp, bị chuyển chậm hoặc đi không đúng thứ tự, mỗi gói dữ liệu được xử lý độc lập với nhau và có thể gửi theo những đường định tuyến khác nhau.

➢ *Mạng X.25*

Được CCITT công bố lần đầu tiên vào 1970 lúc lĩnh vực viễn thông lần đầu tiên tham gia vào thế giới truyền dữ liệu với các đặc tính:

- X25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối đem lại chất lượng đường truyền cao cho dù chất lượng đường dây truyền không cao.
- X25 được thiết kế cho cả truyền thông chuyển mạch lẫn truyền thông điểm nối điểm.
- Được quan tâm và tham gia nhanh chóng trên toàn cầu.

Trong X25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ

phức tạp trong việc phối hợp các thủ tục giữa hai tầng kề nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm cho đường truyền có chất lượng rất cao gần như phi lỗi. Tuy nhiên do vậy khối lượng tính toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí.

Đặc điểm:

- Là mạng truyền dữ liệu công cộng đầu tiên.
- Vận chuyển dữ liệu hướng kết nối.
- Để sử dụng X.25, máy tính đầu tiên phải thiết lập kết nối tới một máy tính ở xa, nghĩa là phải thiết lập một cuộc gọi *(telephone call).*
- Kết nối này được gán 1 connection number để sử dụng cho các gói *(packet)* số liệu vận chuyển:
    - ✓ Nhiều kết nối có thể được sử dụng đồng thời giữa 2 máy tính.
    - ✓ Kết nối trong X.25 là kết nối *ảo (Virtual Circuit).*

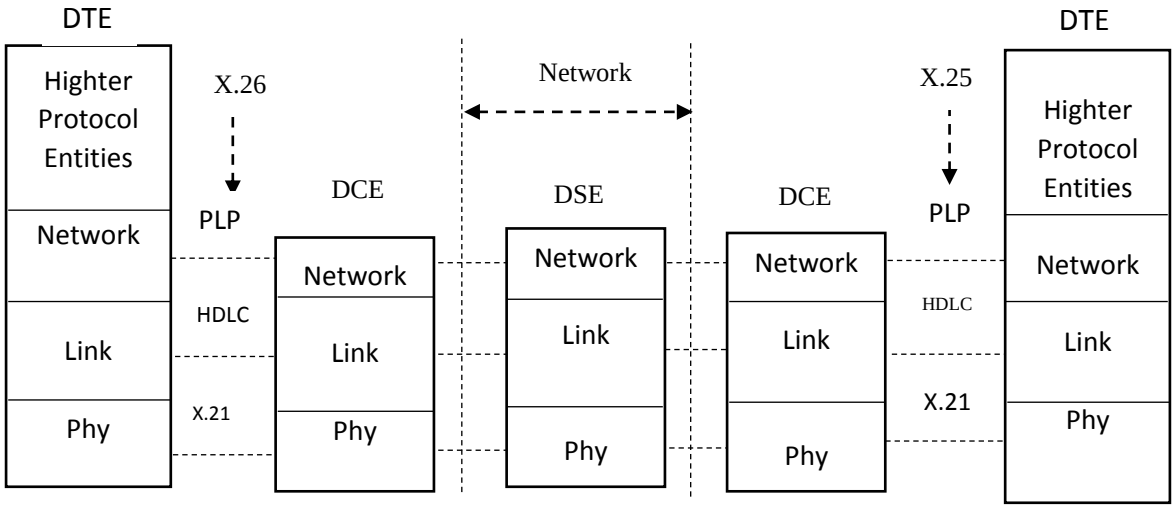
Nguyên tắc hoạt động

- X.25 là một dịch vụ truyền thông máy tính công cộng, dựa trên hệ thống viễnthông diện rộng (PSTN).
- X.25 được CCITT và sau này là ITU chuẩn hoá (1976).
- X.25 chỉ đặc tả giao diện giữa DTE và DCE:
    - ✓ DTE (Data Terminal Equipment)- thiết bị đầu cuối dữ liệu
    - ✓ DCE (Data Circuit-terminating Equipment) - thiết bị mạch đầu cuối dữ liệuhay là thiết bị kết nối mạng.
- X.25 không quy định cụ thể kiến trúc và tổ chức hoạt động nội bộ của mạng.
- Tổ chức và thực hiện hệ thống mạng để cung cấp dịch vụ X.25 tại giao diệnvới NSD là nhiệm vụ của nhà cung cấp dịch vụ X.25 - thường là nhà cung cấp dịch vụ viễn thông công cộng.

X.25 qui định sử dụng các giao thức chuẩn ở các mức như sau:

- *Mức vật lý:*
    - ✓ X.21 cho truyền số liệu số (Digital) giữa DTE và DCE
    - ✓ X.21 bit cho truyền số liệu tương tự (Analog) giữa DTE và DCE
- *Mức liên kết:*LAPB (Link Access Protocol Balanced), là một phần của HDLCđể trao đổi số liệu tin cậy giữa DTE và DCE
- *Mức mạng:*
    - ✓ PLP (Packet Level Protocol): giao thức chuyển mạch gói + hướng kết nối, các subscriber sử dụng để thiết lập VC và truyền thông với nhau.
    - ✓ Là giao thức được đặc tả mới trong X.25

Ba mức trên tương ứng với 3 mức thấp nhất của mô hình ISO/OSI



Hình 2.9 Đặc tả giao diện mạng X25

Các đặc điểm quan trọng nhất của X.25:

- Các gói tin điều khiển cuộc gọiđược dùng để thiết lập và huỷ bỏ các kênh ảo, được gửi trên cùng kênh và mạch ảo như các gói tin dữ liệu.
- Việc dồn kênh của các kênh ảo xảy ra ở tầng 3
- Cả tầng 2 và tầng 3 đều áp dụng cơ chế điều khiển lưu lượng và kiểm soát lỗi.
- X.25 được sử dụng rộng rãi trong khoảng 10 năm.
- Khoảng 1980, X.25 được thay thế bởi một mạng mới - Frame Relay.

➢ ***Công nghệ chuyển mạch nhanh***

▪ *Mạng chuyển mạch khung – Frame Relay (FR)*

Mỗi gói tin trong mạng gọi là Frame, do vậy mạng gọi là Frame relay. Đặc điểm khác biệt giữa mạng Frame Relay và mạng X25 mạng Frame Relay là chỉ kiểm tra lỗi tại hai trạm gửi và trạm nhận còn trong quá trình chuyển vận qua các nút trung gian gói tin sẽ không được kiểm lỗi nữa. Do vậy thời gian xử lý trên mỗi nút nhanh hơn, tuy nhiên khi có lỗi thì gói tin phải được phát lại từ trạm đầu. Với độ an toàn cao của đường truyền hiện nay thì chi phí việc phát lại đó chỉ chiếm một tỷ lệ nhỏ nếu so với khối lượng tính toán được giảm đi tại các nút nên mạng Frame Relay tiết kiệm được tài nguyên của mạng hơn so với mạng X25.

Frame relay không chỉ là một kỹ thuật mà còn là thể hiện một phương pháp tổ chức mới. Với nguyên lý là truyền mạch gói nhưng các thao tác kiểm soát giữa các đầu cuối giảm đáng kể kỹ thuật Frame Relay cho phép thông luợng tối đa đạt tới 2Mbps và hiện nay nó đang cung cấp các giải pháp để tương nối các mạng cục bộ LAN trong một kiến trúc xương sống tạo nên môi trường cho ứng dụng multimedia.

Khác nhau căn bản giữa FR và X.25:

- ✓ Tín hiệu điều khiển cuộc gọi được vận chuyển trên một kết nối logic riêng vì vậy, các node trung gian không cần phải duy trì các bảng trạng thái và xử lý các message này cho từng kết nối.
- ✓ Multiplexing và switching đối với các kết nối logic được thực hiện ở tầng 2, do đó loại bỏ được chi phí xử lý ở một tầng.

- ✓ Điều khiển lưu lượng và kiểm soát lỗi: Không áp dụng các cơ chế điều khiển theo chặng. FR cũng không cung cấp các cơ chế điều khiển End to end, nhiệm vụ này các tầng trên phải giải quyết.

Ưu điểm của FR với X.25:

- ✓ Làm cho quá trình truyền thông hợp lý hơn
- ✓ Chức năng giao thức tại giao diện user-network được giảm bớt
- ✓ Chi phí xử lý bên trong mạng cũng giảm

Lower delay & Higher throughput (cỡ 1 bậc)

- ✓ Ứng dụng quan trọng nhất của Frame Relay: kết nối các mạng LAN ở các văn phòng của một công ty.
- ✓ Frame Relay đạt được mức độ thành công vừa phải, hiện vẫn được sử dụng.

Tóm tắt các đặc trưng công nghệ:

- ✓ FR thực hiện các chức năng cơ bản của mức Data link: tạo và xử lý frame, địa chỉ hoá, quản lý các kênh ảo.
- ✓ Sử dụng kỹ thuật dồn/tách kênh không đồng bộ ở mức data link: Sử dụng hiệu quả hơn đường truyền. Tốc độ trao đổi số liệu: 56 Kbps - 2,048 Mbps.
- ✓ Thiết lập và giải phóng kênh theo giao thức báo hiệu chuẩn Q.931 của mạng ISDN.
- ✓ Không có chức năng xử lý giao thức ở mức mạng.
- ✓ No Link-by-link Flow Control and Error Control: Các ES kiểm tra phát hiện lỗi và khắc phục (end-to-end).
- ✓ Hệ chuyển mạch ở giao diện giữa mạng và hệ thống cuối kiểm tra CRC và không forward các frame bị lỗi.
- ✓ Giao diện quản trị nội tại LMI (Local Management Interface) của FR hỗ trợ việc quản trị trao đổi số liệu trên các kênh ảo trong mạng.

- *Kỹ thuật ATM*

Hiện nay kỹ thuật Cell Relay dựa trên phương thức truyền thông không đồng bộ (ATM) có thể cho phép thông lượng hàng trăm Mbps. Đơn vị dữ liệu dùng trong ATM được gọi là tế bào. Các tế bào trong ATM có độ dài cố định là 53 bytes, trong đó 5 bytes dành cho phần chứa thông tin điều khiển *(cell header)* và 48 bytes chứa dữ liệu của tầng trên.

Trong kỹ thuật ATM, các tế bào chứa các kiểu dữ liệu khác nhau được ghép kênh tới một đường dẫn chung được gọi là đường dẫn ảo *(virtual path).* Trong đường dẫn ảo đó có thể gồm nhiều kênh ảo *(virtual channel)* khác nhau, mỗi kênh ảo được sử dụng bởi một ứng dụng nào đó tại một thời điểm.

ATM đã kết hợp những đặc tính tốt nhất của dạng chuyển mạch liên tục và dạng chuyển mạch gói, nó có thể kết hợp dải thông linh hoạt và khả năng chuyển tiếp cao tốc và có khả năng quản lý đồng thời dữ liệu số, tiếng nói, hình ảnh và multimedia tương tác.

Mục tiêu của kỹ thuật ATM là nhằm cung cấp một mạng dồn kênh và chuyển mạch tốc độ cao, độ trễ nhỏ đáp ứng cho các dạng truyền thông đa phương tiện (multimecdia)

Chuyển mạch cell cần thiết cho việc cung cấp các kết nối đòi hỏi băng thông cao, tình trạng tắt nghẽn thấp, hỗ trợ cho lớp dịch vụ tích hợp lưu thông dữ liệu âm thanh hình ảnh. Đặc tính tốc độ cao là đặc tính nổi bật nhất của ATM.

ATM sử dụng cơ cấu chuyển mạch đặc biệt: ma trận nhị phân các phần tử chuyển mạch *(a matrix of binary switching elements)* để vận hành lưu thông. Khả năng mở rộng (scalability) là một đặc tính của cơ cấu chuyển mạch ATM. Đặc tính này tương phản trực tiếp với những gì diễn ra khi các trạm cuối được thêm vào một thiết bị liên mạng như router. Các router có năng suất tổng cố định được chia cho các trạm cuối có kết nối với chúng. Khi số lượng trạm cuối gia tăng, năng suất của router tương thích cho trạm cuối thu nhỏ lại. Khi cơ cấu ATM mở rộng, mỗi thiết bị thu trạm cuối, bằng con đường của chính nó đi qua bộ chuyển mạch bằng cách cho mỗi trạm cuối băng thông chỉ định. Băng thông rộng được chỉ định của ATM với đặc tính có thể xác nhận khiến nó trở thành một kỹ thuật tuyệt hảo dùng cho bất kỳ nơi nào trong mạng cục bộ của doanh nghiệp.

Như tên gọi của nó chỉ rõ, kỹ thuật ATM sử dụng phương pháp truyền không đồng bộ (asynchronouns) các tề bào từ nguồn tới đích của chúng. Trong khi đó, ở tầng vật lý người ta có thể sử dụng các kỹ thuật truyền thông đồng bộ như SDH (hoặc SONET).

Nhận thức được vị trí chưa thể thay thế được (ít nhất cho đến những năm đầu của thế kỷ 21) của kỹ thuật ATM, hầu hết các hãng khổng lồ về máy tính và truyền thông như IBM, ATT, Digital, Hewlett - Packard, Cisco Systems, Cabletron, Bay Network,... đều đang quan tâm đặc biệt đến dòng sản phẩm hướng đến ATM của mình để tung ra thị trường. Có thể kể ra đây một số sản phẩm đó như DEC 900 Multiwitch, IBM 8250 hub, Cisco 7000 rounter, Cablectron, ATM module for MMAC hub.

Nhìn chung thị trường ATM sôi động do nhu cầu thực sự của các ứng dụng đa phương tiện. Sự nhập cuộc ngày một đông của các hãng sản xuất đã làm giảm đáng kể giá bán của các sản phẩm loại này, từ đó càng mở rộng thêm thị trường. Ngay ở Việt Nam, các dự án lớn về mạng tin học đều đã được thiết kế với hạ tầng chấp nhận được với công nghệ ATM trong tương lai.

2.6.2.4 Tầng giao vận (Transportation)

a) Vai trò và chức năng của tầng giao vận

Tầng giao vận làm nhiệm vụ thiết lập, duy trì và hủy bỏ các cuộc giao tiếp giữa hai máy, đảm bảo việc dữ liệu truyền giống hoàn toàn dữ liệu nhận. Dữ liệu qua các mạng con có thể bị lỗi, tập tin tầng giao vận thực hiện cải thiện chất lượng dịch vụ, đảm bảo dữ liệu được truyền một cách chính xác và truyền lại nếu như phát hiện thấy lỗi. Tầng giao vận quản lý dữ liệu gửi, xác định trật tự của dữ liệu và độ ưu tiên của dữ liệu đó.

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

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

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

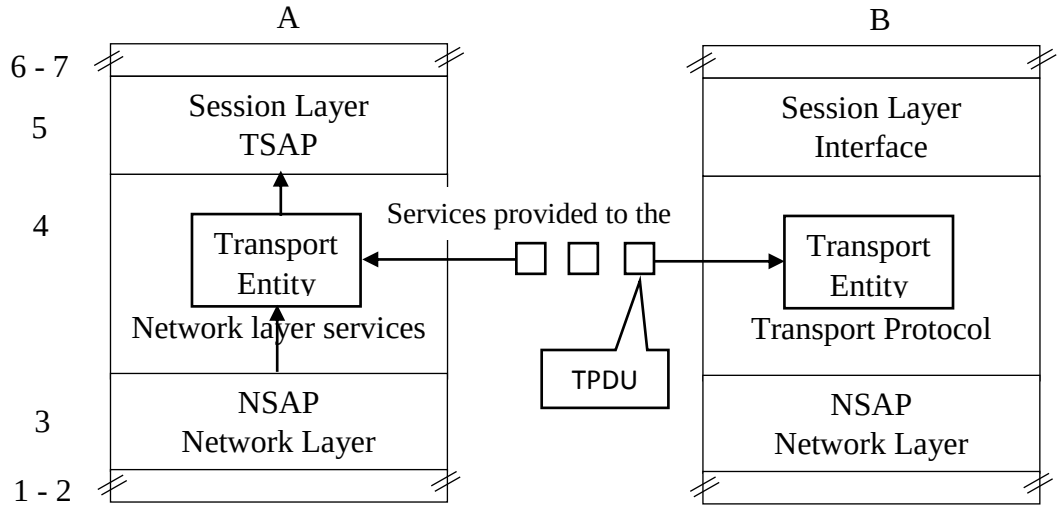
- Mạng loại C: Có tỷ suất lỗi không chấp nhận được (không tin cậy) hay là giao thức không liên kết. Tầng giao vận phải có khả năng phục hồi lại khi xảy ra lỗi và sắp xếp lại thứ tự các gói tin.

b) Các vấn đề của tầng giao vận

➢ *Cung cấp dịch vụ cho tầng phiên*

Để thực hiện mục tiêu chuyển giao dữ liệu tin cậy, an toàn cho tầng 5 và tầng 4 phải dùng các dịch vụ được cung cấp từ tầng 3 *(network layer*). Phần cứng và phần mềm trong phần 4 để thực hiện công việc coi là thực thể giao vận *(transport entity).*

Mối quan hệ giữa các lớp 3,4,5 được mô tả bởi hình sau:



Hình 2.10 Mối quan hệ giữa các thức thể trong tầng phiên

Có hai dịch vụ mạng nên cũng có hai dịch vụ giao vận: dịch vụ có kết nối và không kết nối. Do dữ liệu qua các subnet có thể sai sót, người sử dụng không có được điều khiển trên subnet hoặc tăng cường quản lý lỗi ở tầng hai. Chỉ có khả năng đặt thêm 1 tầng trên lớp 3 để cải thiện chất lượng dịch vụ (QoS). Nếu giữa chúng một tầng giao vận được kết nối mạng được kết thúc đột ngột và không biết được sự cố gì đã xảy ra, nó có thể thiết lập một kết nối mới ở lớp mạng tới tầng giao vận ở xa và gởi yêu cầu hỏi số liệu nào đến, số liệu nào không tự nó biết được sai sót xảy ra ở đâu. Tầng 4 có thể phát hiện mất gói tin, số liệu bị biến đổi, N-RESET ở lớp mạng. Tầng 1 -> 4 cung cấp dịch vụ giao vận. Tầng 5 -> 7 sử dụng dịch vụ giao vận.

➢ *Các hàm dịch vụ của tầng giao vận có kết nối:*

Ngoài phần giao thức chuẩn, ISO còn định nghĩa các dịch vụ mà tầng giao vận cung cấp cho các thực thể ở tầng Phiên trong trường hợp có liên kết, dưới dạng một tập hợp các hàm dịch vụ nguyên thủy *(services primitives)* như sau:

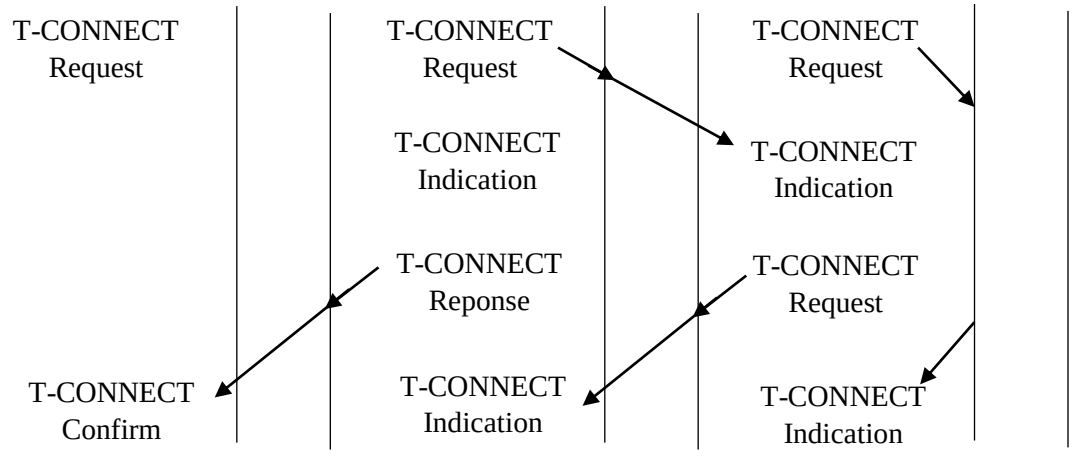
N-CONNECT.Request (callce, caller, exp wanted, qos, user data)
N-CONNECT.Indication (callce, caller, exp wanted, qos, user data)
N-CONNECT.Response (qos, responder, exp wanted, user data)
N-CONNECT.Config (qos, responder, exp wanted, user data)
N-DISCONNECT.Request (user data)
N-DISCONNECT.Indication (reason, user data)
N-DATA.Request (user data)

N-DATA.Indication (reason, user data)
N-EXPEDITED-DATA.Request (user data)
N-EXPEDITED-DATA.Indication reason, (user data)

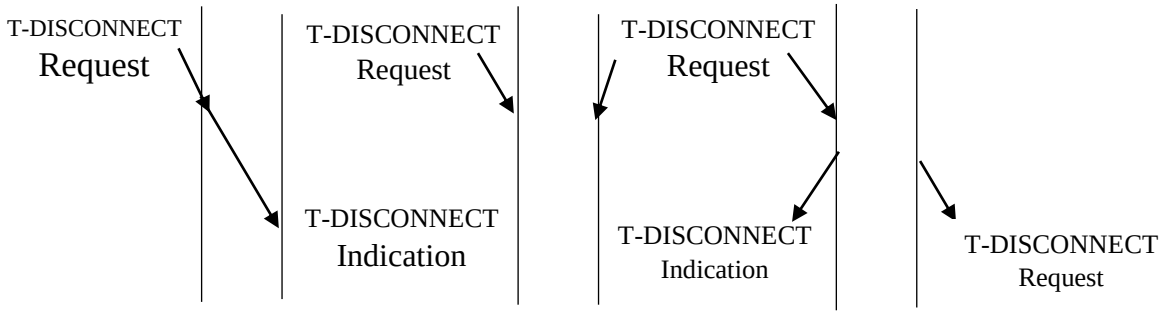
- *Các hàm dịch vụ của tầng giao vận không có kết nối:* Chỉ có hai hàm dịch vụ được định nghĩa:

  T-UNITDATA.request (callce, caller, qos, user data)
  Y-UNITDATA.Indication (callce, caller, qos, user data)

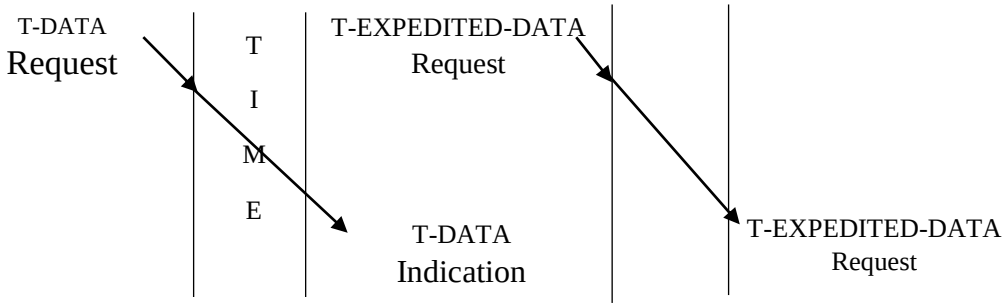
- *Quan hệ giữa các hàm OSI nguyên thủy*: Quá trình nối, tách và trao đổi dữ liệu diễn ra như sau:



(a) Chấp nhận (b) Từ chối bởi bên được gọi (c) Từ chối bởi tầng giao vận



(d) Bình thường (e) Đồng thời tách cả hai phía (f) Tách tầng giao vận



(g) Bình thường (h) Gửi số liệu khẩn

Hình 2.11 Quan hệ giữa các hàm OSI nguyên thủy

Giải thích:

(a) Quá trình nối được chấp nhận.

(b) Quá trình nối bị từ chối bởi bên được gọi.

(c) Quá trình nối bị từ chối bởi tầng giao vận do lỗi của người sử dụng hoặc người cung cấp dịch vị giao vận gây nên.

(d) Quá trình tách bình thường.

(e) Quá trình tách đồng thời cả hai phía.

(f) Quá trình tách từ tầng giao vận.

(g) Quá trình trao đổi dữ liệu bình thường.

(h) Quá trình trao đổi dữ liệu khẩn.

Trong hình (c) việc từ chối có thể do lỗi của người sử dụng hoặc người cung cấp dịch vụ giao vận gây nên. Khi đó, không có gì được phát qua mạng vì vậy đầu kia không nghe được gì cả. Có những qui tắc cho người sử dụng hàm dịch vụ giao vận.

Ví dụ, không được dùng hàm T-DISCONNECT.Request khi tiếp nối chưa được thiết lập.

- *Chất lượng dịch vụ Qos(Quanlity of Service)*

Chức năng cơ bản của tầng 4 là tăng cường chất lượng dịch vụ được cung cấp bởi tầng 3. Nếu lớp chất lượng chưa tốt, tầng giao vận sẽ khắc phục khoảng ngăn cách giữa những gì mà người sử dụng tầng giao vận muốn và những gì mà lớp mạng cung cấp. Các tham số chất lượng dịch vụ Qos bao gồm:

- ✓ *Thời gian thiết lập liên kết* là thời gian từ khi gởi yêu cầu tới thời điểm nhận được xác nhận liên kết.
- ✓ *Xác nhận không thành công của thiết lập liên kết*: là tỷ lệ yêu cầu liên kết không được chấp nhận trong một thời hạn tới đa.
- ✓ *Lưu lượng của liên kết* do số byte hữu ích có thể truyền trong một giây, lưu lượng được tính trong một cuộc trao đổi hoặc dựa vào khả năng của mạng theo 2 chiều.
- ✓ *Thời gian trể (độ trể truyền dẫn)* là khoảng thời gian giữa thời điểm mà ngườisử dụng dịch vụ của tầng giao vận bên phát gởi thông tin báo tới thời điểm thực thể của tầng giao vận bên thu nhận được. Đánh giá theo 2 chiều.
- ✓ *Tỷ lệ lỗi* là tỷ số giữa tin báo bị lỗi (hoặc mất) trên tổng số tin báo được truyền trong một chu kỳ định trước.
- ✓ *Xác nhận sự cố truyền*:tỷ số giữa thời gian có sự cố với thời gian cả chu kỳ quan sát.
- ✓ *Thời gian hủy liên kết* là thời gian từ khi một người sử dụng phát yêu cầu hủy liên kết đến khi liên kết được hủy thật sự tại thiết bị đầu cuối từ xa.
- ✓ *Xác suất lỗi* khi hủy liên kết là tỷ lệ số yêu cầu hủy liên kết không được thực hiện trong thời gian lớn nhất.
- ✓ *Khả năng bảo vệ* là khả năng của người sử dụng cấm thiết bị đầu cuối bên ngoài truy nhập bất hợp pháp hay thay đổi dữ liệu truyền.

- ✓ *Thông số ưu tiên* cho phép người sử dụng có quyền ưu tiên được phục vụ cao hơn đối với một liên kết.
- ✓ *Thông số hủy bỏ* cho phép tầng giao vận tự quyết định hủy liên kết khi có tắc nghẽn hay các vấn đề bên trong mạng.

Người sử dụng khi yêu cầu liên kết sẽ gởi tất cả các thông số với các giá trị yêu cầu tới tầng giao vận và bắt đầu quá trình đàm thoại với các thông số đó.

So sánh các hàm cơ bản của dịch vụ giao vận với dịch vụ mạng, ta thấy các dịch vụ mạng và giao vận giống nhau. Sự khác nhau là dịch vụ mạng cho phép người sử dụng xử lý Acknowledgement và N-ROSOTS. Ngược lại, dịch vụ giao vận không quan tâm đến vì dịch vụ lớp giao vận là tin cậy, không có lỗi. Dịch vụ mạng được dùng bởi tầng giao vận.

➢ *Các lớp giao thức của tầng giao vận*

Các dịch vụ tầng giao vận bảo đảm bằng các giao thức giữa 2 thực thể của tầng cũng tương tự như giao thức của tầng liên kết dữ liệu nó giải quyết vấn đề lỗi, điều khiển lưu lượng và bảo đảm trình tự gói tin.

Tầng liên kết dữ liệu, hai IMP truyền tin trực tiếp qua đường kênh vật lý. Ở tầng giao vận, đường kênh vật lý này được thay bằng subnet. Sự khác nhau này kéo theo sự khác nhau về xây dựng các thủ tục. Ở tầng giao vận phải xác định địa chỉ nơi nhận, ở tầng liên kết dữ liệu thì không cần vì chỉ có một đường truyền tin giữa hai điểm. Quá trình kết nối ở tầng giao vận cũng phức tạp hơn ở tầng liên kết dữ liệu.

Tầng giao vận đòi hỏi khả năng lưu trữ trong mạng để giữ những gói tin bị sự cố và đòi hỏi thủ tục đặc biệt. Tầng giao vận số các kết nối lớn hơn nên các vấn đề bộ đệm và điều khiển dòng phức tạp hơn.

Từ quan điểm thiết kế thủ tục giao vận, các dịch vụ được cho bởi mạng quan trọng hơn các tính chất thực tế của mạng, mặc dù cái sau bị ảnh hưởng mạnh bởi cái trước. Tuy vậy, trong một phạm vi nào đó, dịch vụ mức mạng có thể che những mặt ít được chú ý của mạng và cung cấp ghép nối tốt hơn. Để tiện lợi xem xét các thủ tục giao vận, ta chia các dịch vụ trên mạng thành 3 nhóm:

Nhóm	**Ý nghĩa**
Nhóm A	✓Hoàn thiện, tỷ lệgói tin bị mất, trùng lắp hoặc bị hỏng không đáng kể ✓Lệnh N-RESET có thể bỏ qua ✓Tầng giao vận đơn giản, không cần các dịch vụ phục hồi và sắp xếp lại thứ tự gói tin ✓Thường là mạng cục bộ
Nhóm B	✓Gói tin bị mất, nhưng kiểm soát được ✓Thỉnh thoảng tầng mạng gởi lệnh N-RESET do tắc nghẽn, hỏng phần cứng, vấn đề phần mềm ✓Thông thường là mạng đường dài ✓Các giao thức giao vận có nhiệm vụ: + Thiết lập liên kết, đồng bộ lại.

	+ Theo dõi toàn bộ yêu cầu khởi động lại cho NSD
Nhóm C	✓Truyền tin không tin cậy, không liên kết ✓Mạng đường dài, kết nối nhiều mạng con ✓Giao thức của tầng giao vận phức tạp, phải có khả năng phục hồi lỗi khi xảy ra sự cố và sắp xếp lại thứ tự các gói tin.

Dịch vụ mạng xấu thì giao thức của tầng giao vận sẽ phức tạp hơn. ISO đã nhận thức vấn đề này và chia giao thức của tầng giao vận thành năm lớp ứng với các loại mạng như sau:

Lớp	Ý nghĩa
Lớp 0 Mạng loại A	✓Lớp thủ tục đơn giản ✓Kết nối mạng khi có yêu cầu giao vận không phải giải quyết lỗi ✓Chủ yếu tạo ra trình tự, điều khiển dòng dữ liệu để tầng mạng hoạt động tốt ✓Bao gồm cơ cấu thiết lập và hủy liên kết ở tầng giao diện
Lớp 1 Mạng loại B	Có tính chất tương tự lớp 0, ngoài ra còn có thêm: ✓Khởi động lại mạng sau khi N-RESET, giao thức có khả năng báo nhận (ACK) và truyền dữ liệu khẩn. ✓Đồng bộ lại và sau đó nối lại liên lạc giữa các thực thể giao vận đã bị gián đoạn. ✓Lớp 1 không kiểm tra lỗi và kiểm soát dòng dữ liệu
Lớp 2 Mạng loại A	Lớp 2 là phiên bản của lớp 0 và được xây dựng cho mạng tin cậy và có thêm một số chức năng như sau: ✓Sự ghép kênh: hai hay nhiều liên kết của tầng giao vận có thể dùng chung một kết nối ở tầng mạng ✓Sử dụng khi nhiều liên kết ở tầng giao vận được mở đồng thời, nối liên kết có lưu lượng nhỏ. Ví dụ hệ thống đặt vé máy bay cho phép tiết kiệm đường truyền.
Lớp 3 Mạng loại B	Là tổ hợp lớp 1 và lớp 2 ✓Cho phép dồn kênh ✓Khởi động lại ✓Điều khiển dữ liệu
Lớp 4 Mạng loại C	Lớp 4 có hầu hết chức năng của lớp trước và bổ sung một số khả năng kiểm soát luồng dữ liệu ✓Phải có biện pháp giải quyết vấn đề mất gói tin, gói tin bị hỏng ✓Phải giải quyết yêu cầu khởi động lại ✓Thủ tục giao vận phức tạp nhất

- *Thủ tục giao vận trên X.25*

Các hàm dịch vụ cơ bản:

Các hàm dịch vụ cơ bản được thực hiện bằng các chương trình con minh họa bằng ngôn ngữ Pascal.

1. Hàm Connect thực hiện T-CONNECT.request

   connum = CONNECT (local, remote)

Hàm dịch vụ này thiết lập kết nối giao vận giữa 2 máy. Nếu kết nối thành công, hàm trả về một số dương, ngược lại hàm trả về số âm.

2. Hàm Listen thực hiện T-CONNECT.indication

   connum = LISTEN (local)

Hàm này dùng để thông báo tiếp nhận yêu cầu kết nối

3. Hàm Disconnect thực hiện T-DISCONNECT.request

   status = DISCONNECT (commun)

Hàm này dùng để kết thúc kết nối, tham số commun cho biết kết nối nào sẽ bị ngắt, kết quả thực hiện sẽ được gán cho biến status với giá trị OK hoặc error

4. Hàm Send thực hiện T-DATA.request

   status = ESND (commun, buffer, bytes)

Hàm này để phát nội dung của bufer với kích thước là bytes cho số kết nối đặt ở commun. Kết quả đặt ở status.

5. Hàm Receive thực hiện T-DATA.indication

   status = RECEIVE (commun, buffer, bytes)

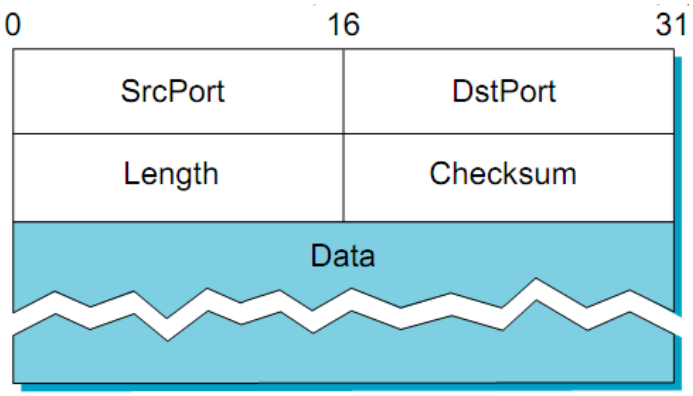
Hàm này để nhận tin vào buffer với kích thước là giá trị biến bytes. Kết quả thực hiện đặt vào status giá trị OK hoặc error.

c) Tầng vận chuyển trong mạng Internet

Tầng vận chuyển trong Internet cũng hỗ trợ hai phương thức hoạt động không nối kết và có nối kết với hai giao thức liên lạc tương ứng là UDP và TCP.

- *Giao thức UDP (User Datagram Protocol)*

UDP là dịch vụ truyền dữ liệu dạng không nối kết. Không có thiết lập nối kết giữa hai bên truyền nhận, do đó gói tin UDP (segment) có thể xuất hiện tại nút đích bất kỳ lúc nào. Các segment UDP tự thân chứa mọi thông tin cần thiết để có thể tự đi đến đích. Khuôn dạng của chúng như sau:



Hình 2.12 Khuôn dạng của một segment UDP

Giải thích:

- *SrcPort:* Địa chỉ cổng nguồn, là số liệu của tiến trình gởi gói tin đi.
- *DstPort:* Địa chỉ cổng đích, là số liệu của tiến trình sẽ nhận gói tin.
- *Length:* Tổng chiều dài của segment, tính luôn cả phần header.
- *Checksum:* Là phần kiểm tra lỗi. UDP sẽ tính toán phần kiểm tra lỗi tổng hợp trên phần header, phần dữ liệu và cả phần header ảo. Phần header ảo chứa 3 trường trong IP header: địa chỉ IP nguồn, địa chỉ IP đích và trường chiều dài UDP. Phương thức tính toán như sau:

```
U_short
Cksum (u_short *buf, int count)
{
        Register u_long sum = 0;
        While (count--)
        {
                Sum += *buf++;
                If (sum & 0xFFFF0000)
                {
                        Sum &=0xFFFF;
                        Sum++;
                }
        }
Return (sum & 0xFFFF);
}
```

Xem thông điệp là một chuỗi các số nguyên 16 bits. Cộng dồn các số nguyên này từng bit một. Kết quả cộng dồn cuối cùng chính là phần kiểm tra lỗi.

Data: Phần dữ liệu hai bên gửi cho nhau.

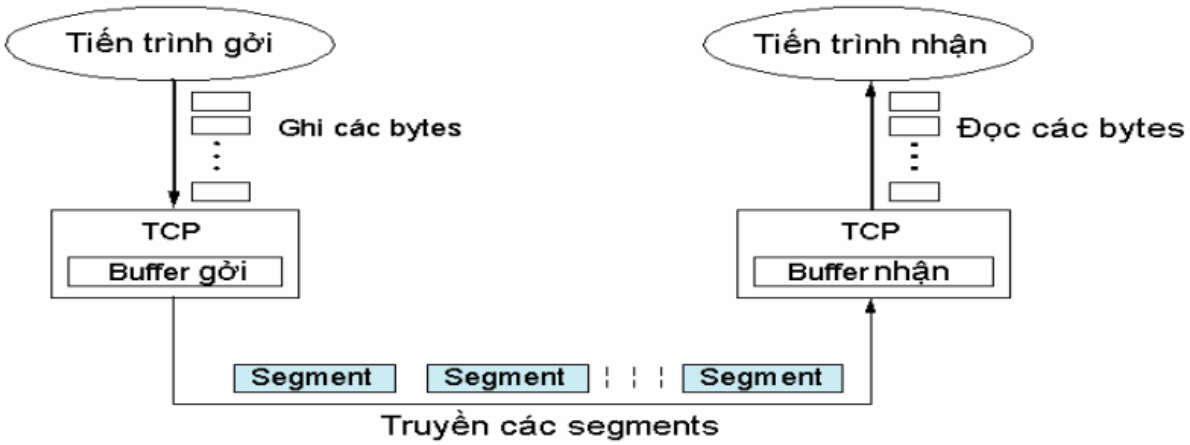
UDP hoạt động không tin cậy, vì:

- Không có báo nhận dữ liệu từ trạm đích.
- Không có cơ chế phát hiện mất gói tin hoặc gói tin đến không theo thứ tự.
- Không có cơ chế tự động gửi lại những gói tin bị mất.
- Không có cơ chế điều khiển luồng dữ liệu và do đó có thể bên gửi sẽ làm ngập bên nhận.

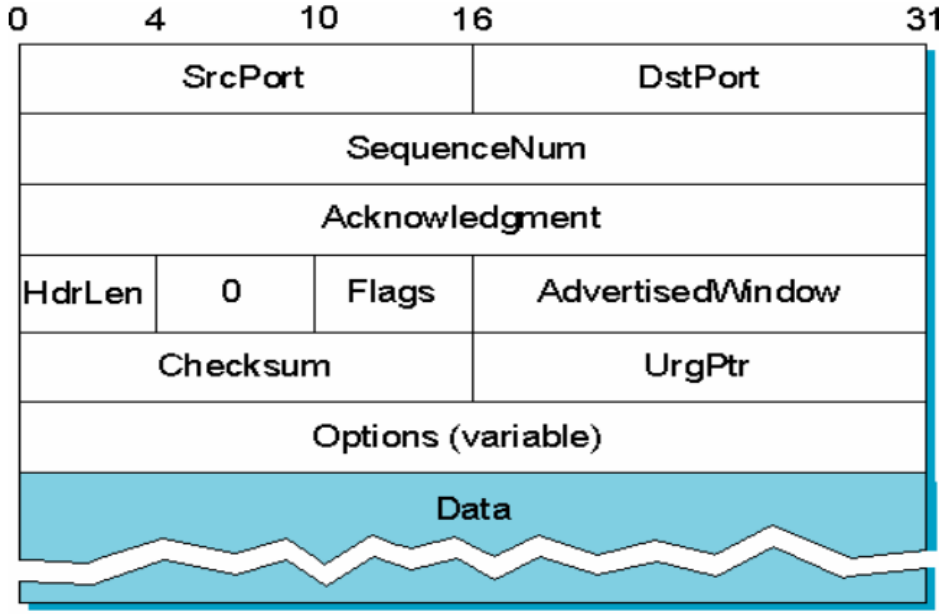
➢ *Giao thức TCP (Transmission Control Protocol)*

Ngược lại với giao thức UDP, TCP là giao thức vận chuyển tinh vi hơn, dùng để cung cấp dịch vụ vận chuyển tin cậy, hướng nối kết theo kiểu truyền thông tin bằng cách phân luồng các bytes. TCP là giao thức truyền hai hướng đồng thời, nghĩa là một nối kết hỗ trợ hai luồng bytes chạy theo hai hướng. Nó cũng bao gồm một cơ chế điều

khiển thông lượng cho mỗi luồng bytes này, để cho phép bên nhận giới hạn lượng dữ liệu mà bên gửi có thể truyền tại một thời điểm nào đó. TCP cũng hỗ trợ cơ chế đa hợp, cho phép nhiều tiến trình trên một máy tính có thể đồng thời thực hiện đối thoại với đối tác của chúng



Hình 2.13 Cách thức TCP quản lý luồng các bytes



Hình 2.14 Khuôn dạng TCP header

2.6.2.5 TẦNG PHIÊN (SESSION)

a) Vai trò và chức năng của tầng phiên

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

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

- Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách lôgic) các phiên (hay còn gọi là các hội thoạidialogues)
- Cung cấp các điểm đồng bộ để kiểm soát việc trao đổi dữ liệu.

- Áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.
- Cung cấp cơ chế "lấy lượt" (nắm quyền) trong quá trình trao đổi dữ liệu.

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

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

Tầng giao dịch có các hàm cơ bản sau:

- *Give Token* cho phép người sử dụng chuyển một token cho một người sử dụng khác của một liên kết giao dịch.
- *Please Token* cho phép một người sử dụng chưa có token có thể yêu cầu token đó.
- *Give Control* dùng để chuyển tất cả các token từ một người sử dụng sang một người sử dụng khác.

b) Dịch vụ OSI cho tầng phiên

Tầng phiên làm việc quản lý các cuộc thoại giữa hai máy tính bằng cách thiết lập, quản lý và kết thúc các phiên truyền thông

➢ *Cung cấp cho người sử dụng dịch vụ tầng phiên (SS-user):*

- ✓ Thiết lập một liên kết với một người sử dụng dịch vụ tầng phiên khác, trao đổi dữ liệu với người sử dụng đó một cách đồng bộ và hủy bỏ liên kết một cách có trật tự khi không dùng đến nó nữa.
- ✓ Thương lượng về việc dùng các thẻ bài (Token) để trao đổi dữ liệu, đồng bộ hóa và hủy bỏ liên kết, sắp xếp các phương thức trao đổi dữ liệu (half-duplex hoặc full-duplex).
- ✓ Thiết lập các điểm đồng bộ hóa trong các hội thoại và khi xảy ra sự cố thì có thể khôi phục lại việc hội thoại bắt đầu từ một điểm đồng bộ hóa đã thỏa thuận.
- ✓ Ngắt hội thoại và khôi phục hội thoại sau đó từ một điểm xác định trước:
    - Các điểm đồng bộ hóa có thể phân tách các phần của một hội thoại.
    - Các điểm đồng bộ hóa có thể dùng để phục hồi lỗi.

Các điểm đồng bộ hóa chính: dùng để cấu trúc quá trình trao đổi dữ liệu thành một chuỗi các đơn vị hội thoại (dialogue), mỗi điểm này phải được xác nhận và người sử dụng sẽ bị hạn chế trong một số dịch vụ nhất định cho tới khi nhận được một sự xác nhận mới. Một điểm đồng bộ hóa chính được dùng để tách biệt các loại đơn vị hội thoại liên tiếp.

Các điểm đồng bộ hóa phụ: được dùng để cấu trúc quá trình trao đổi dữ liệu ở trong một đơn vị hội thoại và các điểm này không cần phải được xác định trước. Việc

dùng các điểm đồng bộ hóa phụ trong quá trình truyền tập nó sẽ ngăn chặn việc truyền lại dữ liệu với một khối lượng lớn.

Một đơn vị hội thoại: là một hành động nguyên tử trong đó mọi hành động truyền thông không liên quan gì đến bất kỳ một hoạt động truyền thông nào trước và sau đó. Một hành động bao gồm nhiều đơn vị hội thoại và đây cũng chính là một tập hợp logic các nhiệm vụ liên quan với nhau; ở một thời điểm thì chỉ có một hành động trên một liên kết phiên nhưng một hành động thì có thể diễn ra trên nhiều liên kết phiên, nó có thể bị ngắt và sau đó có thể khôi phục lại trong một liên kết phiên khác, một vòng đời của một liên kết phiên thì có thể có nhiều hành động liên tiếp.

- *Điều khiển trao đổi dữ liệu*

Việc trao đổi dữ liệu thực hiện một trong ba phương thức như sau: hai chiều đồng thời (full-duplex), hai chiều luân phiên (haft-duplex), một chiều (simplex)

- *Điều hành phiên làm việc*

Phiên làm việc (session) là một cuộc thoại chính thức giữa một bên yêu cầu dịch vụ và một bên cung cấp dịch vụ. Các phiên làm việc thường có ít nhất ba giai đoạn:

Thiết lập tuyến liên kết: Bên yêu cầu dịch vụ sẽ yêu cầu khởi phát một dịch vụ. Trong quá trình xác lập, phiên truyền thông được thiết lập và các quy tắc được thỏa thuận.

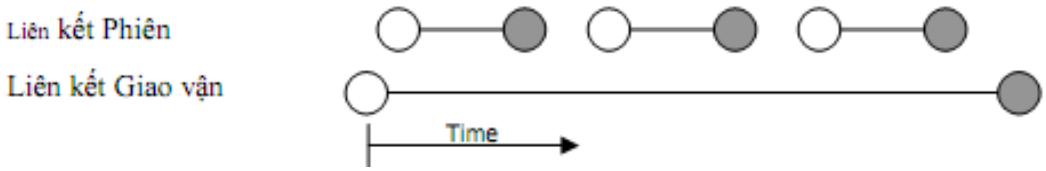
Chuyển giao dữ liệu: Do các quy tắc được thỏa thuận trong khi xác lập, nên mỗi bên của cuộc thoại sẽ biết nội dung mong đợi. Phiên truyền thông sẽ hữu hiệu và các lỗi cũng dễ phát hiện.

Giải phóng các kết nối: Khi hoàn tất phiên làm việc, cuộc thoại kết thúc theo trật tự.

- ***Liên kết phiên***

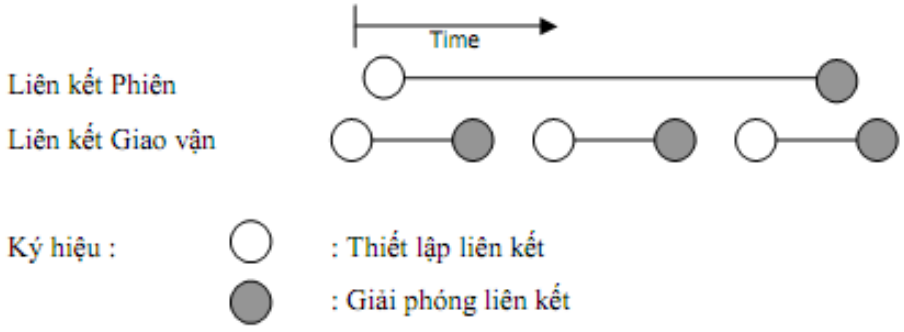
Tầng phiên thực hiện đặt tương ứng liên kết phiên với các liên kết giao vận. Trong quá trình liên kết có thể xảy ra 2 trường hợp:

1) Một liên kết giao vận thiết lập với nhiều liên kết phiên liên tiếp:



Hình 2.15 Liên kết giao vận thiết lập với nhiều liên kết phiên liên tiếp

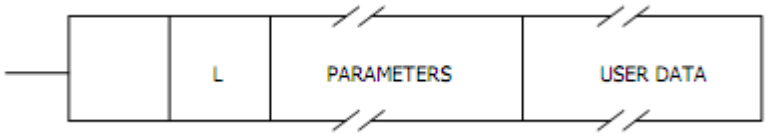
2) Nhiều liên kết giao vận sử dụng cùng một liên kết phiên



Hình 2.16 Nhiều liên kết giao vận sử dụng cùng một liên kết phiên

c) Giao thức chuẩn tầng phiên

Giao thức chuẩn tầng phiên sử dụng tới 34 loại đơn vị dữ liệu (SPDU) khác nhau và có khuôn dạng tổng quát như sau:



Hình 2.17 Khuôn dạng tổng quát

Trong đó:

- SI: Định danh của loại SPDU (một trong 34 loại)
- LI (length inciator): Chỉ độ dài của vùng tham số (parameters)
- PARAMETERS: vùng khai báo các tham số SPDU, mỗi loại SPDU có danh sách tham số riêng. Mỗi tham số được khai báo dưới dạng tổng quát gồm 3 vùng con: parameter indentifier, length indecation, parameter value và chúng được gọi theo đơn vị pi hoặc PGI (mỗi đơn vị PGI gồm có 3 vùng con: PGI, LENGTH INDICATION, PARAMETER VALUE).
- User data: chứa dữ liệu của người sử dụng.

➢ *Các loại SPDU, các tham số và chức năng:*

SPDU	PARAMETERS	FUNCTION
CONNECT	Connection ID, Protocol Options, Version number, Serial Number, Token setting, Maximum TSDU size,Requirements, Calling SSAP, Called SSAP, user data	Initiate session Connection
ACCEPT	Same as CONNECT SPDU	Etablist SESSION CONNECTION
REFUSE	Connection ID, Transport disconnect, Requirement, Version number, Season	Reject connection release
FINISH	Transport Disconnect, User Data	Initiate Order Release
DISCONNECT	User Data	Acknowledged orderly release
NOT FINISHED	User Data	Reject Orderly Release
ABORT	Transport disconnect, Protocol Error Code, User Data	Abormal connection release
ABORT ACCEPT	Transport disconnect, Protocol Error Code, User	Acknowledge Abort

	Data	
DATA TRANSFER	Enclosure item, user Data	Tranfer normal data
EXPEDITED	User Data	Tranfer typed data
CAPABILITY DATA ACK	User Data	Acknowlege Capability data
GIVE TOKENS	Tokens	Tranfer tokens
PLEASE TOKENS	Tokens, User data	Request token Asignment
GIVE TOKENS CONFIRM	-	Transfer all tokens
GIVE TOKENS ACK	-	Acknowlege all tokens
MAJOR SYNS POINT	Confirm required flag, Serial number, User data	Define minor sync point
MINOR SYNC ACK	Serial number, user data	Acknowlege minor sync point
MAJOR SYNC POINT	End of activity flag, serial number, user data	Define major sync point
MAJOR SYNC ACK	Serial number, user data	Acknowlege major sync point
RESYNCHRONIZED	Tokens setting, resync type, serial number, user data	Resynchorize
RESYNCHRONIZED ACK	Tokens setting, Serial number, User Data	Acknowledge resynchronize
PREPERE	Type	Notify type SPDU is coming
EXCEPTION REDORT	SPDU bit pattem	Protocol Error detected
EXCEPTION DATA	Reason, User data	Put protocol in Error state
ACTIVITY START	Acitvity ID, user data	Signal beginning of activity
ACTIVITY RESUME	Connect ID, Old activity ID, new Activity ID, user data	Signal resumption of activity
ACTIVITY INTERRUPT	Reason	Interrup activity
ACTIVITY INTERRUPT ACK	-	Acknowlege interrupt
ACITVITY DISCARD	Reason	Cancel activity
ACTIVITY DISCARD	-	Acknowlege cancellation

ACK		
ACTIVITY END	Serial number/User Data	Signal activity end
ACTIVITY END ACK	Serial number/User Data	Acknowlege activity end

Tầng phiên đóng một vai trò quan trọng trong việc trao đổi thông tin giữa các máy client với máy server. Nhưng thông tin mà chúng cần truyền tải thì được chia nhỏ ra thành các khung (hay gói) trước khi chúng được truyền tải qua một mạng. Mỗi tầng của mô hình 7 tầng OSI đều có thể bổ sung thêm các thông tin vào đầu đoạn và đoạn cuối của một khung dữ liệu và sau đó các thông tin này sẽ được đọc bởi tầng tương đương ở máy trạm tiếp theo. Và một số tầng khác có thể bổ sung thêm phần đầu (header) và cả phần đuôi (*trailer*) vào khung dữ liệu có sẵn. Sau đó, khung dữ liệu này truyền chuyển tới tầng tương đương trên trạm tiếp nhận.

2.6.2.6 Tầng trình diễn (Presentation)

Tầng trình diễn có nhiệm vụ là phân cách giữa các tầng cao hơn và các tầng thấp hơn từ định dạng dữ liệu của tầng ứng dụng, chuyển đổi định dạng dữ liệu từ định dạng của tầng ứng dụng thành định dạng thông thường, gọi là "trình diễn hợp với quy tắc". Tầng trình diễn xử lý dữ liệu không phụ thuộc vào máy tính từ tầng ứng dụng thành dữ liệu có định dạng phụ thuộc vào máy tính để chuyển cho các tầng thấp hơn.

Tầng trình diễn xử lý cú pháp, hoặc các quy tắc văn phạm cần thiết cho phiên truyền thông giữa hai máy tính, bảo đảm cho các hệ thống cuối truyền thông có kết quả khi chúng sử dụng các dạng biểu diễn dữ liệu khác nhau. Tầng này trình bày một dạng dữ liệu đồng dạng cho tầng ứng dụng.

a) Vài trò và chức năng của tầng trình diễn

Mục đích của tầng trình diễn là đảm bảo cho các hệ thống cuối có thể truyền thông tin có kết quả ngay cả khi chúng sử dụng các biểu diễn dữ liệu khác nhau. Để đạt được điều đó nó cung cấp một biểu diễn chung để dùng trong truyền thông và cho phép chuyển đổi từ biểu diễn cục bộ sang biểu diễn chung đó.

Tồn tại 3 dạng cú pháp thông tin được trao đổi giữa các thực thể ứng dụng:

- ✓ Cú pháp dùng bởi thực thể ứng dụng nguồn.
- ✓ Cú pháp dùng bởi thực thể ứng dụng đích
- ✓ Cú pháp dùng bởi giữa các thực thể trình diễn, loại cú pháp này gọi là cú pháp truyền (transfer syntax)

Tầng trình diễn đảm nhận việc chuyển đổi biểu diễn thông tin giữa cú pháp truyền và mỗi một cú pháp kia khi có yêu cầu.

Chú ý rằng không tồn tại một cú pháp truyền xác định trước duy nhất cho mọi hoạt động trao đổi dữ liệu. Cú pháp truyền được duy nhất cho mọi hoạt động. Cú pháp truyền được sử dụng trên một liên kết cụ thể của tầng trình diễn phải được thương lượng giữa các thực thể trình diễn tương ứng. Mỗi bên lựa chọn một cú pháp truyền sao cho có thể sẵn sàng được chuyển đổi sang cú pháp người sử dụng và ngược lại. Ngoài ra cú pháp truyền được chọn phải phản ánh các yêu cầu dịch vụ khác chẳng hạn nhu cầu nén dữ liệu. Việc thương lượng cú pháp truyền sử dụng có thể thay đổi trong vòng đời liên kết đó. Tầng trình diễn chỉ liên quan đến cú pháp truyền vì thế trong giao thức sẽ không quan tâm đến các cú pháp sử dụng bởi thực thể ứng dụng. Tuy nhiên

mỗi thực thể trình diễn phải chịu trách nhiệm chuyển đổi giữa cú pháp người sử dụng và cú pháp truyền.

Phiên dịch dữ liệu

Một mục tiêu quan trọng cần giải quyết khi thiết kế các mạng đó là cho phép kiểu máy tính khác nhau trao đổi dữ liệu. Tuy mục tiêu này ít khi được giải quyết toàn vẹn, nhưng việc vận dụng hiệu quả các kỹ thuật phiên dịch dữ liệu có thể giúp nhiều kiểu máy tính truyền thông với nhau. Có 4 dạng phiên dịch dữ liệu, thứ tự bit, thứ tự byte, mã ký tự và cú pháp tập tin như sau:

- ✓ Thứ tự bit: Khi số nhị phân được truyền qua một mạng, chúng gởi đi theo từng bít, thứ tự byte, mã ký tự và cú pháp tập tin.
- ✓ Phiên dịch thứ tự byte: Các giá trị phức tạp thường phải biểu thị bằng nhiều byte, nhưng các máy tính khác nhau thường dùng quy ước khác nhau về việc sẽ truyền byte nào trước. Các bộ vi xử lý Intel bắt đầu bằng byte ít quan trọng nhất.
- ✓ Phiên dịch mã ký tự: hầu hết các máy tính đều dùng một trong các bảng mã đánh số nhị phân để biểu thị các bộ ký tự: bảng mã ASCII được dùng để biểu thị các ký tự tiếng Anh trên tất cả các máy tính và hầu hết các máy tính mini; EBCDIC (Extended Binary Coded Decimal Interchange Code = Mã hoán đổi thập phân mã hóa nhị phân mở rộng) được dùng để biểu thị cho các ký tự tiếng Anh trên máy tính lớn nhất.
- ✓ Phiên dịch cú pháp tập tin: Khi các dạng thức tập tin khác nhau giữa các máy tính, các dạng đó đòi hỏi phải phiên dịch.

b) Dịch vụ OSI cho tầng trình diễn

Dịch vụ OSI cho tầng trình diễn có 2 loại: một loại bao gồm các dịch vụ liên quan đến biểu diễn của dữ liệu người sử dụng để đảm bảo cho hai thực thể ứng dụng có thể trao đổi dữ liệu thành công ngay khi chúng dùng các biểu diễn cục bộ khác nhau cho dữ liệu đó, loại thứ 2 bao gồm các dịch vụ cho phép các thực thể ứng dụng có thể sử dụng các dịch vụ tầng phiên để quản lý hội thoại.

Để cung cấp loại dịch vụ thứ nhất tầng trình diễn phải thực hiện hai nhiệm vụ sau:

- ✓ Thương lượng về cú pháp truyền: với mỗi kiểu dữ liệu người sử dụng cho trước một cú pháp truyền được thương lượng.
- ✓ Chuyển đổi: dữ liệu cung cấp bởi người sử dụng để chuyển đổi thành biểu diễn theo cú pháp truyền để truyền đi, ngược lại dữ liệu nhận được để giao cho người sử dụng sẽ chuyển đổi từ biểu diễn theo cú pháp truyền sang biểu diễn của người sử dụng.

Ở một thời điểm bất kỳ trong vòng đời của một liên kết trình diễn dịch vụ trình diễn có liên quan đến một hoặc nhiều bối cảnh trình diễn (presentation context). Mỗi bối cảnh chỉ rõ cú pháp trừu tượng của dữ liệu đó. Có hai loại bối cảnh được sử dụng:

- ✓ *Defined context set:* Bao gồm các bối cảnh đã được xác định thông qua sự thỏa thuận giữa người sử dụng dịch vụ trình diễn *(presentation service user)* và người cung cấp dịch vụ trình diễn *(presentation service provider).*

- ✓ *Default context:* là một bối cảnh trình diễn mà người cung cấp dịch vụ trình diễn luôn luôn biết rõ và người sử dụng khi vắng mặt.

Ở tầng phiên do kiến trúc phân tầng của ISO các thực thể ứng dụng không thể truy cập trực tiếp tới các dịch vụ tầng phiên, do vậy các yêu cầu dịch vụ liên quan đến tầng phiên phải được chuyển qua tầng trình diễn đến các dịch vụ tầng phiên.

c) Các giao thức chuẩn tầng trình diễn

Giao thức chuẩn của ISO/CCITT cho tầng trình diễn đặc tả những nội dung chính sau:

- ✓ Cấu trúc và mã hóa các đơn vị dữ liệu của giao thức trình diễn (PPDU) dùng để truyền dữ liệu và thông tin điều khiển.
- ✓ Các thủ tục để truyền dữ liệu và thông tin điều khiển giữa các thực thể trình diễn của hai hệ thống mở.
- ✓ Liên kết giữa giao thức trình diễn với dịch vụ trình diễn và với dịch vụ phiên.

Cũng như các PDU ở các tầng khác nhau, các PPDU cũng có khuôn dạng tổng quát bao gồm một phần đầu (header) chứa các thông tin điều khiển và có thể thêm một phần chứa dữ liệu được truyền từ trên xuống hoặc được truyền lên cho tầng trên.

Qua xem xét các tầng dưới từ tầng phiên trở xuống, chúng ta thấy có 2 nguyên lý sau đây luôn được tuân thủ:

- ✓ Mỗi dịch vụ tầng n được cài đặt nhờ trao đổi các nPDU
- ✓ Mỗi nPDU trở thành User data và được đưa vào trong một (n-1)PDU.

Tuy nhiên ở tầng trình diễn (và cả tầng ứng dụng), các nguyên lý đó không còn luôn luôn được áp dụng. Thực tế là không phải mọi dịch vụ trình diễn đều yêu cầu các PPDU và một số tham số của một số PPDU không được chuyển thành User data trong một SPDU. Để giải thích động cơ của sự khác biệt đó, ta xem xét hai dịch vụ trình diễn: Thiết lập liên kết và chuyển thẻ bài (token passing).

Khi phát triển các giao thức cho 3 tầng cao của mô hình OSI, người ta thấy rõ ràng nên thương lượng và thiết lập đồng thời các liên kết phiên, trình diễn và ứng dụng mặc dù đều đó đòi hỏi một quan hệ 1 – 1 chặt chẽ (không có dồn kênh) với cùng vòng đời cho cả 3 loại liên kết. Quá trình thiết lập đồng thời các liên kết đó được gọi là quá trình nhúng, vì các PDU CONNECT.request và CONNECT.response cho cả ba tầng cao đó, cái này được nhúng vào trong cái kia.

Các chuẩn khác cho tầng trình diễn

Ngoài các chuẩn về dịch vụ và giao thức cho tầng trình diễn như đã trình bày ở trên, ISO và CCIT đã phát triển các chuẩn liên quan đến cú pháp trừu tượng *(Abstract Syntas)* và quy tắc mã hóa (*Encoding Rules*) mà chúng ta đã nói đến khi trình bày vai trò và chức năng của tầng trình diễn.

Các chuẩn của ISO gồm có:

- ✓ ISO 8824: *Abstract Syntax Notation One* (Viết tắt là ISNI.1).
- ✓ ISO 8825: *Basic Encoding Rules* (Viết tắt là BER).
- ✓ Tương tự CCITT có khuyến nghị X.208 (ANSI.1) và X.209 (BER).

Khái niệm cú pháp trừu tượng mà ISO và CCITT định nghĩa được dựa trên khái niệm kiểu dữ liệu (data type) mà chúng ta đã quan thuộc trong các ngôn ngữ lập trình

phổ biến. Thông thường các ngôn ngữ này định nghĩa trước các kiểu dữ liệu đơn giản như integer và boolean, cùng với phương thức tổ hợp các kiểu đơn giản đó để có các cấu trúc dữ liệu phức tạp hơn. Hơn nữa, các phương pháp tổ hợp có thể thực hiện một cách đệ quy cho phép tạo ra các kiểu phức tạp tùy ý.

2.6.2.7 Tầng ứng dụng (Application)

Tầng ứng dụng giao tiếp trực tiếp với người sử dụng. Nhiệm vụ của tầng ứng dụng là hiển thị các thông tin nhận được và gửi các thông tin mới của người sử dụng cho các tầng thấp hơn.

Tầng ứng dụng liên quan đến tiến trình cung cấp các dịch vụ trên mạng, các dịch vụ này bao gồm: dịch vụ tập tin, dịch vụ in, dịch vụ cơ sở dữ liệu và các dịch vụ khác.

a) An toàn thông tin trên mạng

Việc kết nối mạng máy tính nhằm sử dụng và chia sẻ tài nguyên của các đối tượng trong hệ thống mạng cho dù họ có thể cách xa nhau về mặt địa lý. Tài nguyên hệ thống ở đây chủ yếu là thông tin. Tuy nhiên đây là loại tài nguyên dễ bị xâm phạm, bị đánh cắp, bị tráo đổi thông tin, đặc biệt là nó đang được lưu trữ trong môi trường mạng đầy phức tạp và phải chia sẻ cho nhiều người dùng khác nhau ở những vị trí khác nhau.

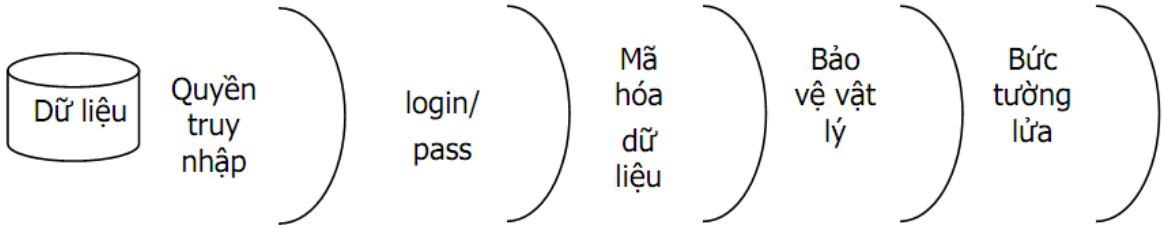
Vấn đề an toàn thông tin trên mạng đòi hỏi phải sử dụng nhiều biện pháp khác nhau từ cơ bản đến phức tạp, tùy theo lượng thông tin cần bảo vệ và khả năng cho phép của từng hệ thống cụ thể.

- ***Các chiến lược an toàn hệ thống***
  - ✓ Quyền hạn tối thiểu: Đây là chiến lược nền tảng nhất. Theo nguyên tắc này bất kì đối tượng nào cũng chỉ có những quyền hạn nhất định đối với những tài nguyên mạng nhất định khi xâm nhập vào mạng.
  - ✓ Bảo vệ theo chiều sâu: Tạo nhiều cơ chế an toàn cho hệ thống để chúng hỗ trợ cho nhau.
  - ✓ Cơ chế nút thắt: Tạo ra một "cửa khẩu" hẹp và cho phép thông tin đi vào hệ thống của mình bằng duy nhất con đường này. Đồng thời phải tổ chức một cơ chế kiểm soát và điều khiển các luồng thông tin đi qua cửa khẩu này.
  - ✓ Tính toàn cục: Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ. Nếu có kẻ nào có thể bẻ gãy một cơ chế an toàn thì chúng có thể thành công bằng cách tấn công hệ thống nội bộ từ bên trong.
  - ✓ Tính đa dạng của việc bảo vệ: Cần phải sử dụng nhiều biện pháp khác nhau cho những hệ thống khác nhau. Nếu không, kẻ nào tấn công được hệ thống này thì cũng có thể tấn công vào hệ thống khác.

Các mức bảo vệ thông tin mạng:

Vì không có giải pháp bảo vệ nào an toàn tuyệt đối nên người ta thường sử dụng nhiều mức bảo vệ khác nhau tạo thành nhiều lớp rào chắn cho hệ thống.

Mô hình như sau:



Hình 2.18 Các mức bảo vệ thông tin trên mạng

➢ *An toàn thông tin bằng mã hóa*

Để bảo vệ thông tin trên đường truyền, người ta chuyển đổi nó từ dạng nhận thức được sang dạng không nhận thức được trước khi truyền đi trên mạng nhằm bảo vệ tính bí mật cần thiết. Quá trình này diễn ra ở trạm phát được gọi là mã hóa thông tin *(Encrypting)*, ở trạm nhận phải thực hiện quá trình ngược lại, tức là biến đổi thông tin từ dạng không nhận thức được (đã mã hóa) sang dạng nhận thức được (dạng gốc), quá trình này gọi là giải mã *(Desrypting)*. Đây là lớp bảo vệ thông tin rất quan trọng và được ứng dụng trong hầu hết các hệ thống mạng.

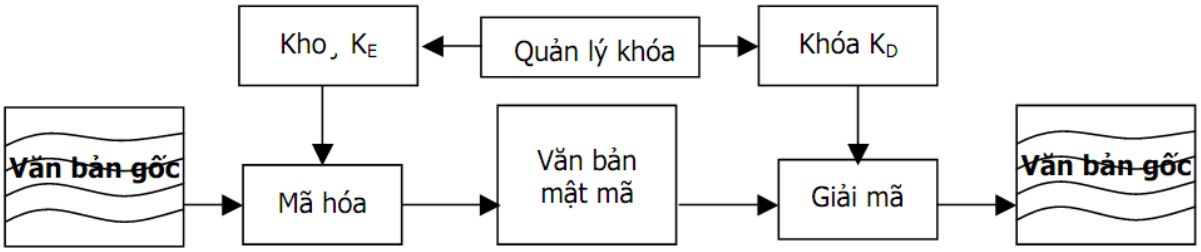
Để bảo vệthông tin bằng mật mã, người ta thường tiếp cận theo hai hướng:

- ✓ Từ nút đến nút *(End to End)*
- ✓ Theo đường truyền *(Link Oriented Security)*

Theo cách thứ nhất, thông tin được mã hóa để bảo vệ trên đường truyền giữa hai nút mà không quan tâm đến nguồn và đích của thông tin đó. Ở đây ta chú ý rằng thông tin chỉ được bảo vệ trên đường truyền, tức là ở mội nút mạng đều có quá trình giải mã để sau đó thông tin được chuyển đi tiếp, do đó các nút cần được bảo vệ tốt.

Ngược lại theo cách hai, thông tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn đến đích. Thông tin sẽ được mã hóa ngay sau khi mới tạo ra và chỉ được giải mã khi đã về đến đích. Cách này có nhược điểm là chỉ có dữ liệu người dùng mới được mã hóa còn các thông tin điều khiển thì phải giữ nguyên để có thể xử lý tại các nút.

Quá trình mã hóa và giải mã được mô tả như sau:



Hình 2.19 Sơ đồ quá trình mã hóa

- Văn bản gốc (*Plaintext*) là văn bản chưa được mã hóa.
- Khóa (*Key*): gồm một số hữu hạn các bit thường được biểu thị dưới dạng các xâu ký tự chữ số, số thập phân hoặc thập lục phân. Trong thực tế thường dùng các khóa có 8 ký tự.

Nếu gọi:

M là văn bản gốc
C là văn bản mật mã (*Ciphertext*)
E là hàm mã hóa (*Encryption Function*)

D là hàm giải mã (*Descryption Function*)

Ta có các hàm biểu diễn sự phụ thuộc giữa văn bản gốc và văn bản mã hóa như sau:

C = E(M)

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

Khóa KE được dùng để mã hóa và khóa KD được dùng để giải mã.

Có rất nhiều phương pháp mã hóa nhưng tất cả đều quy về 2 phương pháp chung tùy theo việc sử dụng cặp khóa KD và KE:

- ✓ Khóa KD trùng với khóa KE: Phương pháp này gọi là mã hóa khóa đối xứng, với phương pháp này yêu cầu khóa phải được giữ bí mật tuyệt đối, vì khóa dùng để mã hóa cũng được dùng để giải mã.
- ✓ Khóa KD khác khóa KE: Phương pháp này gọi là mã hóa khóa công khai. Trong đó, có thể chuyển đổi vai trò giữa 2 khóa và rất khó để suy ra khóa này từ khóa kia. Khóa mã hóa (KE) có thể đưa ra công khai nhưng dùng giải mã (KD) phải được giữ bí mật tuyệt đối.

Người ta còn phân biệt 2 loại khóa:

- ✓ Các khóa dùng trong thời gian dài gọi là khóa chính *(Primary)* hay khóa mã hóa *(Key Encryption).*
- ✓ Các khóa được dùng trong khuôn khổ một cuộc truyền thông gọi là khóa làm việc *(Working)* hay khóa mã hóa dữ liệu *(Data Encryption)*

b) Các phương pháp mã hóa dữ liệu

- ✓ Phương pháp hoán vị: Phương pháp này sắp xếp lại các ký tự trong văn bản gốc để tạo ra văn bản mật mã.
- ✓ Phương pháp thay thế: Phương pháp này mã hóa văn bản bằng cách thay thế mỗi ký tự trong văn bản bằng một ký tự khác nào đó (có thể chữ cái, chữ số, ký hiệu).
- ✓ Phương pháp mã hóa chuẩn DES *(Data Encryption Standard)*: Dùng kết hợp cả hay kỹ thuật thay thế và hoán vị.
- ✓ Phương pháp mã hóa khóa công khai.

c) Cơ chế bảo vệ bằng Firewall

Vấn đề quan trong trong việc quản lý các tài nguyên thông tin là cơ chế bảo vệ chống việc truy cập bất hợp pháp trong khi vẫn cho phép người được ủy nhiệm sử dụng những nguồn thông tin mà họ được cấp quyền và phương pháp chống thất thoát thông tin được truyền tải trên mạng truyền dữ liệu công cộng *(Public Data Communication Network).* Đó chính là yêu cầu của một giải pháp hoặc hệ thống an ninh cho hệ thống mạng hay còn gọi là hệ thống an ninh dữ liệu *(Data Security System).*

Nhu cầu an ninh hệ thống ngày càng trở nên quan trọng vì nhiều nguyên nhân như các đối thủ luôn tìm cách để nắm được mọi thông tin liên quan, ngày càng nhiều Hacker truy cập thông tin từ các trang mạng nội bộ theo nhiều mục đích khác nhau.

Một giải pháp an ninh cho hệ thống mạng được ứng dùng nhiều đó là tường lửa (*Firewall*). Thuật ngữ Firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong công nghệ thông tin, firewall là một kỹ thuật

được tích hợp vào hệ thống mạng để chống lại việc truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn.

Về mặt chức năng hệ thống: firewall là thành phần được đặt giữa hai mạng để kiểm soát tất cả các việc lưu thông và truy cập giữa chúng với nhau, bao gồm:

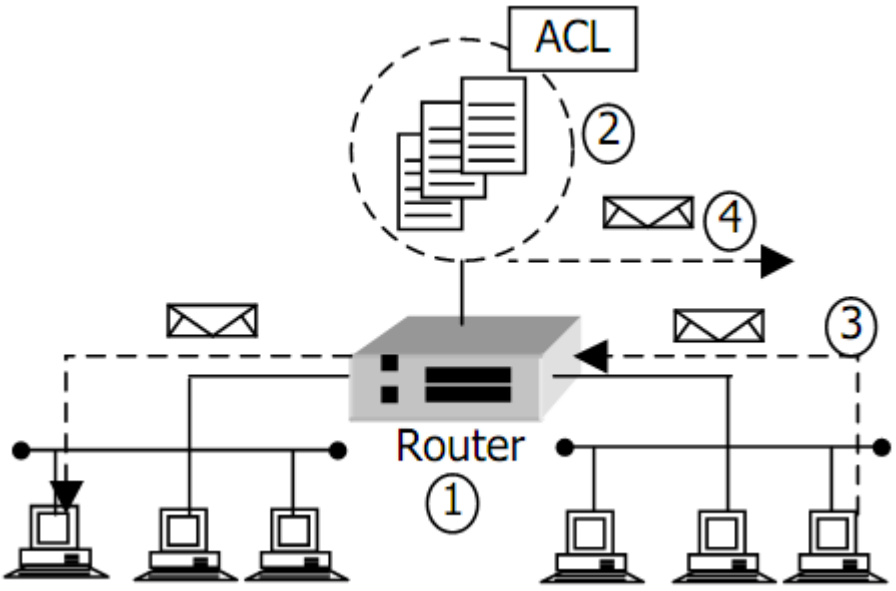
- ✓ Tất cả các trao đổi dữ liệu từ trong ra ngoài và ngược lại phải thực hiện thông qua Firewall.
- ✓ Chỉ có những trao đổi nào được phép bởi chế độ an ninh của hệ thống mạng nội bộ (*Trust Network*) mới được quyền lưu thông qua Firewall.

Về mặt vật lý: firewall bao gồm:

- ✓ Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (Router) hoặc có chức năng router.
- ✓ Các phần mềm quản lý an ninh chạy trên các hệ thống máy chủ. Thông thường là các hệ quản trị xác thực (*Authentication*), cấp quyền (*Authorization*) và kế toán (*Accounting*).

Firewall bao gồm phần cứng và/hoặc phần mềm nằm giữa hai mạng (như mạng LAN và mạng internet), bảo vệ mạng LAN bằng cách cấm các người sử dụng truy cập trái phép đến và đồng thời ngăn chặn những thông điệp không được phép gửi đi cho người nhận bên ngoài mạng. Firewall có thể nằm trên bộ dẫn đường hay trên server. Cơ chế làm việc của firewall dựa trên việc kiểm tra các gói dữ liệu IP lưu chuyển giữa hai mạng tùy thuộc vào các quy tắc mà người quản trị hệ thống đã xác lập.

Khái quát phương thức làm việc của firewall như trong hình sau:



Hình 2.20 Cơ chế hoạt động của Firewall

(1) Router nằm giữa 2 mạng.

(2) Người quản lý soạn một ACL trong đó có các địa chỉ IP hợp lệ.

(3) Một thông điệp được gửi tới router, thiết bị này sẽ kiểm tra địa chỉ của thông điệp này trong ACL, nếu có thông điệp sẽ được gửi đi.

(4) Ngược lại, thông điệp sẽ bị từ chối truy cập.

- ***Các loại Firewall và cơ chế hoạt động***

Khi nói đến việc lưu thông dữ liệu giữa các mạng với nhau thông qua firewall thì điều đó có nghĩa rằng firewall hoạt động kết hợp chặt chẽ với giao thức TCP/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng hay chính xác hơn là các dịch vụ chay trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS,…) thành các gói dữ liệu rồi gán cho các gói này những địa chỉ để có thể nhận dạng tái lập lại ở đích cần gửi đến. Do đó các loại firewall cũng liên quan rất nhiều đến các packet và các địa chỉ của chúng.

Bộ lọc packet (Packet filtering):

Loại firewall này thực hiện việc kiểm tra số nhận dang địa chỉ của các packet để cho phép chúng có thể lưu thông qua lại hay không. Các thông số có thể lọc được của một packet như sau:

- ✓ Địa chỉ IP nơi xuất phát (*Source IP Address*)
- ✓ Địa chỉ IP nơi nhận (*Destination IP Address*)
- ✓ Cổng TCP nơi xuất phát (*TCP Source port*)
- ✓ Cổng TCP nơi nhận (*TCP Destination port*)

Nhờ đó firewall có thể ngăn được các kết nối vào những máy chủ hoặc mạng nào đó được xác định hoặc khóa việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép.

Hơn nữa việc kiểm soát các cổng làm cho firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào máy chủ nào đó hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP,…) được phép mới chạy được trên hệ thống mạng nội bộ.

Cổng ứng dụng (Application Gateway)

Đây là một loại firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy Service (dịch vụ đại diện): một ứng dụng nào đó được quy chiếu đến (hay đại diện bởi) một Proxy Service trong khi các Proxy Service chạy trên các hệ thống máy chủ thì được quy chiếu đến application gateway của firewall. Cơ chế lọc của packet filtering phối hợp kiểm soát với cơ chế "đại diện" của application gateway cung cấp một khả năng an toàn và uyển chuyển hơn.

Ví dụ một hệ thống mạng có chức năng lọc các gói tin ngăn các kết nối bằng Telnet vào hệ thống chỉ trừ một chủ duy nhất – Telnet application gateway là được phép. Một người sử dụng dịch vụ Telnet muốn kết nối vào hệ thống phải thực hiện các bước sau:

- ✓ Thực hiện dịch vụ Telnet đến Telnet application gateway rồi cho biết tên của máy chủ bên trong cần truy cập.
- ✓ Gateway kiểm tra địa chỉ IP nơi xuất phát của người truy cập rồi cho phép hoặc từ chối tùy theo chế độ an ninh của hệ thống.
- ✓ Người truy cập phải vượt qua được hệ thống kiểm tra xác thực.
- ✓ Proxy Service tạo một kết nối Telnet giữa gateway và máy chủ cần truy cập.

- ✓ Proxy Service liên kết lưu thông giữa người truy cập và máy chủ.

Cơ chế hoạt động này có ý nghĩa quan trọng trong việc thiết kế an ninh hệ thống ví dụ như sau:

- ✓ Che giấu các thông tin: Người dùng chỉ có thể nhìn thấy trực tiếp các gateway được phép.
- ✓ Tăng cường kiểm tra truy cập bằng các dịch vụ xác thực *(Authentication).*
- ✓ Giảm đáng kể giá thành cho việc phát triển các hệ quản trị xác thực vì các hệ thống này được thiết kế chỉ quy chiếu đến application gateway.
- ✓ Giảm thiểu các quy tắc kiểm soát của bộ lọc *(Packet filtering).* Điều này làm tăng tốc độ hoạt động của firewall.

Bộ lọc session thông minh (Smart session filtering)

Cơ chế hoạt động phối hợp giữa bộ lọc packet và cổng ứng dụng như trên cung cấp một chế độ an ninh cao tuy nhiên nó cũng bị vài hạn chế. Vấn đề chính hiện nay là làm sao để cung cấp đủ Proxy Service cho rất nhiều ứng dụng khác nhau đang phát triển ồ ạt. Điều này có nghĩa là nguy cơ, áp lực đối với việc đánh lừa firewall gia tăng lên rất lớn nếu các proxy không kịp đáp ứng.

Trong khi giám sát các packet ở những mức phía trên, nếu như lớp network đòi hỏi nhiều công sức hơn đối với việc lọc các packet đơn giản thì việc giám sát các giao dịch lưu thông ở mức mạng (Session) đòi hỏi ít công việc hơn. Cách này cũng loại bỏ được các dịch vụ đặc thù cho từng loại ứng dụng khác nhau.

Nếu kết hợp khả năng ghi nhận thông tin về session và sử dụng nó để tạo các quy tắc cho bộ lọc thì sẽ có được một bộ lọc thông minh hơn. Đó chính là cơ chế hoạt động của bộ lọc session thông minh.

Vì một session ở mức network được tạo bởi 2 packet lưu thông theo 2 chiều, cho nên nếu thiết kế 2 quy tắc lọc cho 2 chiều này: một để kiểm soát các packet lưu thông từ host phát sinh ra nó đến máy chủ cần tới, một để kiểm soát packet trở về theo chiều ngược lại nên quy tắc thứ 2 là không cần thiết. Do vậy, cách để tiếp nhận các packet không mong muốn sinh ra từ bên ngoài firewall sẽ khác biệt rất rõ với cách tiếp cận cho các packet do những kết nối được phép (ra bên ngoài). Và như vậy dễ dùng nhận dạng các packet "bất hợp pháp".

Firewall hỗn hợp (Hybrid firewall)

Trong thực tế các firewall được sử dụng là sự kết hợp của nhiều kỹ thuật để tạo ra hiệu quả an ninh tối đa. Ví dụ việc để lọt lưới tại các kiểm soát của bộ lọc packet có thể được thực hiện tại bộ lọc session thông minh ở mức ứng dụng. Các giám sát của bộ lọc lại được bóc lót chặt chẽ bởi các dịch vụ proxy của application gateway.

Một vài ứng dụng của firewall

Từ các chế độ hoạt động trên, firewall được ứng dụng nhiều vào hệ thống an ninh dữ liệu. Có 3 yêu cầu chính cho vấn đề an ninh hệ thống theo tiêu chuẩn ISO cho mô hình mạng OSI:

- ✓ Quản lý xác thực *(Authentication)*
- ✓ Quản lý cấp quyền *(Authorization)*

- ✓ Quản lý kế toán *(Acounting management)*
- ✓ …

Ưu điểm của firewall

Firewall là điểm kiểm tra các kết nối giữa mạng nội bộ và mạng Internet bên ngoài, mọi kết nối đều phải đi qua cửa khẩu này. Đây chính là một bộ lọc an toàn bởi vì có rất nhiều dịch vụ đang hoạt động trên internet, nếu chúng ta không có cơ chế kiểm soát chặt chẽ thì các dịch vụ này sẽ tự động mang thông tin tràn vào mạng của chúng ta và ngược lại.

Firewall có thể được sử dụng để ghi nhận lại các hoạt động kết nối với Internet. Bởi vì, mọi hoạt động như vậy đều thông qua firewall nên nó có thể cung cấp thêm chức năng thu thập mọi thông tin các kết nối xảy ra giữa mạng nội bộ và mạng internet bên ngoài.

Ta cũng có thể sử dụng firewall để bảo vệ một máy đơn của người sử dụng.

Hạn chế của Firewall

Bên cạnh những mặt tích cực của Firewall kể trên, nó còn có những hạn chế và những việc mà nó không thể thực hiện được như sau:

- ✓ Bên cạnh việc ngăn chặn các người dùng trong mạng nội bộ kết nối ra ngoài khi không được phép thì nó cũng ngăn cản các việc làm tốt của họ.
- ✓ Firewall không thể chống lại các mối nguy hiểm mới, bởi vì chúng nằm ngoài sự kiểm soát của firewall.
- ✓ Do không kiểm tra trên nội dung của các gói tin, nên firewall không sử dụng để ngăn ngừa các thông tin xấu trên một dịch vụ đã được cho phép và cũng không thể nhận biết các đoạn mã virus trong các tập tin truyền đi.

d) Hệ quản trị mạng

Hệ thống quản trị mạng (Network Management) còn gọi là mô hình Manager/Agent bao gồm các thành phần sau:

- ✓ Hệ quản trị.
- ✓ Hệ bị quản trị.
- ✓ Một cơ sở dữ liệu chứa thông tin quản trị và giao thức quản trị mạng.

Thực hiện cung cấp giao diện giữa người quản trị mạng và các thiết bị mạng được quản trị, bao gồm các thông tin thể hiện dưới dạng đồ họa, đồ thị, số liệu thống kê, báo cáo. Ví dụ như hiển thị dạng đồ họa về topology liên mạng thể hiện các vị trí của các LAN segments, từ đó có thể chọn xem trạng thái hoạt động hiện hành của nó.

TỔNG KẾT CHƯƠNG

Các điểm quan trọng bạn cần nắm được trong chương này:

1. Mục đích và tầm quan trọng của phân tầng.
2. Một số nguyên tắc của kiến trúc mạng phân tầng và vẽ mô hình OSI.
3. Chức năng và đơn vị truyền của các tầng trong mô hình OSI.
4. Các thuật ngữ trong mô hình OSI?
5. Nguyên lý hoạt động của hàm nguyên thủy.
6. Phương thức hoạt động của mô hình OSI?
7. Vai trò, chức năng và đặc điểm của các tầng trong mô hình OSI.

CHƯƠNG 3
MẠNG CỤC BỘ (LOCAL AREA NETWORK)

3.1 ĐỊNH NGHĨA

LAN *(Local Area Network)* là một hệ thống mạng dùng để kết nối các máy tính và các thiết bị xử lý dữ liệu hoạt động với nhau trong một khu vực địa lý nhỏ như ở một tầng của tòa nhà, phòng làm việc, trường học,… (100m đến vài km), có tốc độ truyền dữ liệu cao, tỷ lệ sai số dữ liệu nhỏ. Các máy tính trong mạng LAN có thể chia sẻ tài nguyên với nhau, điển hình là chia sẻ tập tin, máy in, máy quét và một số thiết bị khác.

3.2 ĐẶC TRƯNG MẠNG CỤC BỘ

Do nhu cầu thực tế của các cơ quan, trường học, doanh nghiệp, tổ chức cần kết nối các máy tính đơn lẻ thành một mạng nội bộ để tạo khả năng trao đổi thông tin, sử dụng chung tài nguyên (phần cứng, phần mềm). Ví dụ trong một văn phòng có một máy in, để tất cả mọi người sử dụng chung máy in này thì giải pháp nối mạng có thể khắc phục được hạn chế này.

Theo tiêu chí đánh giá là khoảng cách địa lý thì người ta thường phân loại mạng máy tính thành ba kiểu:

- Mạng nội bộ - *Local Area Network* (LAN)
- Mạng đô thị - *Metropolitan Area Network* (MAN)
- Mạng diện rộng - *Wide Area Network* (WAN)
- Mạng toàn cầu - *Global Area Network* (GAN)

Trong thực tế, LAN và WAN thường được cài đặt nhất. Mạng LAN được sử dụng để nối kết một dải rộng các thiết bị trong một phạm vi hẹp, ví dụtrên cùng một tầng, một tòa nhà hay một khuôn viên. Ngày nay, LAN là loại mạng được sử dụng rất phổ biến trong mọi lĩnh vực của xã hội. Người ta thường nghĩ đến LAN như là mạng có thông lượng cao, độ trì hoãn thấp.

Hiện tại có rất nhiều công nghệ xây dựng mạng LAN mà chúng ta sẽ xem xét đến ngay sau đây. Nhiều chuẩn mạng LAN đã được phát triển trong đó Ethernetvà FDDI là phổ biến nhất. Người ta thường gọi chung họ các chuẩn mạng LAN là IEEE 802.

Về góc độ kỹ thuật, LAN có các tính chất quan trọng sau:

- Tất cả các host trong mạng LAN cùng chia sẻ đường truyền chung. Do đó chúng hoạt động dựa trên kiểu quảng bá (*broadcast)*.
- Không yêu cầu phải có hệ thống trung chuyển (*routing/switching*) trong một LAN đơn.

Thông thường, một mạng LAN được định nghĩa dựa trên các thông số sau:

- Hình thái (*topology*): chỉ ra kiểu cách mà host trong mạng được đấu nối với nhau.
- Đường truyền chia sẻ (xoắn đôi, đồng trục, cáp quang): chỉ ra các kiểu đường truyền mạng được dùng để đấu nối các host trong LAN lại với nhau.

- Kỹ thuật truy cập đường truyền (*Medium Access Control - MAC*): chỉ ra cách thức mà các host trong mạng LAN sử dụng để truy cập và chia sẻ đường truyền mạng. MAC sẽ quản trị việc truy cập đến đường truyền trong LAN và cung cấp cơ sở cho việc định danh các tính chất của mạng LAN theo chuẩn IEEE.

3.3 KIẾN TRÚC VÀ CẤU HÌNH MẠNG CỤC BỘ

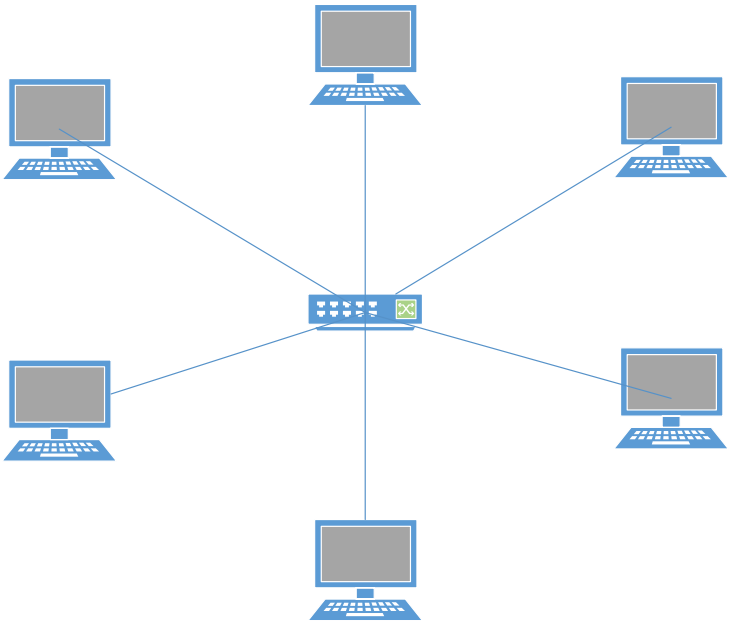
3.3.1 Kiến trúc

Kiến trúc mạng sẽ xác định hình dáng tổng quát của một mạng. Hiện nay, người ta đã định nghĩa ra được nhiều hình thái mạng khác nhau tương ứng với những tính chất đặc thù của chúng. Kiến trúc mạng là tiêu chí bắt buộc dùng để xây dựng mạng LAN và nó chủ yếu quan tâm đến việc làm cho mạng được liên thông và che giấu chi tiết về các thiết bị thực đối với người dùng.

3.3.1.1Mạng hình sao (Star)

- Tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích của tín hiệu.
- Thiết bị trung tâm có thể là Hub, Switch, Router.

Vai trò của thiết bị trung tâm là thực hiện việc "bắt tay" giữa các trạm cần trao đổi thông tin với nhau, thiết lập các liên kết điểm - điểm giữa chúng.



Hình 3.1 Sơ đồ mạng hình sao

Ưu điểm: Dễ kiểm soát. Do sử dụng liên kết điểm - điểm nên tận dụng được tối đa tốc độ của đường truyền vật lý.

Nhược điểm: Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế.

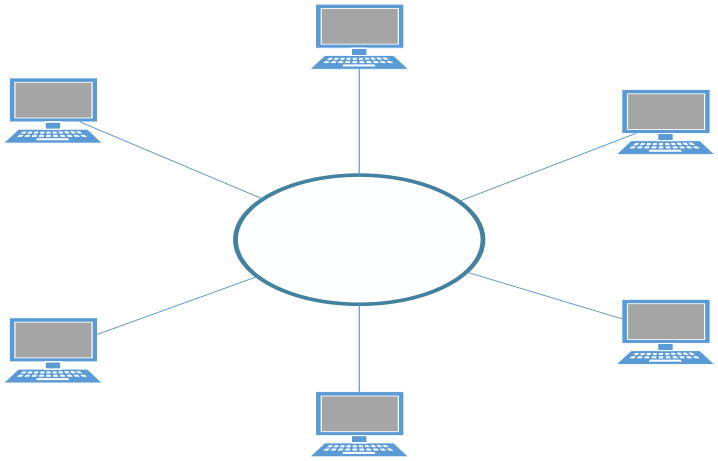
3.3.1.2 Mạng hình vòng (Ring)

- Tín hiệu được lưu chuyển theo một chiều duy nhất.
- Mỗi trạm làm việc được nối với vòng qua một bộ chuyển tiếp (repeater), có nhiệm vụ nhận tín hiệu rồi chuyển đến trạm kế tiếp trên vòng

- Tín hiệu được lưu chuyển trên vòng theo một chuỗi liên tiếp các liên kết Point to Point giữa các bộ chuyển tiếp.

Để tăng độ tin cậy của mạng, phải lắp vòng dự phòng, khi đường truyền trên vòng chính bị sự cố thì vòng phụ được sử dụng với chiều đi của tín hiệu ngược với chiều đi của mạng chính.

Thực tế, có một đoạn cable ngắn nối máy tính với vòng

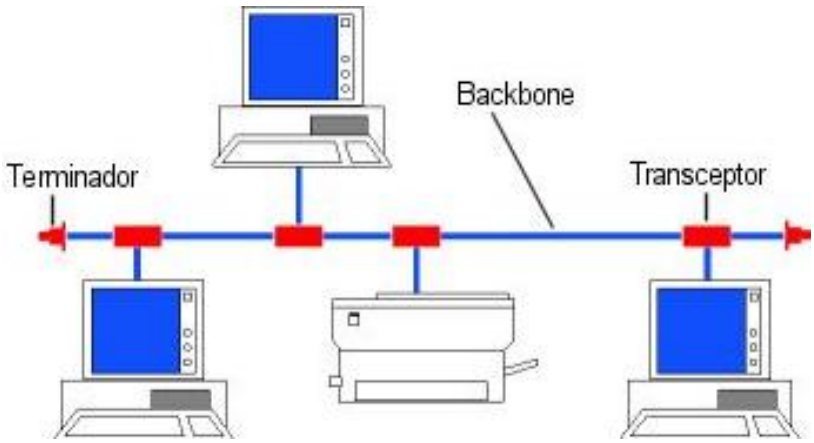


Hình 3.2 Sơ đồ mạng hình vòng (ring)

- *Nhược điểm:* Nếu xảy ra sự cố trên đường truyền, tất cả các máy trong mạng không thể giao tiếp với nhau. Đòi hỏi giao thức truy nhập đường truyền khá phức tạp (Tuy nhiên toàn bộ công việc này được hệ phần mềm giải quyết)

3.3.1.3Mạng hình tuyến (Bus)

- Tất cả các trạm đều dùng chung một đường truyền chính (Bus) được giới hạn bởi hai đầu nối (Terminator)
- Mỗi trạm được nối vào Bus qua một đầu nối chữ T (T-Connector)
- Khi một trạm truyền dữ liệu thì tín hiệu được quảng bá trên 2 chiều của Bus (tất cả các trạm khác đều có thể nhận tín hiệu)
- Mạng hình tuyến hoạt động theo các liên kết Point to Multipoint hoặc Broadcast.



Hình 3.3 Sơ đồ kết nối đường thẳng (bus)

- *Nhược điểm:* nếu xảy ra sự cố trên đường truyền, toàn bộ các máy trong mạng không thể giao tiếp với nhau được nữa. Giao thức quản lý truy nhập đường truyền phức tạp.

*** So sánh giữa các cách kết nối và ưu nhược điểm của chúng:**

- *Khác nhau:* kiểu hình sao là kết nối điểm - điểm trực tiếp giữa hai máy tính thông qua một thiết bị trung tâm. Kiểu vòng thì tín hiệu lưu chuyển trên vòng là một chuỗi các kết nối điểm - điểm. Kiểu tuyến tính thì dữ liệu truyền dựa trên điểm - nhiều điểm hoặc quảng bá.
- *Giống nhau:* Cả ba cách kết nối đều đơn giản, dễ lắp đặt, dễ thay đổi cấu hình.

Do ưu, nhược điểm của từng loại mà trong thực tế người ta thường chọn kiểu kết nối là tổ hợp của các kiểu kết nối trên.

3.3.2 Đường truyền vật lý

Mạng cục bộ thường sử dụng 3 loại đường truyền vật lý: cáp đôi xoắn, cáp đồng trục, và cáp sợi quang. Ngoài ra gần đây người ta cũng đã bắt đầu sử dụng nhiều các mạng cục bộ không dây nhờ radio hoặc viba.

Cáp đồng trục được sử dụng nhiều trong các mạng dạng tuyến tính, hoạt động truyền dẫn theo dải cơ sở (baseband) hoặc dải rộng (*broadband*). Với dải cơ sở, toàn bộ khả năng của đường truyền được dành cho một kênh truyền thông duy nhất, trong khi đó với dải rộng thì hai hoặc nhiều kênh truyền thông cùng phân chia dải thông của kênh truyền.

Hầu hết các mạng cục bộ đều sử dụng phương thức dải rộng. Với phương thức này tín hiệu có thể truyền đi dưới cả hai dạng: tương tự (*analog*) và số (*digital*) không cần điều chế.

Cáp đồng trục có hai loại là cáp gầy (*thin cable*) và cáp béo *(thick cable*). Cả hai loại cáp này đều có tốc độ làm việc 10Mb/s nhưng cáp gầy có độ suy hao tín hiệu lớn hơn, có độ dài cáp tối đa cho phép giữa hai repeater nhỏ hơn cáp béo. Cáp gầy thường dùng để nối các trạm trong cùng một văn phòng, phòng thí nghiệm, còn cáp béo dùng để nối dọc theo hành lang, lên các tầng lầu, …

Phương thức truyền thông theo dải rộng có thể dùng cả cáp đôi xoắn, nhưng cáp đôi xoắn chỉ thích hợp với mạng nhỏ hiệu năng thấp và chi phí đầu tư ít.

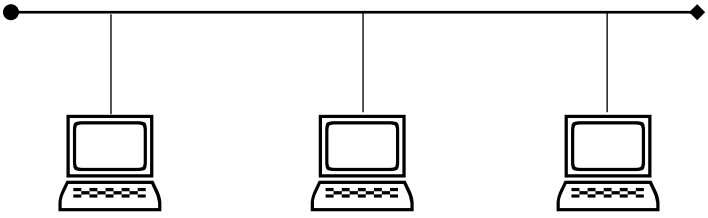
Phương thức truyền theo dải rộng chia dải thông (tần số) của đường truyền thành nhiều dải tần số con (kênh), mỗi dải tần số con đó cung cấp một kênh truyền dữ liệu tách biệt nhờ sử dụng một cặp modem đặc biệt. Phương thức này vốn là một phương tiện truyền một chiều: Các tín hiệu đưa vào đường truyền chỉ có thể truyền đi theo một hướng => không cài đặt được các bộ khuyếch đại để chuyển tín hiệu của một tần số theo cả hai chiều. Vì thế xảy ra tình trạng chỉ có trạm nằm dưới trạm truyền là có thể nhận được tín hiệu. Vậy làm thế nào để có hai đường dẫn dữ liệu trên mạng. Điểm gặp nhau của hai đường dẫn đó gọi là điểm đầu cuối. Ví dụ, trong topo dạng bus thì điểm đầu cuối đơn giản chính là đầu mút của bus (*terminator*), còn với topo dạng cây (*tree*) thì chính là gốc của cây (*root)*. Các trạm khi truyền đều truyền về hướng điểm đầu cuối (gọi là đường dẫn về), sau đó các tín hiệu nhận được ở điểm đầu cuối sẽ truyền theo đường dẫn thứ hai xuất phát từ điểm đầu cuối (gọi là đường dẫn đi). Tất cả các trạm đều nhận dữ liệu trên đường dẫn đi. Để cài đặt đường dẫn về và đi, có thể sử dụng cấu hình vật lý như trên hình 3.4.

Trong cấu hình cáp đôi (*dual cable*), các đường dẫn về và đi chạy trên các cáp riêng biệt và điểm đầu cuối đơn giản chỉ là một đầu nối thụ động của chúng. Trạm gửi và nhận cùng một tần số.

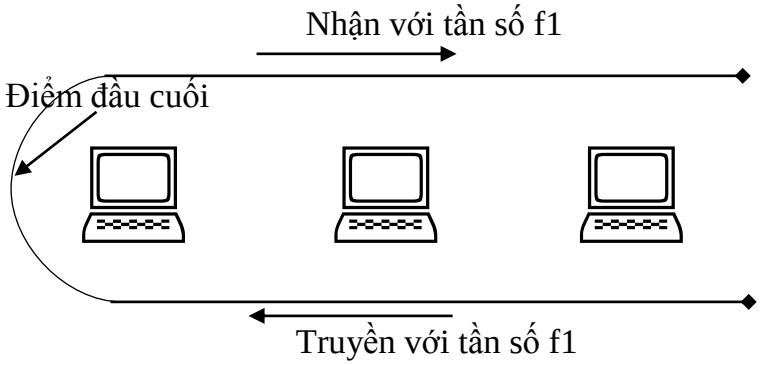
Trong cấu hình tách (*split*), cả hai đường dẫn đều ở trên cùng một cáp nhưng tần số khác nhau: đường dẫn về có tần số thấp và đường dẫn đi có tần số cao hơn. Điểm đầu cuối là bộ chuyển đổi tần số.

Chú ý: việc lựa chọn đường truyền và thiết kế sơ đồ đi cáp (trong trường hợp hữu tuyến) là một trong những công việc quan trọng nhất khi thiết kế và cài đặt một mạng máy tính nói chung và mạng cục bộ nói riêng. Giải pháp lựa chọn pháp đáp ứng được nhu cầu sử dụng mạng thực tế không chỉ cho hiện tại mà cho cả tương lai.

Ví dụ: Muốn truyền dữ liệu đa phương tiện thì không thể chọn loại cáp chỉ cho phép thông lượng tối đa là vài Mb/s, mà phải nghĩ đến loại cáp cho phép thông lượng trên 100 Mb/s. Việc lắp đặt hệ thống trong cáp trong nhiều trường hợp (toà nhà nhiều tầng) là tốn rất nhiều công phải lựa chọn cẩn thận, không thể để xảy ra trường hợp sau 1 - 2 năm gỡ bỏ và lắp đặt lại hệ thống mới.



a) Split Broadband



b) Dual Cable Broadband

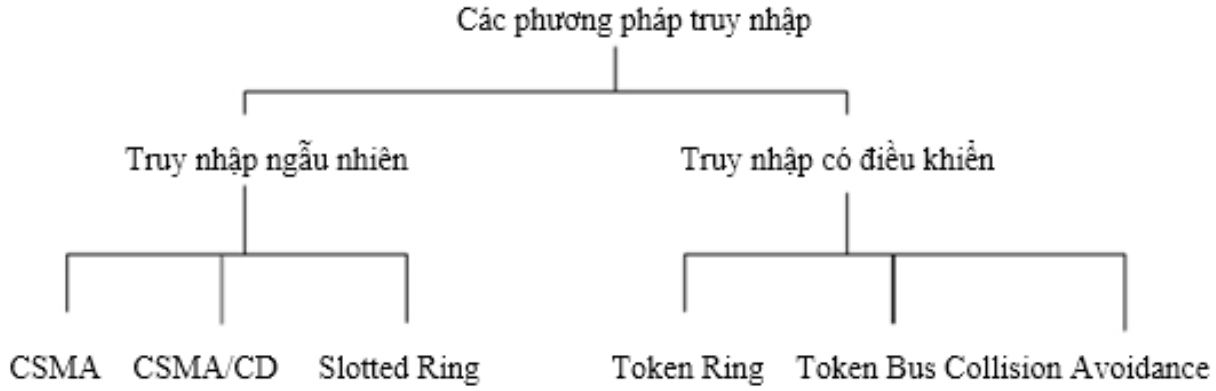
Hình 3.4 Cấu hình vật lý cho Broadband

3.4 CÁC PHƯƠNG PHÁP TRUY NHẬP ĐƯỜNG TRUYỀN VẬT LÝ

3.4.1 Giới thiệu

Đối với topo dạng hình sao, khi một liên kết được thiết lập giữa hai trạm thì thiết bị trung tâm sẽ đảm bảo đường truyền được dành riêng trong suốt cuộc truyền. Tuy nhiên đối với topo dạng vòng và tuyến tính thì chỉ có một đường truyền duy nhất nối tất cả các trạm với nhau bởi vậy cần phải có một quy tắc chung cho tất cả các trạm nối vào mạng để bảo đảm rằng đường truyền được truy nhập và sử dụng một cách tốt đẹp.

Có nhiều phương pháp để truy nhập đường truyền vật lý, được phân làm hai loại: phương pháp truy nhập ngẫu nhiên và phương pháp truy nhập có điều kiện.



Hình 3.5 Các phương pháp truy nhập đường truyền

Trong đó có 3 phương pháp hay dùng nhất trong các mạng cục bộ hiện nay:

- ✓ Phương pháp CSMA/CD.
- ✓ Phương pháp Token Bus.
- ✓ Phương pháp Token Ring.

3.4.2 Phương pháp CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*)

Phương pháp đa truy nhập sử dụng sóng mang có phát hiện xung đột - CSMA/CD. Phương pháp này sử dụng cho topo dạng bus, trong đó tất cả các trạm của mạng đều được nối trực tiếp vào bus. Mọi trạm đều có thể truy nhập vào bus chung (đa truy nhập) một cách ngẫu nhiên và do vậy rất có thể dẫn đến xung đột (hai hoặc nhiều trạm đồng thời truyền dữ liệu). Dữ liệu được truyền trên mạng theo một khuôn dạng đã định sẵn trong đó có một vùng thông tin điều khiển chứa địa chỉ trạm đích.

Phương pháp CSMA/CD là phương pháp cải tiến từ phương pháp CSMA hay còn gọi là LBT (*Listen Before Talk* - Nghe trước khi nói). Tư tưởng của nó: một trạm cần truyền dữ liệu trước hết phải "nghe" xem đường truyền đang rỗi hay bận. Nếu rỗi thì truyền dữ liệu đi theo khuôn dạng đã quy định trước. Ngược lai, nếu bận (tức là đã có dữ liệu khác) thì trạm phải thực hiện một trong 3 giải thuật sau (gọi là giải thuật "kiên nhẫn"):

1. Tạm "rút lui" chờ đợi trong một thời gian ngẫu nhiên nào đó rồi lại bắt đầu nghe đường truyền (*Non- persistent*)
2. Tiếp tục "nghe" đến khi đường truyền rỗi thì truyền dữ liệu đi với xác suất bằng 1 (*1- persistent*)
3. Tiếp tục "nghe" đến khi đường truyền rỗi thì truyền đi với xác suất p xác định trước ($0 < p < 1$) (*p- persistent*)

Với giải thuật 1 có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền khi thấy đường truyền bận sẽ cùng "rút lui" chờ đợi trong các thời đoạn ngẫu nhiên khác. Nhược điểm có thể có thời gian chết sau mỗi cuộc truyền.

Giải thuật 2 khắc phục nhược điểm có thời gian chết bằng cách cho phép một trạm có thể truyền ngay sau khi một cuộc truyền kết thúc. Nhược điểm: Nếu lúc đó có hơn một trạm đang đợi thì khả năng xảy ra xung đột là rất cao.

Giải thuật 3 trung hoà giữa hai giải thuật trên. Với giá trị p lựa chọn hợp lý có thể tối thiểu hoá được cả khả năng xung đột lẫn thời gian chết của đường truyền. Xảy ra xung đột là do độ trễ của đường truyền dẫn: một trạm truyền dữ liệu đi rồi nhưng do độ trễ đường truyền nên một trạm khác lúc đó đang nghe đường truyền sẽ tưởng là rỗi và cứ thế truyền dữ liệu đi dẫn đến xung đột. Nguyên nhân xảy ra xung đột của phương pháp này là các trạm chỉ "nghe trước khi nói" mà không "nghe trong khi nói" do vậy trong thực tế có xảy ra xung đột mà không biết, vẫn cứ tiếp tục truyền dữ liệu đi và gây ra chiếm dụng đường truyền một cách vô ích.

Để có thể phát hiện xung đột, cải tiến thành phương pháp CSMA/CD (LWT - Listen While Talk - nghe trong khi nói) tức là bổ sung thêm các quy tắc:

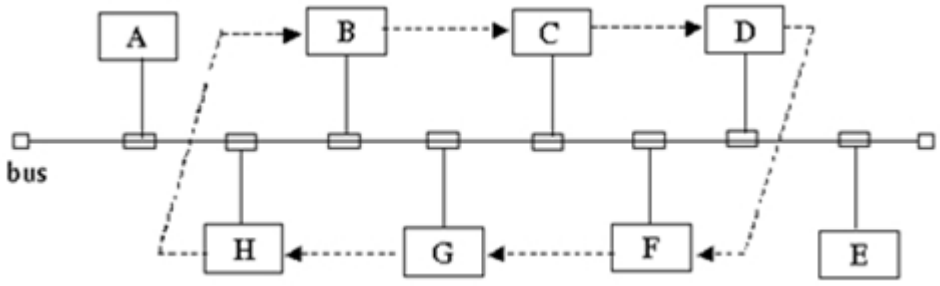
- Khi một trạm đang truyền, nó vẫn tiếp tục nghe đường truyền. Nếu phát hiện thấy xung đột thì nó ngừng ngay việc truyền nhưng vẫn tiếp tục gửi sóng mang thêm một thời gian nữa để đảm bảo rằng tất cả các trạm trên mạng đều có thể nghe được sự kiện xung đột đó.
- Sau đó trạm chờ đợi một thời gian ngẫu nhiên nào đó rồi thử truyền lại theo các quy tắc của CSMA

Rõ ràng với CSMA/CD thời gian chiếm dụng đường truyền vô ích giảm xuống bằng thời gian để phát hiện xung đột. CSMA/CD cũng sử dụng một trong 3 giải thuật "kiên nhẫn" ở trên, trong đó giải thuật 2 được ưa dùng hơn cả.

3.4.3 Phương pháp Token Bus

Phương pháp truy nhập có điều khiển dùng kỹ thuật *"chuyển thẻ bài"* để cấp phát quyền truy nhập đường truyền. Thẻ bài (*Token*) là một đơn vị dữ liệu đặc biệt, có kích thước và có chứa các thông tin điều khiển trong các khuôn dạng.

Nguyên lý: Để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu, một thẻ bài được lưu chuyển trên một vòng logic thiết lập bởi các trạm đó. Khi một trạm nhận được thẻ bài thì nó có quyền sử dụng đường truyền trong một thời gian định trước. Trong thời gian đó nó có thể truyền một hoặc nhiều đơn vị dữ liệu. Khi đã hết dữ liệu hay hết thời gian cho phép, trạm phải chuyển thẻ bài đến trạm tiếp theo trong vòng logic. Như vậy công việc phải làm đầu tiên là thiết lập vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang có nhu cầu truyền dữ liệu được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kề trước và sau nó. Thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu thì không được đưa vào vòng logic và chúng chỉ có thể tiếp nhận dữ liệu.



….. Vòng logic ►Đường truyền vật lý

Hình 3.6 Token Bus

Trong hình, trạm A và E nằm ngoài vòng logic chỉ có thể tiếp nhận dữ liệu dành cho chúng.

Vấn đề quan trọng là phải duy trì được vòng logic tùy theo trạng thái thực tế của mạng tại thời điểm nào đó. Cụ thể cần phải thực hiện các chức năng sau:

- Bổ sung một trạm vào vòng logic: Các trạm nằm ngoài vòng logic cần được xem xét định kỳ để nếu có nhu cầu truyền dữ liệu thì bổ sung vào vòng logic.
- Loại bỏ một trạm khỏi vòng logic: Khi một trạm không còn nhu cầu truyền dữ liệu cần loại nó ra khỏi vòng logic để tối ưu hoá việc điều khiển truy nhập bằng thẻ bài.
- Quản lý lỗi: một số lỗi có thể xảy ra, chẳng hạn trùng địa chỉ (hai trạm đều nghĩ rằng đến lượt mình) hoặc "đứt vòng" (không trạm nào nghĩ đến lượt mình).
- Khởi tạo vòng logic: Khi cài đặt mạng hoặc sau khi "đứt vòng" thì cần phải khởi tạo lại vòng logic.

Các giải thuật cho các chức năng trên có thể làm như sau:

- Bổ sung một trạm vào vòng logic, mỗi trạm trong vòng có trách nhiệm định kỳ tạo cơ hội cho các trạm mới nhập vào vòng. Khi chuyển thẻ bài đi, trạm sẽ gửi thông báo "tìm trạm đứng sau" để mời các trạm (có địa chỉ giữa nó và trạm kế tiếp nếu có) gửi yêu cầu nhập vòng. Nếu sau một thời gian xác định trước mà không có yêu cầu nào thì trạm sẽ chuyển thẻ bài tới trạm kề sau nó như thường lệ. Nếu có yêu cầu thì trạm gửi thẻ bài sẽ ghi nhận trạm yêu cầu trở thành trạm đứng kề sau nó và chuyển thẻ bài tới trạm mới này. Nếu có hơn một trạm yêu cầu nhập vòng thì trạm giữ thẻ bài sẽ phải lựa chọn theo giải thuật nào đó.
- Loại một trạm khỏi vòng logic: Một trạm muốn ra khỏi vòng logic sẽ đợi đến khi nhận được thẻ bài sẽ gửi thông báo "nối trạm đứng sau" tới trạm kề trước nó yêu cầu trạm này nối trực tiếp với trạm kề sau nó.
- Quản lý lỗi: Để giải quyết các tình huống bất ngờ. Chẳng hạn, trạm đó nhận được tín hiệu cho thấy đã có các trạm khác có thẻ bài. Lập tức nó phải chuyển sang trạng thái nghe (bị động, chờ dữ liệu hoặc thẻ bài). Hoặc sau khi kết thúc truyền dữ liệu, trạm phải chuyển thẻ bài tới trạm kề sau nó và tiếp tục nghe xem trạm kề sau đó có hoạt động hay đã bị hư hỏng. Nếu trạm kề sau bị hỏng thì phải tìm cách gửi các thông báo để vượt qua trạm hỏng đó, tìm trạm hoạt động để gửi thẻ bài.
- Khởi tạo vòng logic: Khi một trạm hay nhiều trạm phát hiện thấy đường truyền không hoạt động trong một khoảng thời gian vượt quá một giá trị ngưỡng (time out) cho trước - thẻ bài bị mất (có thể do mạng bị mất nguồn hoặc trạm giữ thẻ bài bị hỏng). Lúc đó trạm phát hiện sẽ gửi đi thông báo "yêu cầu thẻ bài" tới một trạm được chỉ định trước có trách nhiệm sinh thẻ bài mới và chuyển đi theo vòng logic.

3.4.4 Phương pháp Token Ring

Phương pháp Token Ring dựa trên nguyên lý dùng thẻ bài để cấp phát quyền truy nhập đường truyền. Thẻ bài lưu chuyển theo vòng vật lý chứ không cần thiết lập vòng logic như phương pháp trên.

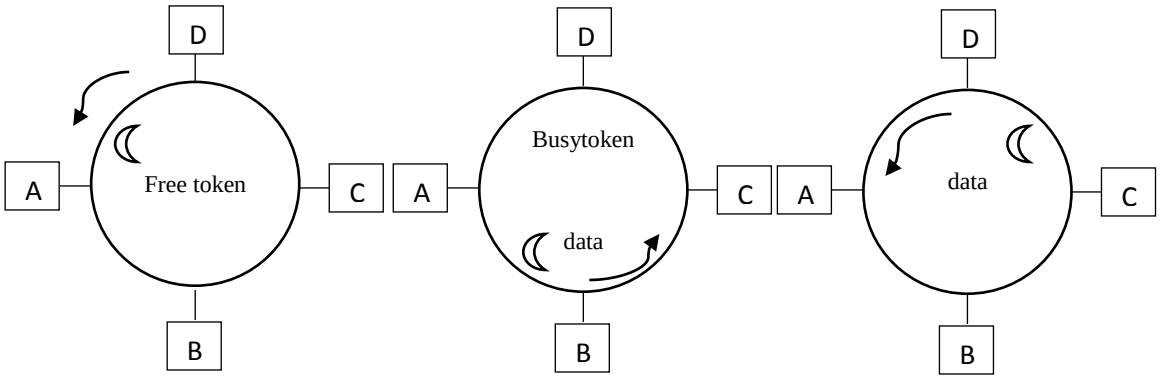
Thẻ bài là một đơn vị dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái sử dụng của nó (bận hoặc rỗi). Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài rỗi. Khi đó nó sẽ đổi bit trạng thái thành bận và truyền một đơn vị dữ liệu cùng với thẻ bài đi theo chiều của vòng và không còn thẻ bài rỗi trên vòng nữa, do đó các trạm có dữ liệu cần truyền buộc phải đợi. Dữ liệu đến trạm đích sẽ được lưu lại, sau đó cùng với thẻ bài đi tiếp cho đến khi quay về trạm nguồn. Trạm nguồn sẽ xóa bỏ dữ liệu, đổi bit trạng thái thành rỗi cho lưu chuyển tiếp trên vòng để các trạm khác có thể nhận được quyền truyền dữ liệu.

Sự quay về trạm nguồn của dữ liệu và thẻ bài nhằm tạo ra một cơ chế nhận tự nhiên: trạm đích có thể gửi vào đơn vị dữ liệu các thông tin về kết quả tiếp nhận dữ liệu của mình.

- Trạm đích không tồn tại hoặc không hoạt động.
- Trạm đích tồn tại nhưng dữ liệu không sao chép được.
- Dữ liệu đã được tiếp nhận.

Phương pháp này cần phải giải quyết hai vấn đề có thể gây phá vỡ hệ thống:

- Mất thẻ bài: trên vòng không còn thẻ bài lưu chuyển nữa.
- Một thẻ bài bận lưu chuyển không dừng trên vòng.



A có dữ liệu cần truyền đến C. Nhận được thẻ bài rồi nó đổi sang trạng thái bận và truyền dữ liệu đi cùng với thẻ bài

Trạm đích C sao dữ liệu dành cho nó và chuyển tiếp dữ liệu cùng thẻ bài đi về hướng trạm nguồn A sau khi đã gửi thông tin báo nhận và đơn vị dữ liệu

A nhận được dữ liệu cùng thẻ bài quay về, trạng thái của thẻ bài thành "rỗi" và chuyển tiếp trên vòng, xóa dữ liệu đã truyền

Hình 3.7 Truyền và nhận thẻ bài với phương pháp Token Ring

Giải quyết:

Đối với vấn đề mất thẻ bài, có thể quy định trước một trạm điều khiển chủ động. Trạm này sẽ phát hiện tình trạng mất thẻ bài bằng cách dùng cơ chế ngưỡng thời gian (time out) và phục hồi bằng cách phát đi một thẻ bài "rỗi" mới.

Đối với vấn đề thẻ bài bận lưu chuyển không dừng, trạm monitor sử dụng một bit trên thẻ bài (gọi là monitor bit) để đánh dấu đặt giá trị 1 khi gặp thẻ bài bận đi qua nó. Nếu nó gặp lại một thẻ bài bận với bit đã đánh dấu đó thì có nghĩa là trạm nguồn đã không nhận lại được đơn vị dữ liệu của mình và thẻ bài "bận" cứ quay vòng mãi. Lúc đó trạm monitor sẽ đổi bit trạng thái của thẻ thành rỗi và chuyển tiếp trên vòng. Các trạm còn lại sẽ có vai trò bị động: chúng theo dõi phát hiện tình trạng sự cố của trạm

monitor chủ động và thay thế vai trò đó. Cần giải thuật để chọn trạm thay thế cho trạm monitor hỏng.

3.4.5 So sánh các phương pháp

- Độ phức tạp của các phương pháp dùng thẻ bài đều lớn hơn nhiều so với CSMA/CD.
- Những công việc mà một trạm phải làm trong phương pháp CSMA/CD đơn giản hơn nhiều so với hai phương pháp dùng thẻ bài.
- Hiệu quả của phương pháp dùng thẻ bài không cao trong điều kiện tải nhẹ: một trạm phải đợi khá lâu mới đến lượt.

Tuy nhiên phương pháp dùng thẻ bài cùng có những ưu điểm: Khả năng điều hoà lưu thông trong mạng, hoặc bằng cách cho phép các trạm truyền số lượng đơn vị dữ liệu khác nhau khi nhận được thẻ bài, hoặc bằng cách lập chế độ ưu tiên cấp phát thẻ bài cho các trạm cho trước. Đặc biệt phương pháp dùng thẻ bài có hiệu quả cao hơn CSMA/CD trong trường hợp tải nặng.

3.5 MÔI TRƯỜNG TRUYỀN DẪN

3.5.1 Đường truyền hữu tuyến

3.5.1.1 Cáp xoắn

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

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

- Cáp có bọc kim loại: Lớp bọc bên ngoài có tác dụng chống nhiễu điện từ, có loại có một đôi dây xoắn vào nhau và có loại có nhiều đôi dây xoắn với nhau.
- Cáp không bọc kim loại: Tính tương tự như STP nhưng kém hơn về khả năng chống nhiễu và suy hao vì không có vỏ bọc.

(a) Cáp không bọc kim *(b) Cáp có bọc kim*

Hình 3.8 Cáp UTP và STP

Các đặc tính của cáp xoắn đôi là:

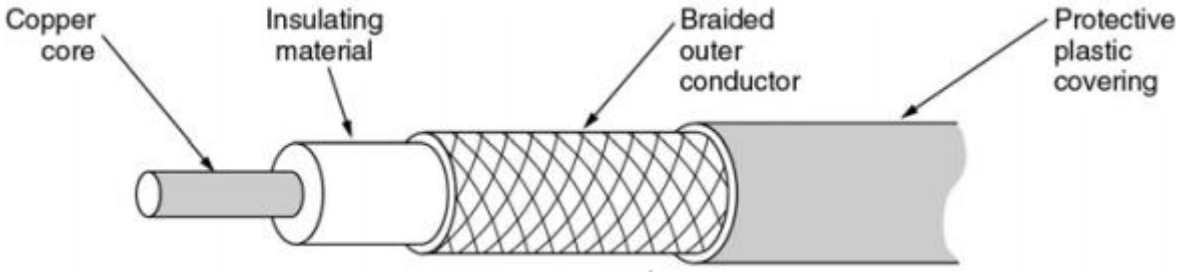
- Được sử dụng trong mạng token ring (cáp loại 4 tốc độ 16MBps), chuẩn mạng Ethernet 10BaseT (Tốc độ 10MBps), hay chuẩn mạng 100BaseT (tốc độ 100Mbps).
- Giá cả chấp nhận được
- UTP thường được sử dụng bên trong các tòa nhà vì nó ít có khả năng chống nhiễu hơn so với STP
- Cáp loại 2 có tốc độ đạt đến 1Mbps (cáp điện thoại)
- Cáp loại 3 có tốc độ đạt đến 10Mbps (dùng trong mạng Ethernet 10BaseT) (Hình a)

- Cáp loại 5 có tốc độ đạt đến 100MBps(dùng trong mạng 10BaseT, 100BaseT) (Hình b)
- Cáp loại 5E và loại 6 có tốc độ đạt đến 1000 MBps (dùng trong mạng 1000BaseT)

3.5.1.2Cáp đồng trục

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

Cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác (ví dụ như cáp xoắn đôi) do ít bị ảnh hưởng của môi trường. Các mạng cục bộ sử dụng cáp đồng trục có thể có kích thước trong phạm vi vài ngàn mét, cáp đồng trục được sử dụng nhiều trong các mạng dạng đường thẳng.



Hình 3.9 Cáp đồng trục

Hai loại cáp thường được sử dụng là cáp đồng trục gầy và cáp đồng trục béo

- Cáp đồng trục gầy, ký hiệu RG-58AU, Hình 3.10 là cáp đồng trục gầy, được dùng trong chuẩn mạng Ethernet 10Base2.
- Cáp đồng trục béo, ký hiệu RG-11, được dùng trong chuẩn mạng 10Base5

Các loại đầu nối được sử dụng với cáp đồng trục gầy là đầu nối chữ T (T connector), đầu nối BNC và thiết bị đầu cuối (Terminator)

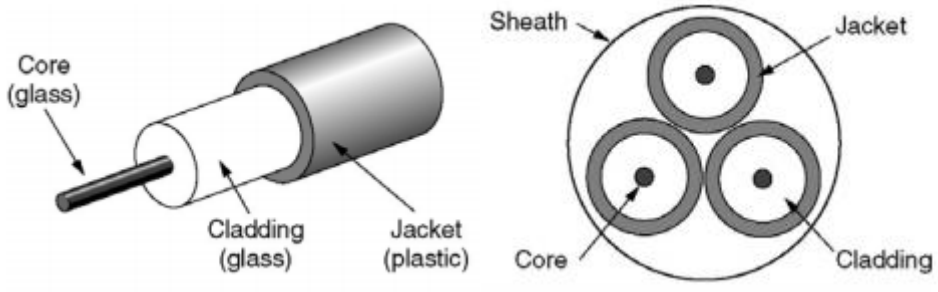
Hình 3.10 Đầu nối chữ T và BNC

Các mạng cục bộ thường sử dụng cáp đồng trục có dải thông từ 2,5 - 10 Mb/s, cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác vì nó có lớp vỏ bọc bên

ngoài, độ dài thông thường của một đoạn cáp nối trong mạng là 200m, thường sử dụng cho dạng Bus.

3.5.1.3Cáp sợi quang (Fiber - Optic Cable)

Cáp quang truyền tải sóng điện từ dưới dạng ánh sáng. Sự xuất hiện của một sóng ánh sáng tương ứng với bit "1"và sự mất ánh sáng tương ứng với bit "0". Các tín hiệu điện tử được chuyển sang tín hiệu ánh sáng bởi bộ phát, sau đó các tín hiệu ánh sáng sẽ được chuyển thành các sung điện tử bởi bộ nhận. Nguồn phát quang có thể là các đèn LED (*Light Emitting Diode*) cổ điển, hay các diod laser. Bộ dò ánh sáng có thể là các tế bào quang điện truyền thống hay các tế bào quang điện dạng khối.



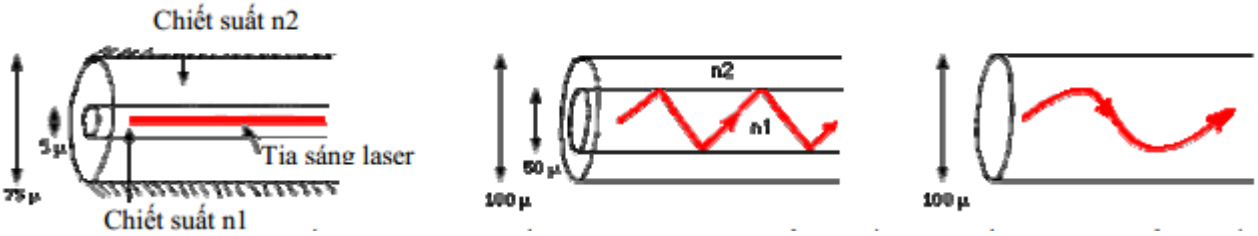
(a) *(b)*

Hình 3.11 Cấu trúc cáp quang

Sự lan truyền tín hiệu được thực hiện bởi sự phản xạ trên bề mặt. Thực tế, tồn tại 3 loại cáp quang.

- Chế độ đơn: một tia sáng trên đường truyền tải.
- Hai chế độ còn lại gọi là chế độ đa: nhiều tia sáng được truyền song song nhau.

Trong chế độ đơn, chiết suất n2 > n1. Tia laser có bước sóng từ 5 đến 8 micromètres được tập trung về một hướng. Các sợi loại này cho phép tốc độ bit cao nhưng khó xử lý và phức tạp trong các thao tác nối kết.



Hình 3.12 Cáp quang chế độ đơn - chế độ đa không thẩm thấu - chế độ đa thẩm thấu

- Chế độ đa không thẩm thấu

Các tia sáng di chuyển bằng cách phản xạ giữa bề mặt của 2 môi trường có chiết suất khác nhau (n2>n1) và mất nhiều thời gian hơn để các sóng di chuyển so với chế độ đơn. Độ suy giảm đường truyền từ 30 dB/km đối với các loại cáp thủy tinh và từ 100 dB/km đối với loại cáp bằng chất dẽo.

- Chế độ đa bị thẩm thấu

Chiết suất tăng dần từ trung tâm về vỏ của ống. Vì thế sự phản xạ trong trường hợp này thì rất nhẹ nhàng.

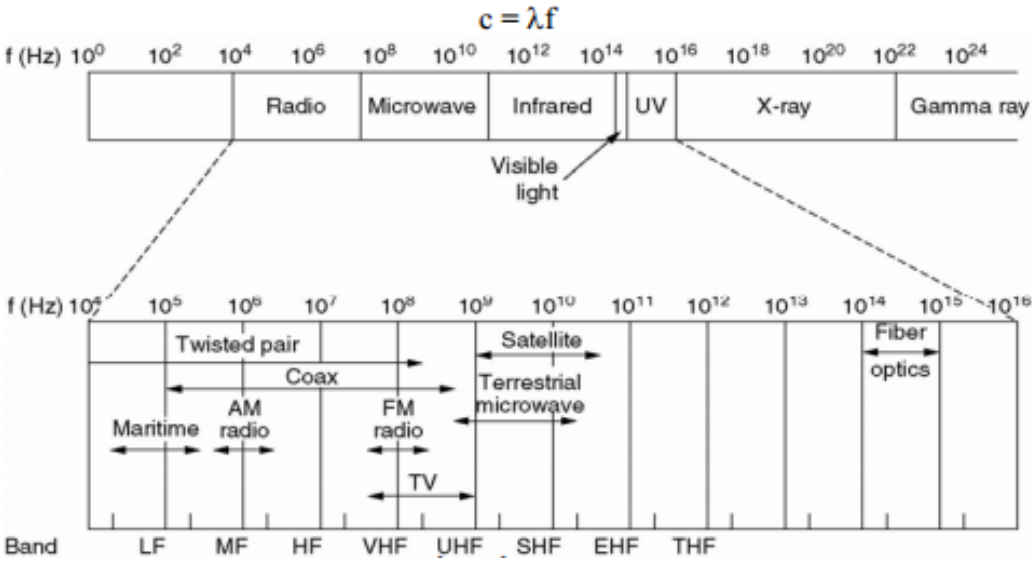
Từ cách đây nhiều năm người ta có thể thực hiện đa hợp trên cùng một sợi quang nhiều thông tin bằng cách dùng các sóng có độ dài khác nhau. Kỹ thuật này được gọi là WDM (*Wavelength Division Multiplexing*).

3.5.2 Đường truyền vô tuyến

Kênh truyền vô tuyến thì thật sự tiện lợi cho tất cả chúng ta, đặc biệt ở những địa hình mà kênh truyền hữu tuyến không thể thực hiện được hoặc phải tốn nhiều chi phí (rừng, hải đảo, miền núi). Kênh truyền vô tuyến truyền tải thông tin ở tốc độ ánh sáng. Gọi:

- c là tốc độ ánh sáng,
- f là tần số của tín hiệu sóng
- λ là độ dài sóng.

Khi đó ta có:



Hình 3.13 Phân bổ phổ sóng điện từ

Tín hiệu có độ dài sóng càng lớn thì khoảng cách truyền càng xa mà không bị suy giảm, ngược lại những tín hiệu có tần số càng cao thì có độ phát tán càng thấp. Hình 3.13mô tả phổ của sóng điện từ được dùng cho truyền dữ liệu. Khoảng tần số càng cao càng truyền tải được nhiều thông tin.

3.5.2.1 Sóng hồng ngoại

- Môi trường định hướng.
- Thích hợp cho mạng diện hẹp bán kính 0.5m – 20m với các thiết bị ít duy chuyển, không có vật cản sóng ánh sáng trên hướng thu phát.
- Tốc độ truyền dữ liệu xung quanh là 10Mbps.

3.5.2.2 Sóng Laser

- Môi trường định hướng.
- Diện rộng với bán kính đến 20km.
- Dùng liên kết LAN trong môi trường không có điều kiện thi công cáp quang.
- Tốc độ truyền hàng chục Mbps.

3.5.2.3 Sóng radio

- Môi trường không định hướng.
- Diện rộng với bán kính đến 30km.
- Dùng trong liên kết LAN
- Tốc độ truyền hàng chục Mbps

3.6 THIẾT BỊ CẤU THÀNH MẠNG MÁY TÍNH

Máy chủ (*file server - FS*), các trạm làm việc (*Workstation - WS*), các thiết bị ngoại vi dùng chung (máy in, ổ đĩa cứng...), card mạng, các đầu nối, đường truyền, và một số thiết bị khác như Hub, Switch.

3.6.1 Máy chủ

- Hoạt động như máy chính của mạng, quản lý các hoạt động của mạng (như phân chia tài nguyên chung, trao đổi thông tin giữa các trạm,..). Thông thường máy chủ còn đặt cơ sở dữ liệu dùng chung. Thường thì máy chủ có cấu hình mạnh.
- Trong dạng mạng ngang hàng (*Peer to Peer*) thì không có máy chủ.

3.6.2 Các trạm làm việc

- Là các máy tính cá nhân kết nối với nhau và nối với máy chủ.
- Các máy trạm có thể sử dụng tài nguyên chung của toàn bộ hệ thống mạng.

3.6.3 Card mạng (NIC)

- Là thiết bị để điều khiển việc truyền thông và chuyển đổi dữ liệu sang dạng tín hiệu điện hay quang.
- Gồm các bộ điều khiển và thu phát thông tin:

Bộ điều khiển thực hiện các chức năng điều khiển truyền thông, đảm bảo dữ liệu được truyền chính xác tới các nút mạng.

Bộ thu phát thông tin làm nhiệm vụ chuyển dữ liệu sang dạng tín hiệu điện hay quang và ngược lại.

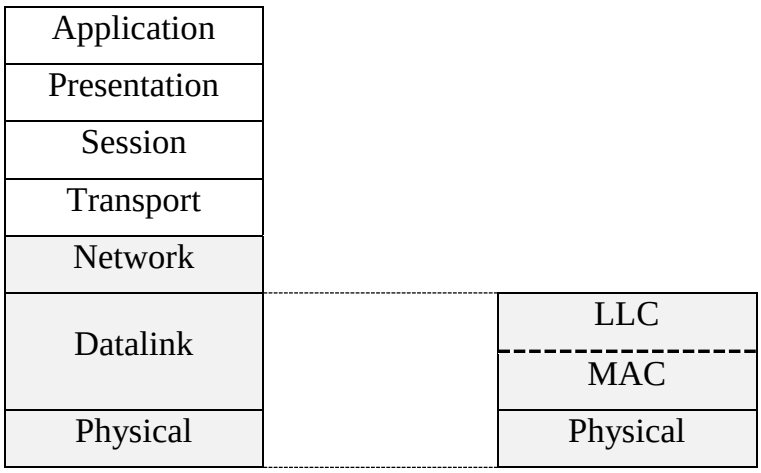
- Tuỳ theo yêu cầu sử dụng lựa chọn card mạng cho phù hợp với máy tính, đường truyền dẫn, nhu cầu phát triển trong tương lai.

3.6.4 Đường truyền

- Là môi trường truyền dẫn, liên kết các nút mạng, truyền dẫn các tín hiệu điện hay quang.
- Mạng cục bộ sử dụng chủ yếu là các loại cáp, trong đó có hai loại cáp thường được sử dụng: cáp đồng trục, cáp đôi dây xoắn.

3.7 CÁC CHUẨN MẠNG LAN

Ngoài mô hình OSI dùng cho việc chuẩn hóa các mạng nói chung, việc chuẩn hóa mạng cục bộ cũng đã được thực hiện trong một khoảng thời gian dài. Do đặc trưng riêng, việc chuẩn hóa mạng cục bộ chỉ được thực hiện trên hai tầng thấp nhất, tương ứng với tầng vật lý và liên kết dữ liệu trong mô hình OSI.



Mô hình tham khảo OSI *Mô hình tham khảo cho mạng LAN*

Hình 3.14 Mô hình phân tầng của mạng cục bộ

Trong LAN, tầng liên kết dữ liệu được chia làm hai tầng con: LLC (*Logical Link Layer*) và MAC. MAC quản lý việc truy cập đường truyền, trong khi LLC đảm bảo tính độc lập của việc quản lý các liên kết dữ liệu với đường truyền vật lý và phương pháp truy cập đường truyền MAC.

IEEE (*Institute of Electrical and Electronic Engineers*) là tổ chức đi tiên phong trong lĩnh vực chuẩn hóa mạng cục bộ với dự án IEEE 802 nổi tiếng bắt đầu được triển khai từ năm 1980 và kết quả là hàng loạt chuẩn thuộc họ IEEE 802.x ra đời, tạo nền tảng quan trọng cho việc thiết kế và cài đặt mạng nội bộ trong thời gian qua. Vị trí của họ chuẩn này càng cao hơn khi ISO đã xem xét và tiếp nhận chúng thành chuẩn quốc tế mang tên 8802.x.

Đến nay họ IEEE 802.x bao gồm các chuẩn sau:

IEEE 802.1 : High Level Interface

IEEE 802.2 : Logical Link Control

(LLC) IEEE 802.3: CSMA/CD

IEEE 802.4: Token bus

IEEE 802.5: Token ring

IEEE 802.6: MAN

IEEE 802.7: Broadband Technical Advisory Group

IEEE 802.8: Fiber Technical Advisory Group

IEEE 802.9: Intergrated Data and Voice Network

IEEE 802.10: Standard for Interoperable LAN security

IEEE 802.11: Wireless LAN

IEEE 802.12: 100VG – AnyLAN

- IEEE 802.1 là chuẩn đặc tả kiến trúc mạng, nối kết giữa các mạng và việc quản trị mạng đối với mạng cục bộ.
- IEEE 802.2 là chuẩn đặc tả tầng LLC (dịch vụ, giao thức) của mạng cục bộ.

Có 3 kiểu giao thức LLC chính được định nghĩa:

LLC type 1: Là giao thức kiểu không liên kết, không báo nhận.
LLC type 2: Là giao thức kiểu có liên kết.
LLC type 3: Là giao thức dạng không liên kết, có báo nhận.

Các giao thức này được xây dựng dựa theo phương thức cân bằng của giao thức HDLC và có các khuôn dạng dữ liệu và các chức năng tương tự, đặc biệt là trong trường hợp LLC-type 2.

- IEEE 802.3: Là chuẩn đặc tả một mạng cục bộ dựa trên mạng Ethernet nổi tiếng do Digital, Intel và Xerox hợp tác phát triển từ năm 1990. IEEE 802.3 bao gồm cả tầng vật lý và tầng con MAC với các đặc tả sau:
  - ✓ Đặc tả dịch vụ MAC.
  - ✓ Giao thức MAC.
  - ✓ Đặc tả vật lý độc lập với đường truyền.
  - ✓ Đặc tả vật lý phụ thuộc vào đường truyền. Phần cốt lõi của IEEE 802.3 là giao thức MAC dựa trên phương pháp CSMA/CD đã trình bày phần trước.
- IEEE 802.4 là chuẩn đặc tả mạng cục bộ với hình trạng bus sử dụng thẻ bài để điều khiển truy cập đường truyền. IEEE 802.4 cũng bao gồm cả tầng vật lý và tầng con MAC với các đặc tả sau:
  - ✓ Đặc tả dịch vụ MAC.
  - ✓ Giao thức MAC.
  - ✓ Đặc tả dịch vụ tầng vật lý.
  - ✓ Đặc tả thực thể tầng vật lý.
  - ✓ Đặt tả đường truyền.
- IEEE 802.5 là chuẩn đặc tả mạng cục bộ với hình trạng vòng sử dụng thẻ bài để điều khiển truy cập đường truyền. IEEE 802.5 cũng bao gồm cả tầng vật lý và tầng con MAC với các đặc tả sau:
  - ✓ Đặc tả dịch vụ MAC.
  - ✓ Giao thức MAC.
  - ✓ Đặc tả thực thể tầng vật lý.
  - ✓ Đặc tả nối trạm.
- IEEE 802.6 là chuẩn đặc tả một mạng tốc độ cao nối kết nhiều LAN thuộc các khu vực khác nhau của một đô thị. Mạng này sử dụng cáp quang với hình trạng dạng bus kép (dual-bus), vì thế còn được gọi là DQDB *(Distributed Queue Dual Bus)*. Lưu thông trên mỗi bus là một chiều và khi cả cặp bus cùng hoạt động sẽ tạo thành một cấu hình chịu lỗi. Phương pháp điều khiển truy cập dựa theo một giải thuật xếp hàng phân tán có tên là QPDS *(Queued-Packet, Distributed-Switch)*.
- IEEE 802.9 là chuẩn đặc tả một mạng tích hợp dữ liệu và tiếng nói bao gồm 1 kênh dị bộ 10 Mbps cùng với 95 kênh 64 Kbps. Dải thông tổng cộng 16 Mpbs.

Chuẩn này được thiết kế cho các môi trường có lưu lượng lưu thông lớn và cấp bách.

- IEEE 802.10 là chuẩn đặc tả về an toàn thông tin trong các mạng cục bộ có khả năng liên tác.
- IEEE 802.11 là chuẩn đặc tả mạng LAN không dây (Wireless LAN). Xu hướng chọn phương pháp truy cập CSMA được khẳng định.
- IEEE 802.12 là chuẩn đặc tả mạng cục bộ dựa trên công nghệ được đề xuất bởi AT&T, IBM và HP, gọi là 100VG – AnyLAN. Mạng này sử dụng hình trạng mạng hình sao và một phương pháp truy cập đường truyền có điều khiển tranh chấp. Khi có nhu cầu truyền dữ liệu, trạm sẽ gởi yêu cầu đến hub và trạm chỉ có thể truyền dữ liệu khi được hub cho phép. Chuẩn này nhằm cung cấp một mạng tốc độ cao (100Mbps và có thể lớn hơn) có thể hoạt động trong các môi trường hỗn hợp Ethernet và Token Ring, bởi thế nó chấp nhận cả hai dạng khung 100VG – AnyLAN là đối thủ cạnh tranh đáng gờm của 100BASE-T (Fast Ethernet) nhờ một số tính năng trội hơn, chẳng hạn về khoảng cách đi cáp tối đa cho phép…

3.7.1 Chuẩn Ethernet (IEEE802.3)

Các chuẩn Ethernet LAN hiện đang sử dụng phổ biến nhất, đến mức đôi khi hiểu đồng nghĩa với LAN. Sự phát triển của nó trải qua các giai đoạn với tên gọi là DIX standard Ethernet và IEEE802.3 standard.

Năm 1972 công ty Xerox triển khai nghiên cứu về chuẩn LAN. 1980 chuẩn này được 3 công ty DEC (Digital), Intel, Xerox chấp nhận phát triển và gọi là chuẩn DIX Ethernet. Nó đảm bảo tốc độ truyền thông 10Mpbs, dùng môi trường truyền dẫn là cáp đồng trục béo, cơ chế truyền tin CSMA/CD.

IEEE (*Institute of Electrical and Electrionics Engineers*) - một tổ chức chuẩn hoá của Mỹ đưa ra chuẩn IEEE802.3 về giao thức LAN dựa trên DIX Ethernet với các môi trường truyền dẫn khác nhau, gọi là IEEE802.3: 10BASE-5, 10BASE-2 và 10BASE-T. Đảm bảo tốc độ truyền thông 10Mbps.

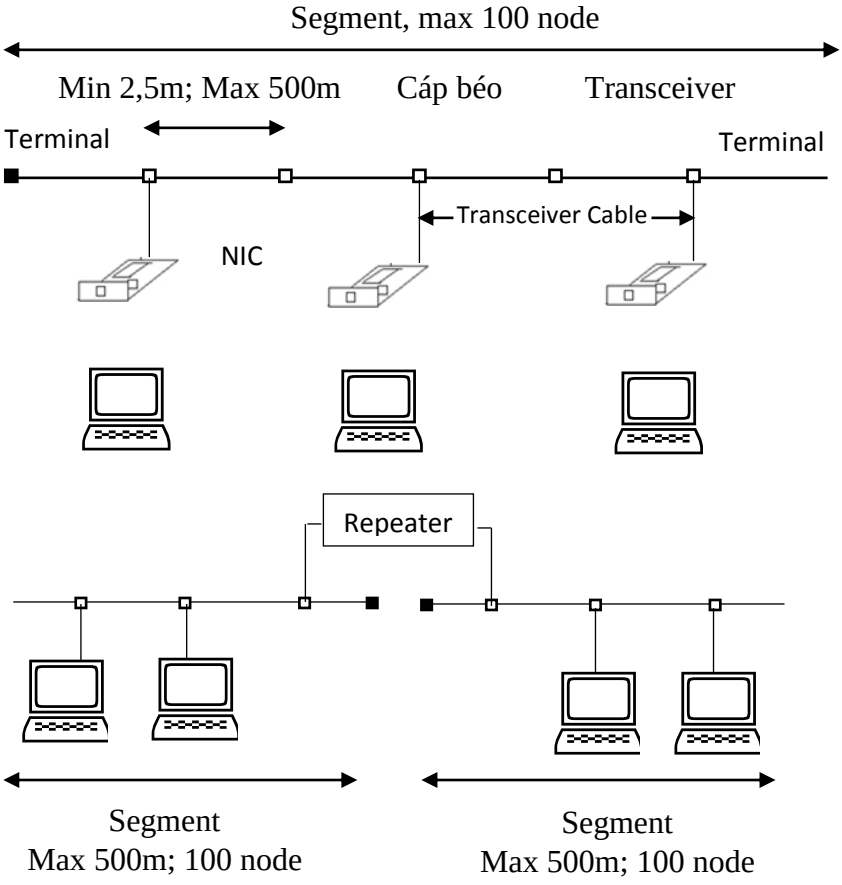
3.7.1.1 10BASE-5

- *Mô hình phần cứng của mạng*
  - ✓ Topo dạng BUS
  - ✓ Dùng cáp đồng trục béo 50 Ω còn gọi là cáp vàng, AUI connector *(AttachementUnit Interface)*
  - ✓ Hai đầu cáp có hai Terminator 50 Ω, chống phản hồi sóng mang tín hiệu. Dữ liệu truyền thông sẽ không được đảm bảo đúng đắn nếu một trong hai Terminator này bị thiếu hoặc bị lỗi.
  - ✓ Trên mỗi đoạn cáp có thể liên kết tối đa 100 AUI Transceiver Connector "cái". Khoảng cách tối đa giữa hai AUI là 2,5 m; khoảng cách tối đa là 500m trên cáp có đánh các dấu hiệu theo từng đoạn bội số của 2,5m và để đảm bảo truyền thông. Người ta thường chọn khoảng cách tối thiểu giữa hai AUI là 5m.
  - ✓ Việc liên kết các máy tính vào mạng được thực hiện bởi các đoạn cáp nối từ các AUI connector đến NIC trong máy tính, gọi là cáp AUI. Hai đầu cáp AUI

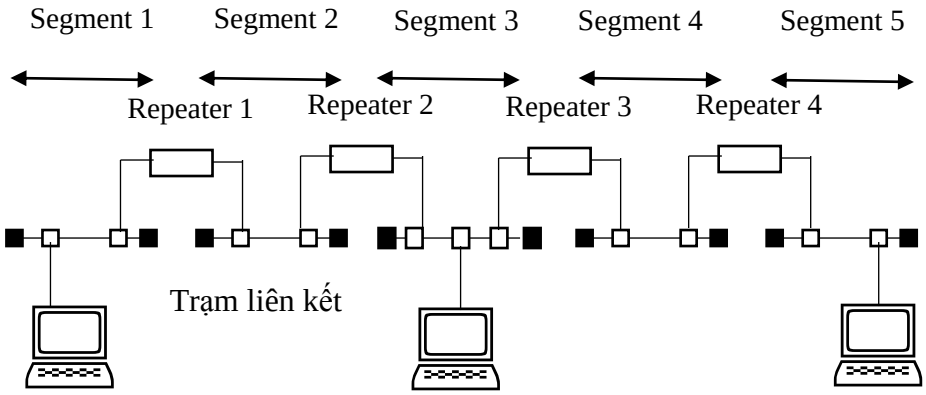
liên kết với hai AUI connector "đực". Chiều dài tối đa của một cáp AUI là 50m.

- ✓ Số 5 trong tên gọi 10BASE-5 là bắt nguồn từ điều kiện khoảng cách tối đa giữa hai AUI trên cáp là 500m.

- *Quy tắc 5- 4-3*
  - ✓ Repeater: Như đã trình bày ở trên, trong mỗi đoạn mạng dùng cáp đồng trục béo không được có quá 100 AUI, khoảng cách tối đa giữa hai AUI không được vượt quá 500m. Trong trường hợp muốn mở rộng mạng với nhau bằng một thiết bị chuyển tiếp tín hiệu gọi là Repeater. Repeater có hai cổng, tín hiệu được nhận vào ở cổng này thì sẽ được phát tiếp ởcổng kia sau khi đã được khuyếch đại. Tuy nhiên có những hạn chế bắt buộc về số lượng các đoạn mạng và nút mạng có thể có trên một Ethernet LAN.
  - ✓ Quy tắc 5 – 4-3 là quy tắc tiêu chuẩn của Ethernet được áp dụng trong trường hợp muốn mở rộng mạng, nghĩa là muốn xây dựng một LAN có bán kính hoạt động rộng hoặc có nhiều trạm làm việc vượt quá những hạn chế trên một đoạn cáp mạng (segment).
  - ✓ Quy tắc 5 – 4-3 được áp dụng cho chuẩn 10BASE-5 dùng Repeater như sau:
    - Không được có quá 5 đoạn mạng
    - Không được có quá 4 Repeater giữa hai trạm làm việc bất kỳ
    - Không được có quá 3 đoạn mạng có trạm làm việc. Các đoạn mạng không có trạm làm việc gọi là các đoạn liên kết.



Hình 3.15 Mở rộng chuẩn 10Base5 bằng repeater



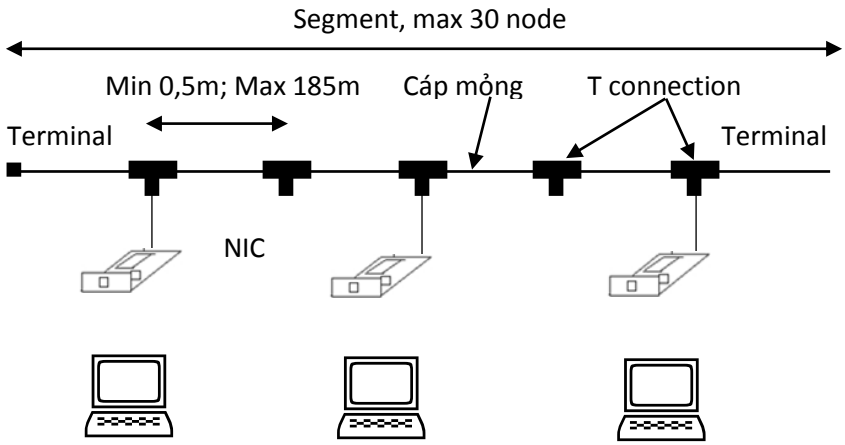
Hình 3.16 Luật 5 – 4 – 3

3.7.1.2 10BASE-2

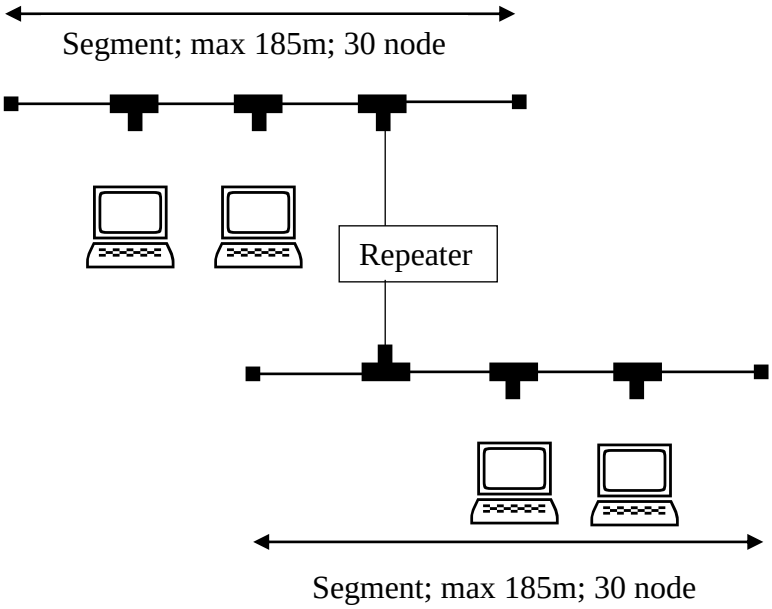
- *Mô hình phần cứng:*
  - ✓ Topo dạng BUS
  - ✓ Dùng cáp đồng trục mỏng 50 Ω, đường kính xấp xỉ5mm, T-connector, BNCconnector.
  - ✓ Hai đầu cáp có hai Terminator 50 Ω, chống phản hồi sóng mang dữ liệu. Dữ liệu truyền thông sẽ không được đảm bảo đúng đắn nếu một trong hai Terminator này bị thiếu hoặc bị lỗi.
  - ✓ Trên mỗi đoạn cáp có thể liên kết tối đa 30 trạm làm việc. Khoảng cách tối thiểu giữa hai trạm là 0.5m. Khoảng cách tối đa giữa hai trạm là 185m. Để bảo đảm chất lượng truyền thông người ta thường chọn khoảng cách tối thiểu giữa hai trạm là 5m.
  - ✓ Việc liên kết các máy tính vào mạng được thực hiện bởi các T- connector và BNC
  - ✓ Số 2 trong tên gọi 10BASE-2 là bắt nguồn từ điều kiện khoảng cách tối đa giữa hai trạm trên đoạn cáp là 185m ≈ 200m.
- *Quy tắc 5 - 4 -3*

Quy tắc 5 – 4 - 3 được áp dụng cho chuẩn 10BASE-2 dùng Repeater cũng tương tự như đối với trường hợp cho chuẩn 10BASE-5

- ✓ Không được có quá 5 đoạn mạng.
- ✓ Không được có quá 4 repeater giữa hai trạm làm việc bất kỳ.
- ✓ Không được có quá 3 đoạn mạng có trạm làm việc. Các đoạn mạng không có trạm làm việc gọi là các đoạn liên kết.



Hình 3.17 Chuẩn 10 Base-2

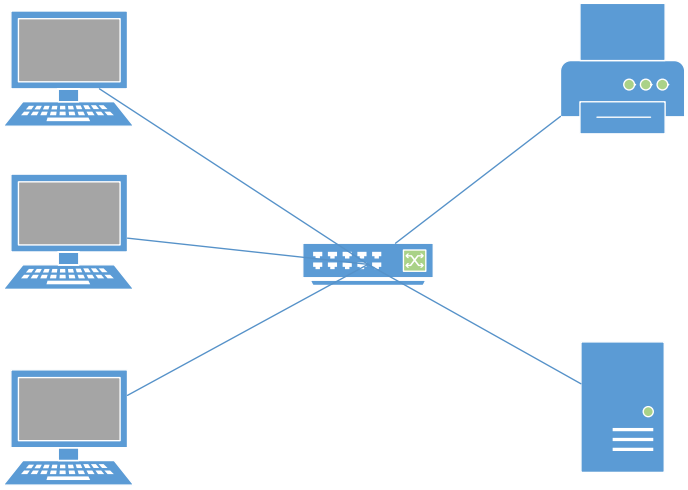


Hình 3.18 Mở rộng chuẩn 10 Base-5 bằng repeater

3.7.1.310BASE-T

♦ *Mô hình phần cứng của mạng*

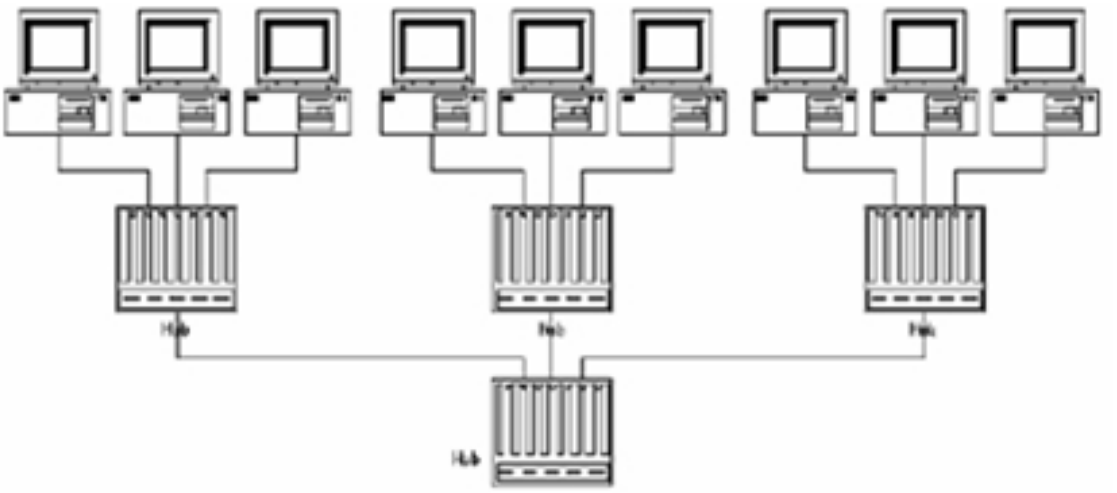
- ✓ Dùng cáp UTP, RJ 45 connector và thiết bị ghép nối trung tâm gọi là HUB.
- ✓ Mỗi HUB có thể nối từ 4 tới 24 cổng RJ45, các trạm làm việc được kết nối từ NIC tới cổng HUB bằng cáp UTP với hai đầu RJ45.
- ✓ Về mặt vật lý (hình thức) topo của mạng có dạng hình sao.
- ✓ Tuy nhiên về bản chất HUB là một loại Repeater nhiều cổng vì vậy về mặt logic, mạng theo chuẩn 10BASE-T vẫn là mạng dạng BUS.
- ✓ Chữ T trong tên gọi 10BASE-T bắt nguồn từ chữ Twisted pair cable.



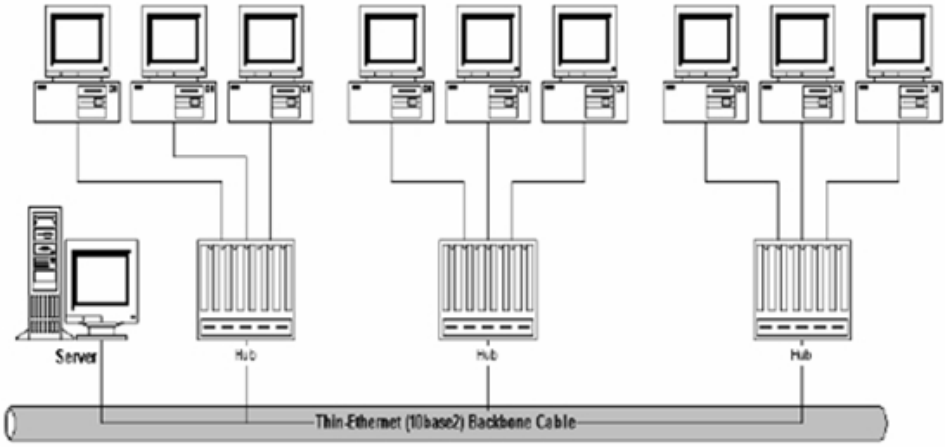
Hình 3.19 Chuẩn 10 Base- T

♦ *Quy tắc mở rộng mạng*

- ✓ Vì HUB là một loại Repeater nhiều cổng nên để mở rộng mạng có thể liên kết nối tiếp các HUB với nhau và cũng không được có quá 4 HUB giữa hai trạm làm việc bất kỳ của mạng.
- ✓ HUB có khả năng xếp chồng: là loại HUB có cổng riêng để liên kết các chúng lại với nhau bằng cáp riêng thành như một HUB. Như vậy dùng loại HUB này người dùng có thể dễ dàng mở rộng số cổng của HUB trong tương lai khi cần thiết. Tuy nhiên số lượng HUB có thể xếp chồng cũng có giới hạn và phụ thuộc vào từng nhà sản xuất, thông thường không vượt quá 5 HUB.
- ✓ 10BASE-2 với HUB: HUB có khả năng xếp chồng, người sử dụng có thể tăng số lượng máy kết nối trong mạng nhưng bán kính hoạt động của mạng vẫn không thay đổi vì khoảng cách từ cổng HUB đến NIC không thể vượt quá 100m. Một giải pháp để có thể mở rộng được bán kính hoạt động của mạng là dùng HUB có hỗ trợ một cổng AUI để liên kết các HUB bằng cáp đồng trục béo theo chuẩn 10BASE-2 (hoặc 10Base-5). Một cáp đồng trục béo theo chuẩn 10BASE-5 có chiều dài tối đa là 500m.



Hình 3.20 Mở rộng mạng 10BaseT khi số Hub nhiều hơn 4



Hình 3.21 Mở rộng mạng 10 Base T với mạng10 Base-2 làm trục chính

3.7.2 Token Ring

Chuẩn Token Ring hay còn được gọi rõ hơn là IBM Token Ring được phát triển bởi IBM, đảm bảo tốc độ truyền thông qua 4Mbps hoặc 16Mbps. Chuẩn này được IEEE chuẩn hoá với mã IEEE 802.5 và được ISO công nhận với mã ISO 8802.5.

♦ *Mô hình phần cứng*

- ✓ Topo hình vòng tròn
- ✓ Dùng các MAU (multistation Access Unit) nhiều cổng MAU và cáp STP để liên kếtcác MAU thành một vòng tròn khép kín.
- ✓ Các trạm làm việc được liên kết vào mạng bằng các đoạn cáp STP nối từ cổng MAU tới cổng của NIC. Chiều dài đoạn cáp này được quy định dưới 100m. Số lượngtối đa các trạm làm việc trên một Ring là 72 (4Mbps) và 260 (16Mbps) khoảng cách tối đa giữa hai trạm là 770m (4Mbps) và 346 (16Mbps).
- ✓ Hiện tại chuẩn mạng này cũng đã hỗ trợ sử dụng cáp UTP với connector RJ45 và cáp sợi quang với connector SC.

♦ *Cơ chế thâm nhập*

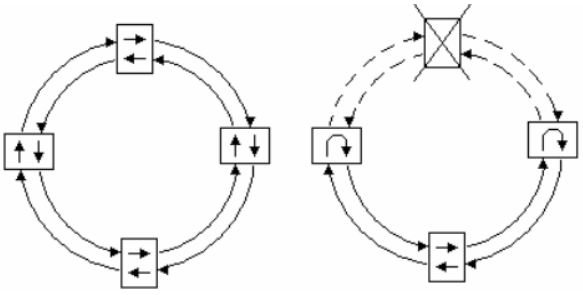
Thâm nhập theo cơ chế phân phối lần lượt theo thẻ bài (Token)

3.7.3 FDDI (Fiber Distributed Data Interface)

Được chuẩn hoá bởi ANSI, đảm bảo tốc độ đường truyền 100Mbps.

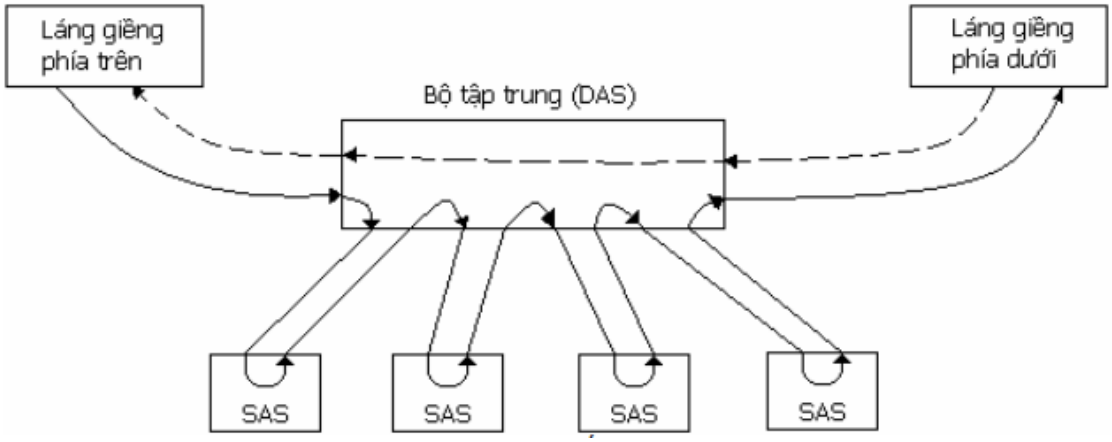
♦ *Mô hình phần cứng*

Không giống như mạng 802.5, một mạng FDDI bao gồm một vòng đôi bằng hai vòng độc lập truyền dữ liệu theo hai chiều ngược nhau (xem Hình 3.22.a).



a) hoạt động bình thường; b) vòng chính bị hỏng
Hình 3.22 Vòng quang đôi

Vòng phụ không được sử dụng trong khi hệ thống hoạt động bình thường, nó chỉ vào cuộc khi vòng chính bị sự cố (xem Hình 3.22 b). Nghĩa là vòng chính sẽ quành lại vòng phụ để tạo ra một vòng hoàn chỉnh, và chính điều này giúp cho FDDI có khả năng chịu lỗi khi một cộng cáp bị đứt hay một trạm trong vòng bị hỏng. Do phải chịu phí tổn khi cấu hình theo kiểu vòng đôi, nên FDDI còn cho phép một trạm chọn nối vào chỉ một vòng đơn thôi. Những trạm như vậy gọi là những "trạm nối đơn" *(Single Attachment Station – SAS)*. Những trạm nối cả vào hai vòng dĩ nhiên sẽ được gọi là những "trạm đấu đôi" *(Dual Attachment Station – DAS)*. Một bộ tập trung (concentrator) sẽ được sử dụng để nối các SAS vào vòng đôi (xem Hình 3.23)



Hình 3.23 Các SAS được nối vào bộ tập trung

Nếu một SAS bị hỏng, bộ tập trung sẽ phát hiện ra tình trạng này và sử dụng cơ chế bỏ qua tín hiệu quang để cô lập SAS bị hỏng, vì thế giữ cho vòng được thông suốt.

Trong FDDI, bộ đệm của giao diện mạng có thể có kích thước khác nhau tại những trạm khác nhau, mặc dù kích thước của nó không bao giờ nhỏ hơn 9 bit và lớn hơn 80 bit. Một trạm cũng có thể bắt đầu phát các bit trong bộ đệm đi trước khi bộ đệm của nó bị đầy. Dĩ nhiên là tổng thời gian để một thẻ bài di chuyển hết một vòng là một hàm của kích thước của các bộ đệm này. Ví dụ, FDDI là mạng tốc độ 100 Mbps, nó có thời gian xử lý 1 bit là 10ns. Nếu mỗi trạm cài đặt buffer dài 10 bit và chờ cho đến khi buffer bị đầy một nửa mới bắt đầu truyền, thì mỗi trạm tạo ra thời gian trì hoãn là 5×10ns = 50ns đối với tổng thời gian xoay vòng mạng.

FDDI còn có các tính chất vật lý khác. Chẳng hạn, một mạng đơn có giới hạn chuẩn là có tối đa 500 trạm làm việc với khoảng cách xa nhất giữa một cặp trạm bất kỳ là 2 km. Nhưng trên hết, mạng lại bị giới hạn với kích thước tổng cộng là 200 km cáp quang. Do tính chất là vòng đôi nên tổng kích thước cáp quang nối tất cả các trạm là 100 km. Ngoài ra, mặc dù ký tự "F" ám chỉ cáp quang, nhưng chuẩn FDDI đã được định nghĩa để có thể chạy trên một số thiết bị tải khác, bao gồm cả cáp đồng trục và cáp xoắn đôi. Tuy nhiên cũng nên cẩn thận khi xét đến tổng kích thước mà vòng bao phủ và lượng thời gian bỏ ra để cho thẻ bài đi hết một vòng mạng sẽ đóng vai trò quan trọng trong giải thuật điều khiển truy cập.

FDDI sử dụng phương pháp mã hóa 4B/5B. Do FDDI chuẩn mạng phổ biến đầu tiên sử dụng cáp quang, nên các con chíp mã hóa dạng 4B/5B chạy trên tốc độ của FDDI có rất nhiều ngoài thị trường.

♦ *Cơ chế thâm nhập*: Dùng cơ chế thẻ bài

3.8 CÁC BƯỚC THỰC HIỆN THIẾT KẾ MẠNG

Thiết kế mạng là công việc dựa trên sự phân tích đánh giá khối lượng thông tin phải xử lý và giao tiếp trong hệ thống để xác định mô hình mạng, phần mềm và tập hợp các máy tính, thiết bị, vật liệu xây dựng mạng. Các bước và trình tự thực hiện trong công tác thiết kế mạng được thực hiện như sau:

Bước 1: Phân tích

Mạng máy tính là cơ sở hạ tầng của hệ thống thông tin. Vì vậy trước khi thiết kế mạng phải phân tích hệ thống thông tin.

Mục đích của phân tích là để hiểu được nhu cầu về mạng của hệ thống của người sử dụng. Để thực hiện được mục đích đó phải phân tích tất cả các chức năng nghiệp vụ, giao dịch của hệ thống.

Trong giai đoạn phân tích yêu cầu cần tránh những định kiến chủ quan về khả năng, cách thức sử dụng mạng cũng như những nghiệp vụ không thể thực hiện trên máy tính, trên mạng.

Bước 2: Đánh giá lưu lượng truyền thông

Việc đánh giá lưu lượng truyền thông dựa trên các nguồn thông tin chủ yếu:

- ✓ Lưu lượng truyền thông đòi hỏi bởi mỗi giao dịch.
- ✓ Giờ các điểm của các giao dịch.
- ✓ Sự gia tăng lưu lượng truyền thông trong tương lai.

Để đơn giản, có thể đưa ra các giả định lượng ở bước cơ sở để tiến hành tính toán được ở bước sau. Cũng có thể giả thuyết rằng mỗi giao dịch cùng sử dụng một khối lượng như nhau về dữ liệu và có lưu lượng truyền thông giống nhau.

Để xác định giờ cao điểm và tính toán dung lượng truyền thông trong giờ cao điểm cần thống kê dung lượng truyền thông trong từng giờ làm việc hằng ngày (D). Giờ cao điểm là giờ có dung lượng truyền thông cao nhất trong ngày (H).

Tỷ số giữa dung lượng truyền thông trong giờ cao điểm trên dung lượng truyền thông hàng ngày gọi là độ tập trung truyền thông cao điểm (R=H/D).

Sự gia tăng dung lượng truyền thông trong tương lai có thể đến vì 2 lý do (a):

- ✓ Sự tiện lợi của hệ thống sau khi nó được hoàn thành người dùng sử dụng tự do.
- ✓ Sự tiện lợi của hệ thống sau khi nó được hoàn thành làm người dùng sử dụng nó thường xuyên hơn.

Nhu cầu mở rộng hệ thống do sự mở rộng hoạt động của các cơ quan trong tương lai (b)

Công thức sau dùng để tính toán dung lượng truyền thông trong giờ cao điểm trong tương lai:

$$Tn = D\ (R/100)\ (1+a)\ (1+b)^n$$

Trong đó:

n là số năm kể từ thời điểm hiện tại

Tn là dung lượng truyền thông trong giờ cao điểm n năm sau.

D là dung lượng truyền thông trong ngày tại thời điểm hiện tại.

a là tỷ lệ gia tăng truyền thông vì sự hiện tiện lợi.

b là tỷ lệ gia tăng truyền thông hằng năm.

Bước 3: Tính toán số lượng trạm làm việc

Có hai phương pháp tính toán số trạm làm việc cần thiết.

- ✓ Tính số trạm làm việc cho mỗi người
- ✓ Tính số trạm làm việc cần thiết để hoàn thành giao dịch trong các hoàn cảnh:
  - Số trạm làm việc cần thiết để hoàn thành giao dịch trong giờ cao điểm.
  - Số trạm làm việc cần thiết để hoàn thành tất cả các giao dịch hàng ngày.

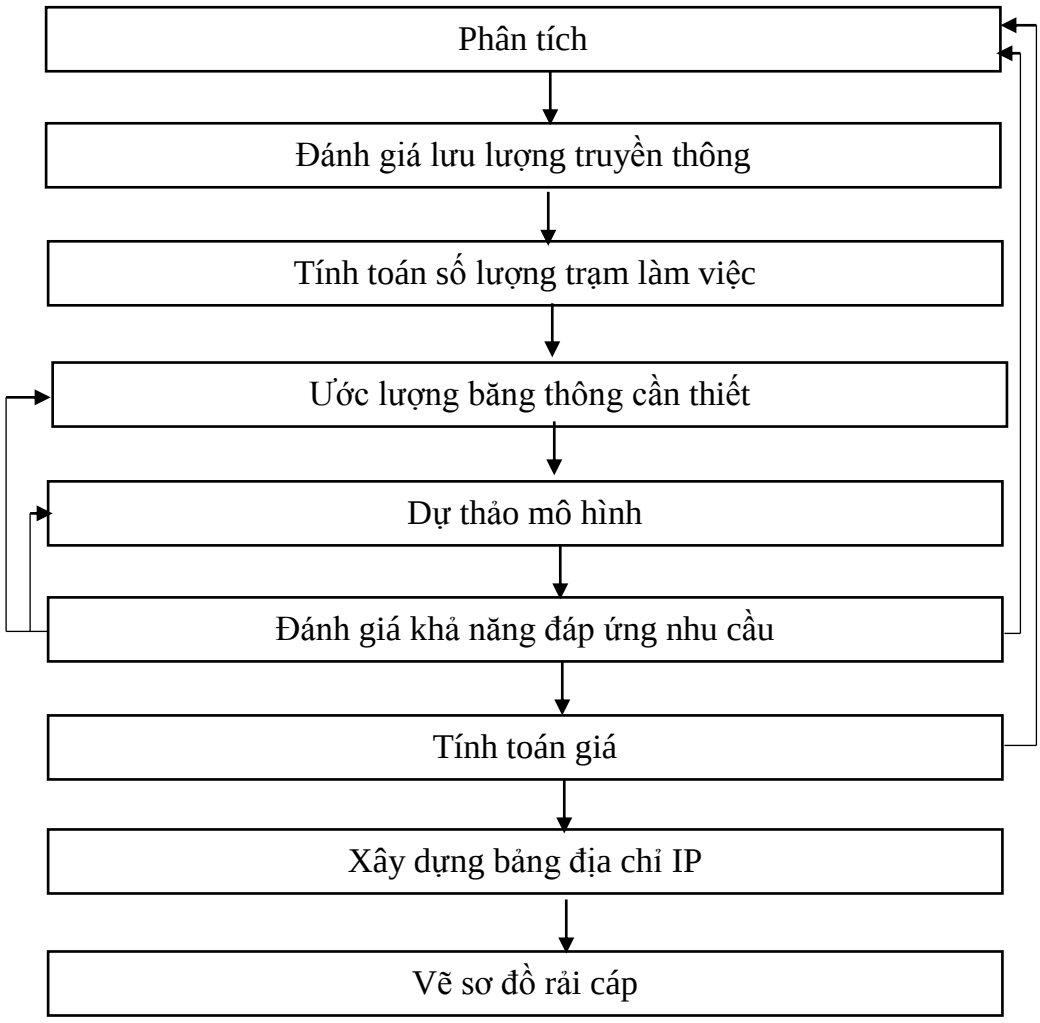
Chú ý rằng, các điều kiện sau phải được thỏa mãn:

- Số trạm làm việc $M \geq D.R.T/60$
- Số trạm làm việc $M \geq D.T/W$

Trong đó:

T là thời gian tính bằng phút để hoàn thành một giao dịch.

W là thời gian tính bằng phút của một ngày làm việc



Hình 3.24 Mô hình các bước thiết kế mạng

Bước 4: Ước lượng băng thông cần thiết

Việc ước lượng băng thông cần thiết cần căn cứ vào các thông tin sau:

- ✓ Hiệu quả truyền thông (H): được tính bằng tỷ số giữa kích thước dữ liệu (byte) trên tổng số byte của một khung dữ liệu.
- ✓ Tỷ lệ hữu ích đường truyền (R): được khuyến cáo cho hai cơ chế truy nhập truyền thông là CSMA/CD: 0.2; token ring: 0.4
- ✓ Băng thông đòi hỏi phải thỏa mãn điều kiện lớn hơn hoặc bằng dung lượng truyền thông tính theo byte/giờ, 8/(3600.H.R).

Bước 5: Dự thảo mô hình

Bước này là bước phải thực hiện các công việc:

- ✓ Khảo sát vị trí các trạm làm việc, vị trí đi các đường cáp mạng, ước tính độ dài, vị trí có thể đặt các repeater,…
- ✓ Lựa chọn kiểu LAN
- ✓ Lựa chọn thiết bị mạng lên danh sách thiết bị.

Bước 6: Đánh giả khả năng đáp ứng nhu cầu

Mục đích của bước này là đánh giá xem dự thảo thực hiện trong bước 5 có đáp ứng được nhu cầu của người sử dụng hay không?. Có thể quay lại bước 5 để thực hiện bổ sung, sửa đổi, thậm chí phải xây dựng lại bảng đồ dự thảo mới. Đôi khi cũng phải đối chiếu xem xét lại các chi tiết ở bước 1.

Có nhiều khía cạnh khác nhau cần đánh giá về khả năng thực hiện và đáp ứng nhu cầu của một mạng, nhưng điều kiện quan trọng trước tiên là thời gian trễ của mạng (delay time) cũng như thời gian hồi đáp của mạng (response time) vì thời gian trễ dài cũng có nghĩa là thời gian hồi đáp lớn.

Để tính toán được delay time có hai phương pháp:

- ✓ *Thực nghiệm:* xây dựng một mạng thí nghiệm có cấu hình tương tự như dự thảo. Đây là việc đòi hỏi nhiều công sức và tỷ mỉ.
- ✓ *Mô phỏng:* dùng các công cụ mô phỏng (simulation tool) để tính toán. Dùng phương pháp này buộc phải có simulation tool rất đắc tiền (hàng trăm ngàn USD).

Bước 7: Tính toán giá

Dựa trên danh sách thiết bị mạng có ở bước 5, ở bước này nhóm thiết kế phải thực hiện các công việc:

- ✓ Khảo sát thị trường, lựa chọn sản phẩm thích hợp. Đôi khi phải quay lại thực hiện các bổ sung các sửa đổi ở bước 5 hay đối chiếu lại các yêu cầu đã phân tích ở bước 1.
- ✓ Bổ sung danh sách các phụ kiện cần thiết cho việc thi công.
- ✓ Tính toán nhân công cần thiết để thực hiện thi công bao gồm cả nhân công quản lý điều hành.
- ✓ Lập bảng giá và tính toán tổng giá thành của tất cả các khoản mục.

Bước 8: Xây dựng bảng địa chỉ IP

Trong bước này phải lập:

- ✓ Bảng địa chỉ Network cho mỗi Subnet.
- ✓ Bảng địa chỉ IP cho từng trạm làm việc trong mỗi Subnet.

Bước 9: Vẽ sơ đồ rải cáp

- ✓ Sơ đồ rải cáp phải được thiết kế chi tiết để hướng dẫn thi công và tài liệu phải lưu trữ sau khi thi công.
- ✓ Cần xây dựng sơ đồ tỷ mỉ để đảm bảo tính thực thi, tránh tối đa các sửa đổi trong quá trình thi công.
- ✓ Trong quá trình thi công nếu có lý do bắt buộc phải sửa đổi đường đi cáp thì phải cập nhật lại bản vẽ để sau khi thi công xong, bản vẽ thể hiện chính xác sơ đồ đi cáp mạng.

TỔNG KẾT CHƯƠNG

Các điểm quan trọng bạn cần nắm được trong chương này:

1. Các đặc trưng về LAN.
2. Định nghĩa mạng cục bộ (LAN). Đặc điểm của mạng khách/chủ (Client/Server) và mạng ngang hàng (peer-to-peer).
3. Các chuẩn 10base2, 10base5, 10baseT và quy tắc mở rộng.
4. Các loại đường truyền.
5. Các bước thiết kế mạng.

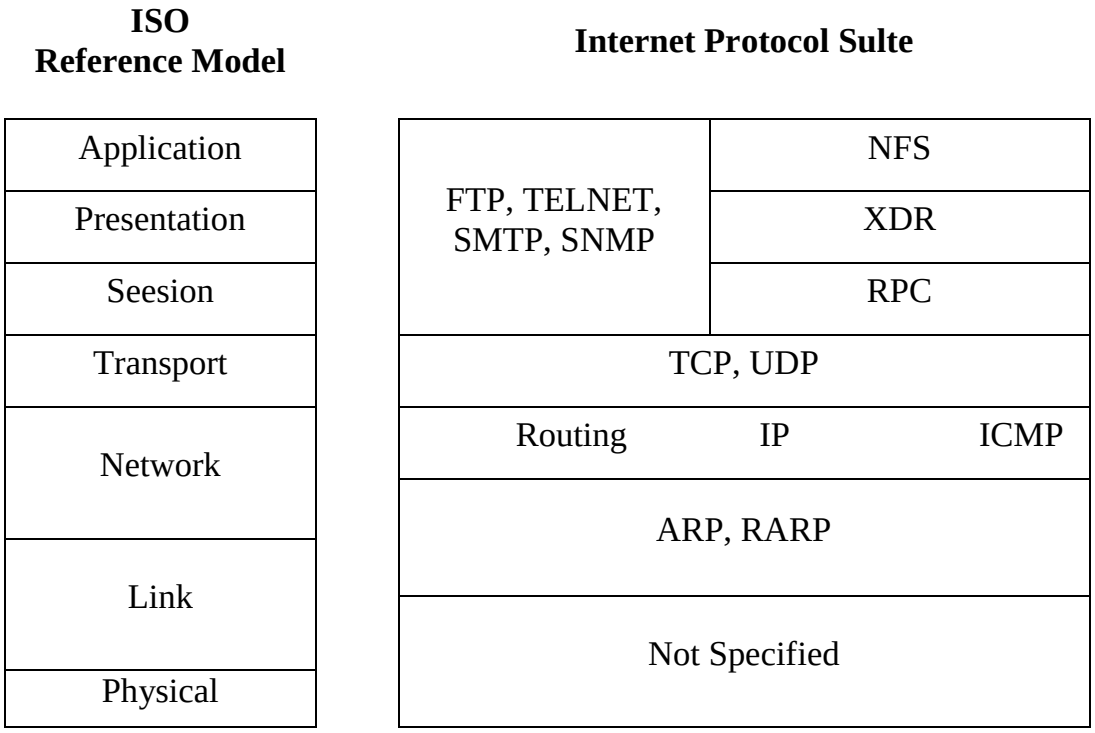
CHƯƠNG 4
GIAO THỨC TCP/IP

4.1 TỔNG QUAN VỀ BỘ GIAO THỨC TCP/IP

Các giao thức liên mạng là bộ giao thức cho các hệ thống mở nổi tiếng nhất trên thế giới bởi vì chúng có thể được sử dụng để giao tiếp qua bất kỳ các liên mạng nào cũng như thích hợp cho các giao tiếp trong mạng LAN và WAN. Các giao thức liên mạng bao gồm một bộ các giao thức truyền thông, trong đó nổi tiếng nhất là giao thức điều khiển truyền tải *(TCP – Transmission Control Protocol)* và giao thức liên mạng *(IP – Internet Protocol)* hoạt động ở tầng 4 và tầng 3 trong mô hình OSI. Ngoài hai giao thức này, bộ giao thức IP còn đặc tả nhiều giao thức cho tầng ứng dụng, ví dụ như giao thức cho dịch vụ thư điện tử, giao thức mô phỏng thiết bị đầu cuối và giao thức truyền tải tập tin.

Bộ giao thức liên mạng lần đầu tiên được phát triển vào giữa những năm của thập niên 70 khi văn phòng các dự án nghiên cứu chuyên sâu của bộ quốc phòng Mỹ *(DARPA-Defense Advanced Research Projects Agency)* quan tâm đến việc xây dựng một mạng chuyển mạch gói (packetswitched network) cho phép việc trao đổi thông tin giữa các hệ thống máy tính khác nhau của các viện nghiên cứu trở nên dễ dàng hơn. Với ý tưởng nối các hệ thống máy tính không đồng nhất lại với nhau, DARPA đã cấp kinh phí nghiên cứu cho đại học Stanford, Bolt, Beranek, and Newman (BBN) về vấn đề này. Kết quả của những nổ lực phát triển của dự án là bộ giao thức liên mạng đã được hoàn thành vào những năm cuối của thập niên 70.

Sau đó TCP/IP được tích hợp vào hệ điều hành UNIX phiên bản BSD *(Berkeley Software Distribution)* trở thành nền tảng cho mạng Internet và dịch vụ WWW *(World Wide Web)*.



Hình 4.1 Kiến trúc của mạng TCP/IP so với mô hình OSI

4.2 GIAO THỨC CƠ BẢN TRONG BỘ GIAO THỨC TCP/IP

4.2.1 Giao thức liên mạng IP (Internet Protocol)

Giao thức liên mạng, thường gọi là giao thức IP *(Internet Protocol)* là một giao thức mạng hoạt động ở tầng 3 của mô hình OSI, nó qui định cách thức định địa chỉ các máy tính và cách thức chuyển tải các gói tin qua một liên mạng. IP được đặc tả trong bảng báo cáo kỹ thuật có tên RFC *(Request For Comments)* mã số 791 và là giao thức chủ yếu trong bộ giao thức liên mạng. Cùng với giao thức TCP, IP trở thành trái tim của bộ giao thức Internet. IP có hai chức năng chính: cung cấp dịch vụ truyền tải dạng không nối kết để chuyển tải các gói tin qua một liên mạng và phân mãnh cũng như tập hợp lại các gói tin để hỗ trợ cho tầng liên kết dữ liệu với kích thước đơn vị truyền dữ liệu là khác nhau.

Định dạng gói tin IP (IP Packet Format)

Hình sau mô tả cấu trúc của một gói tin IP

32 bit

Version	IHL	Type of service	Total length	
Identification			Flags	Fragment offse
Time to live		Protocol	Header checksum	
Source Address				
Destination address				
Options (+ padding)				
Data (variable)				

Hình 4.2 Cấu trúc gói tin IP

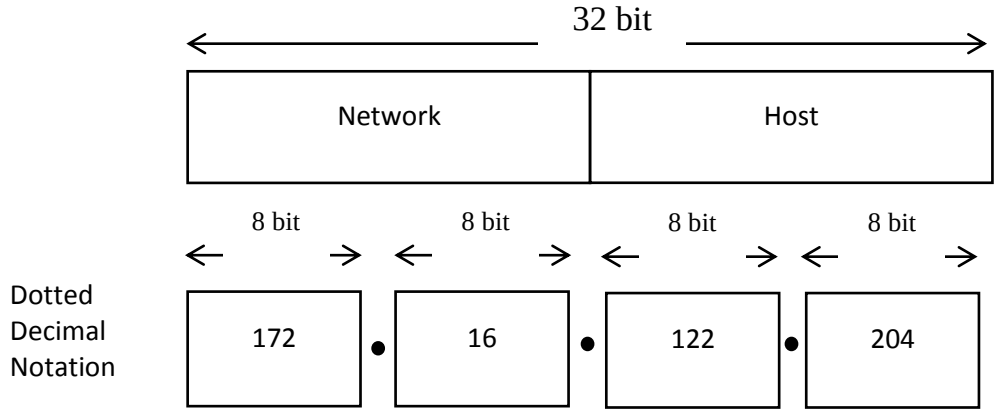
Ý nghĩa của các trường được mô tả như sau:

- *Version (Phiên bản):* Xác định phiên bản của giao thức đang được sử dụng.
- *IP Header Length (Chiều dài của phần tiêu đề)*: Xác định chiều dài phần tiêu đề của gói tin, tính bằng đơn vị là từ - 32 bits (32-bit word).
- *Type-of-Service (Kiểu của dịch vụ)*: Đặc tả mức độ quan trọng mà giao thức phía trên muốn xử lý gói tin.
- *Total Length (Tổng chiều dài gói tin)*: Đặc tả chiều dài, tính bằng byte, của cả gói tin IP, bao gồm cả phần dữ liệu và tiêu đề.
- *Identification (Số nhận dạng):* Số nguyên nhận dạng gói tin dữ liệu hiện hành. Trường này được sử dụng để ráp lại các phân đoạn của gói tin.
- *Flags (Cờ hiệu):* Gồm 3 bít, bit có trọng số nhỏ để xác định gói tin có bị phân đoạn hay không. Bit thứ 2 xác định có phải đây là phân đoạn cuối cùng của gói tin hay không. Bit có trọng số lớn nhất chưa sử dụng.

- *Fragment Offset (Vị trí của phân đoạn):* Biểu thị vị trí của phân đoạn dữ liệu so với vị trí bắt đầu của gói dữ liệu gốc, nó cho phép máy nhận xây dựng lại gói tin ban đầu.
- *Time-to-Live (Thời gian sống của gói tin):* Lưu giữ bộ đếm thời gian, giá trị sẽ được giảm dần đến khi nó có giá trị là 0 thì gói tin sẽ bị xóa. Điều này giúp ngăn ngừa tình trạng gói tin được truyền đi lòng vòng không bao giờ đến được đích.
- *Protocol(Giao thức):* Biểu hiện giao thức ở tầng trên sẽ nhận gói tin khi nó đã được giao thức IP xử lý.
- *Header Checksum (Tổng kiểm tra lỗi tiêu đề):* kiểm tra tính toàn vẹn của phần tiêu đề.
- Source Addres: Địa của máy gởi gói tin.
- *Destination Address:* Địa chỉ của máy nhận gói tin.
- *Options:* Tùy chọn cho phép để hỗ trợ một số vấn đề, chẳng hạn vấn đề bảo mật.
- *Data*

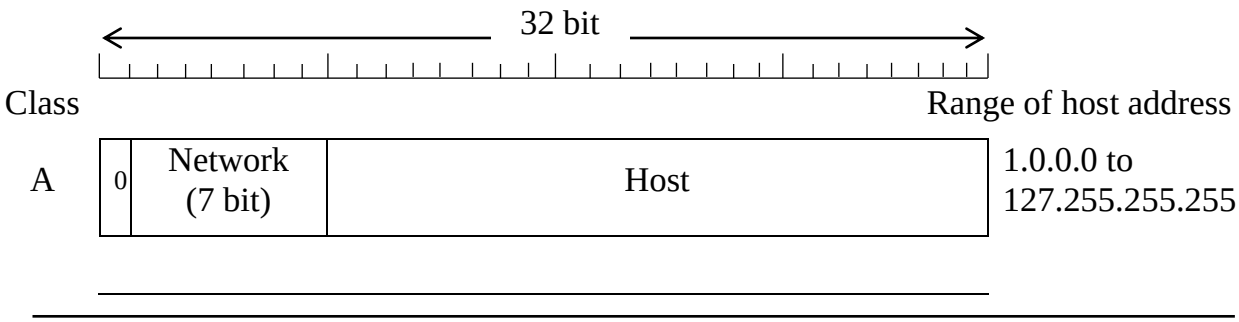
4.2.2 Cấu trúc địa chỉ IP

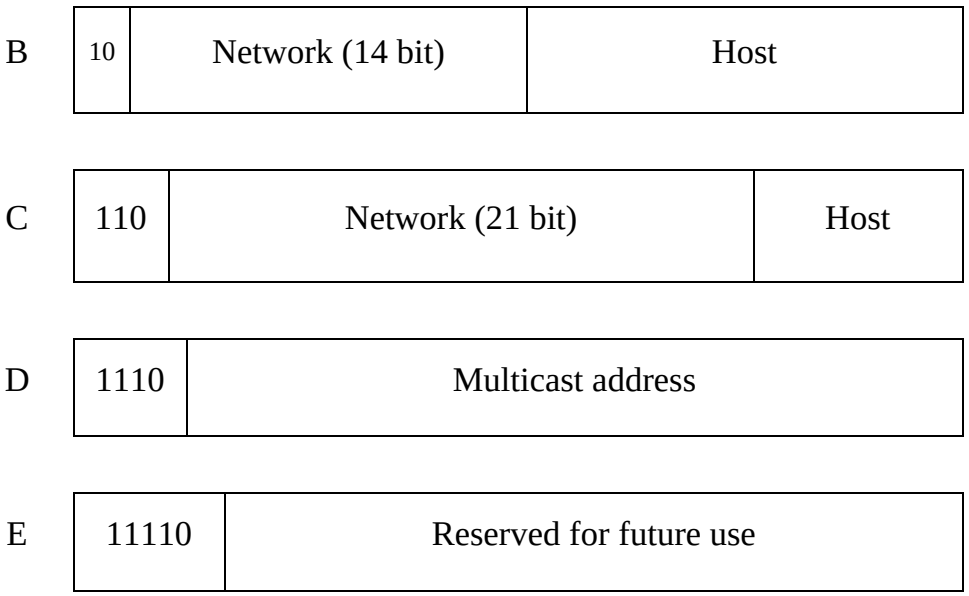
Mỗi máy tính trên mạng TCP/IP phải được gán một địa chỉ luận lý có chiều dài 32 bits, gọi là địa chỉ IP.



Hình 4.3 Cấu trúc địa chỉ IP

32 bits của địa chỉ IP được chia thành 2 phần: Phần nhận dạng mạng *(Network Id)* và phần nhận dạng máy tính *(Host Id).* Phần nhận dạng mạng được dùng để nhận dạng một mạng và phải được gán bởi trung tâm thông tin mạng Internet *(InterNIC - Internet Network Information Center)* nếu muốn nối kết vào mạng Internet. Phần nhận dạng máy tính dùng để nhận dạng một máy tính trong một mạng.





Hình 4.4 Phân lớp địa chỉ IP

Để dễ dàng cho việc đọc và hiểu bởi con người, 32 bits của địa chỉ IP được nhóm lại thành 4 bytes và được phân cách nhau bởi 3 dấu chấm (.). Giá trị của mỗi bytes được viết lại dưới dạng thập phân, với giá trị hợp lệ nằm trong khoảng từ 0 đến 255.

Câu hỏi được đặt ra là bao nhiêu bits dành cho phần nhận dạng mạng và bao nhiêu bits dành cho phần nhận dạng máy tính. Người ta phân các địa chỉ ra thành 5 lớp: A, B, C, D và E. Trong đó, chỉ có lớp A, B và C được dùng cho các mục đích thương mại. Các bits có trọng số cao nhất chỉ định lớp mạng của địa chỉ. Hình sau mô tả cách phân chia lớp cho các địa chỉ IP.

Thông tin chi tiết về các lớp được mô tả như bảng sau :

Lớp	**Dạng**	**Mục đích**	**Các bit cao nhất**	**Khoảng địa chỉ**	**Số bít phần nhận dạng mạng/Số bít phần nhận dạngmáy tính**	**Tổng số máy tínhtrong một mạng**
A	N.H.H.H	Cho một số ít các tổ chức lớn	0	1.0.0.0 đến 126.0.0.0	7/24	16.777. 214 (2^{24} - 2)
B	N.N.H.H	Cho các tổ chức có kích thước trung bình	10	128.1.0.0 đến 191.254.0.0	14/16	65. 543 (2^{16} - 2)
C	N.N.N.H	Cho các tổ chức có kích thước nhỏ	110	192.0.1.0 đến 223.255.254.0	21/8	254 (2^{8} - 2)
D		Truyền nhóm	1110	224.0.0.0 đến 239.255.255.255		
E		Dành cho thí nghiệm	11110	240.0.0.0 đến 254.255.255.255		

Ghi chú H: Host, N: Network

4.2.3 Một số địa chỉ IP đặc biệt

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

Ví dụ : 10.0.0.0; 172.18.0.0 ; 192.1.1.0

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

Ví dụ : 10.255.255.255, 172.18.255.255, 192.1.1.255

- Mặt nạ mạng chuẩn (Netmask): Là địa chỉ IP mà giá trị của các bits ở phần nhận dạng mạng đều là 1, các bits ở phần nhận dạng máy tính đều là 0. Như vậy ta có 3 mặt nạ mạng tương ứng cho 3 lớp mạng A, B và C là :
  - ✓ Mặt nạ mạng lớp A: 255.0.0.0
  - ✓ Mặt nạ mạng lớp B: 255.255.0.0
  - ✓ Mặt nạ mạng lớp C: 255.255.255.0

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

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

- Địa chỉ mạng 127.0.0.0 là địa chỉ được dành riêng để đặt trong phạm vi một máy tính. Nó chỉ có giá trị cục bộ (trong phạm vi một máy tính). Thông thường khi cài đặt giao thức IP thì máy tính sẽ được gián địa chỉ 127.0.0.1. Địa chỉ này thông thường để kiểm tra xem giao thức IP trên máy hiện tại có hoạt động không.
- Địa chỉ dành riêng cho mạng cục bộ không nối kết trực tiếp Internet: Các mạng cục bộ không nối kết trực tiếp vào mạng Internet có thể sử dụng các địa chỉ mạng sau để đánh địa chỉ cho các máy tính trong mạng của mình
  - ✓ Lớp A : 10.0.0.0
  - ✓ Lớp B : 172.16.0.0 đến 172.32.0.0
  - ✓ Lớp C : 192.168.0.0

4.2.4 Ý nghĩa của Netmask

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

Network Address = IP Address & Netmask

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

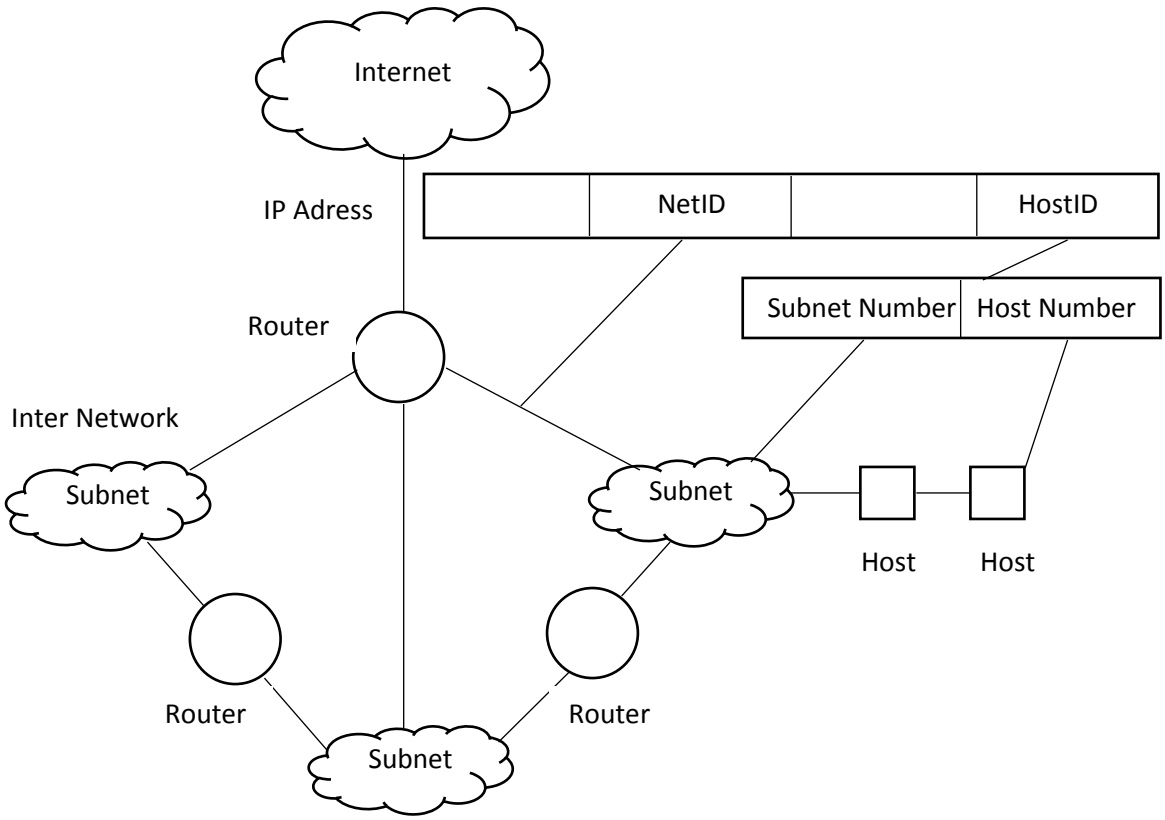
	Biểu diễn thập phân	**Biểu diễn nhị phân**
IP Address	198.53.147.45	11000110 00110101 10010011 00101101
Netmask	255.255.255.0	11111111 11111111 11111111 00000000
Network Address	198.53.147.0	11000110 00110101 10010011 00000000

4.2.5 Phân mạng con (Subnetting)

4.2.5.1Giới thiệu

Phân mạng con là một kỹ thuật cho phép nhà quản trị mạng chia một mạng thành những mạng con nhỏ, nhờ đó có được các tiện lợi sau:

- Đơn giản hóa việc quản trị: Với sự trợ giúp của các router, các mạng có thể được chia ra thành nhiều mạng con (subnet) mà chúng có thể được quản lý như những mạng độc lập và hiệu quả hơn.
- Có thể thay đổi cấu trúc bên trong của mạng mà không làm ảnh hưởng đến các mạng bên ngoài. Một tổ chức có thể tiếp tục sử dụng các địa chỉ IP đã được cấp mà không cần phải lấy thêm khối địa chỉ mới.
- Tăng cường tính bảo mật của hệ thống: Phân mạng con sẽ cho phép một tổ chức phân tách mạng bên trong của họ thành một liên mạng nhưng các mạng bên ngoài vẫn thấy đó là một mạng duy nhất.
- Cô lập các luồng giao thông trên mạng: Với sự trợ giúp của các router, giao thông trên mạng có thể được giữ ở mức thấp nhất có thể.



Hình 4.5 Địa chỉ mạng con đối với thế giới bên ngoài

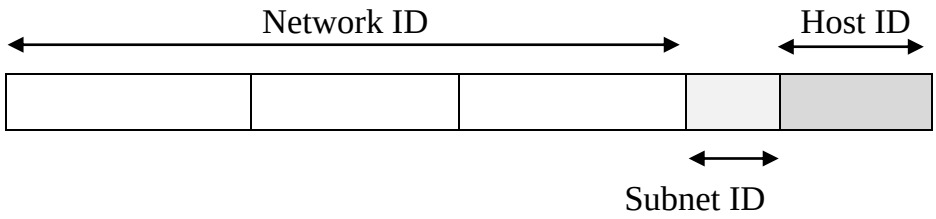
Hình trên mô tả một địa chỉ IP đã được phân mạng con xuất hiện với thế giới Internet bên ngoài và với mạng Intranet bên trong. Internet chỉ đọc phần nhận dạng mạng và các router trên Internet chỉ quan tâm tới việc vạch đường cho các gói tin đến được router giao tiếp giữa mạng Intranet bên trong và mạng Internet bên ngoài. Thông thường ta gọi router này là cửa khẩu của mạng (Gateway). Khi một gói tin IP từ mạng bên ngoài đến router cửa khẩu, nó sẽ đọc phần nhận dạng máy tính để xác định xem

gói tin này thuộc về mạng con nào và sẽ chuyển gói tin đến mạng con đó, nơi mà gói tin sẽ được phân phát đến máy tính nhận.

4.2.5.2Phương pháp phân mạng con

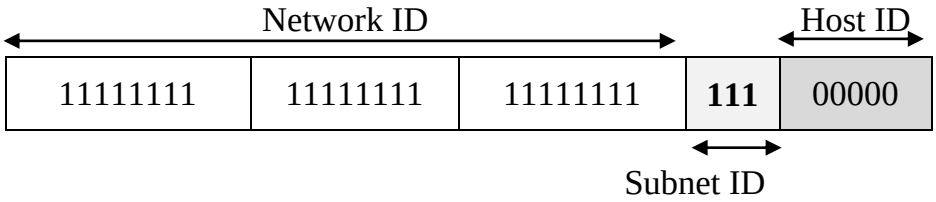
Nguyên tắc chung để thực hiện phân mạng con là :

- Phần nhận dạng mạng (Network ID) của địa chỉ mạng ban đầu được giữ nguyên.
- Phần nhận dạng máy tính của địa chỉ mạng ban đầu được chia thành 2 phần: Phần nhận dạng mạng con (Subnet ID) và phần nhận dạng máy tính trong mạng con (Host ID).



Hình 4.6 Cấu trúc địa chỉ IP khi phân mạng con

Để phân mạng con, người ta phải xác định mặt nạ mạng con (subnetmask). Mặt nạ mạng con là một địa chỉ IP mà giá trị các bit ở phần nhận dạng mạng (Network Id) và phần nhận dạng mạng con (Subnet Id) đều là 1 trong khi giá trị của các bits ở phần nhận dạng máy tính (Host Id) đều là 0. *Hình 4.7*mô tả mặt nạmạng con cho một mạng ở lớp C.



Hình 4.7 Mặt nạ mạng con khi phân mạng con

Khi có được mặt nạ mạng con, ta có thể xác định địa chỉ mạng con (Subnetwork Address) mà một địa chỉ IP được tính bằng công thức sau :

Subnetwork Address = IP & Subnetmask

Có hai chuẩn để thực hiện phân mạng con là :

- ✓ Chuẩn phân lớp hoàn toàn *(Classfull standard)*
- ✓ Chuẩn vạch đường liên miền không phân lớp CIDR (*Classless Inter-Domain Routing)*. Thực tế, CIDR chỉ mới được đa số các nhà sản xuất thiết bị và hệ điều hành mạng hỗ trợ nhưng vẫn chưa hoàn toàn chuẩn hóa.

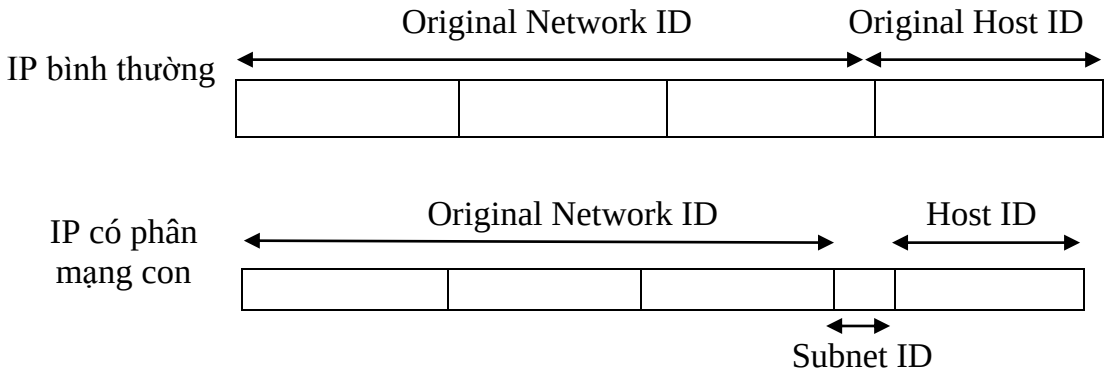
a) Phương pháp phân lớp hoàn toàn (Classfull Standard)

Chuẩn này qui định địa chỉ IP khi phân mạng con sẽ gồm 3 phần :

- Phần nhận dạng mạng của địa chỉ ban đầu (Network Id)

- Phần nhận dạng mạng con (Subnet Id): Được hình thành từ một số bits có trọng số cao trong phần nhận dạng máy tính (Host Id) của địa chỉ ban đầu
- Và cuối cùng là phần nhận dạng máy tính trong mạng con (Host Id) bao gồm các bit còn lại.

Ví dụ: Hình sau mô tả cấu trúc địa chỉ IP lớp C khi thực hiện phân mạng con



Hình 4.8 Địa chỉ IP phân mạng con theo chuẩn Phân lớp hoàn toàn

Số lượng bits thuộc phần nhận dạng mạng con xác định số lượng mạng con. Giả sử phần nhận dạng mạng con chiếm 4 bits. Như vậy, về mặt lý thuyết ta có thể phân ra thành 24 = 16 mạng con. Tuy nhiên phần nhận dạng mạng con gồm toàn bit 0 hoặc bit 1 không được dùng để đánh địa chỉ cho mạng con vì nó trùng với địa chỉ mạng và địa chỉ quảng bá của mạng ban đầu.

Ví dụ: Cho địa chỉ mạng lớp C: 192.168.1.0 với mặt nạ mạng mặc định là 255.255.255.0.

Xét trường hợp phân mạng con cho mạng trên sử dụng 2 bit để làm phần nhận dạng mạng con.

Mặt nạ mạng trong trường hợp này là 255.255.255.192. Khi đó ta có các địa chỉ mạng con như sau :

Địa chỉ IP	**Biểu diễn dạng thập phân**	**Biểu diễn dạng nhị phân**			
Mạng ban đầu	192.168.1.0	1100 0000	1010 1000	0000 0001	0000 0000
Mạng con 1	192.168.1.0	1100 0000	1010 1000	0000 0001	0000 0000
Mạng con 2	192.168.1.64	1100 0000	1010 1000	0010 0001	**01**00 0000
Mạng con 3	192.168.1.128	1100 0000	1010 1000	0000 0001	**10**00 0000
Mạng con 4	192.168.1.192	1100 0000	1010 1000	0000 0001	**11**00 0000

Ta nhận thấy rằng:

- Địa chỉ mạng con thứ nhất 192.168.1.0 trùng với địa chỉ mạng ban đầu.
- Địa chỉ mạng con thứ tư 192.168.1.192 có địa chỉ quảng bá trùng với địa chỉ quảng bá của mạng ban đầu.

Chính vì thế mà hai địa chỉ này (có phần nhận dạng mạng con toàn bit 0 hoặc toàn bit 1) không được dùng để đánh địa chỉ cho mạng con.

Nói tóm lại, với **n** bits làm phần nhận dạng mạng con ta chỉ có thể phân ra được 2n-2 mạng con mà thôi. Mỗi mạng con cũng có địa chỉ quảng bá. Đó là địa chỉ mà các bits ở phần nhận dạng máy tính đều có giá trị là 1.

Ví dụ :

Địa chỉ IP	**Biểu diễn thập phân**	**Biểu diễn dạng nhị phân**			
Mạng con 1	192.168.1.64	1100 0000	1010 1000	0010 0001	**01**00 0000
Địa chỉ quảng bá	192.168.1.127	1100 0000	1010 1000	0010 0001	**01**11 1111
Mạng con 2	192.168.1.128	1100 0000	1010 1000	0000 0001	**10**00 0000
Địa chỉ quảng bá	192.168.1.191	1100 0000	1010 1000	0000 0001	**10**11 1111

Như vậy qui trình phân mạng con có thể được tóm tắt như sau :

- Xác định số lượng mạng con cần phân, giả sử là **N**.
- Biểu diễn (N+1) thành số nhị phân,số lượng bit cần thiết để biểu diễn (N+1) chính là số lượng bits cần dành cho phần nhận dạng mạng con. Ví dụ N=6, khi đó biểu diễn của (6+1) dưới dạng nhị phân là 111. Như vậy cần dùng 3 bits để làm phần nhận dạng mạng con
- Tạo mặt nạ mạng con
- Liệt kê tất cả các địa chỉ mạng con có thể, trừ hai địa chỉ mà ở đó phần nhận dạng mạng con toàn các bits 0 và các bit 1.
- Chọn ra N địa chỉ mạng con từ danh sách các mạng con đã liệt kê.

b) Phương pháp vạch đường liên miền không phân lớp CIDR (Classless Inter-Domain Routing)

CIDR là một sơ đồ đánh địa chỉ mới cho mạng Internet hiệu quả hơn nhiều so với sơ đồ đánh địa chỉ cũ theo kiểu phân lớp A, B và C.

CIDR ra đời để giải quyết hai vấn đề bức xúc đối với mạng Internet là :

- Thiếu địa chỉ IP
- Vượt quá khả năng chứa đựng của các bảng chọn đường.

4.2.5.3Vấn đề thiếu địa chỉ IP

Với sơ đồ đánh địa chỉ truyền thống, các địa chỉ được phân ra thành các lớp A, B và C. Mỗi địa chỉ có 2 phần, phần nhận dạng mạng và phần nhận dạng máy tính. Khi đó số lượng mạng và số máy tính tối đa cho từng mạng được thống kê như bảng sau :

Lớp mạng	**Số lượng mạng**	**Số máy tính tối đa trong mạng**
A	126	16.777.214

B	65.000	65.534
C	Hơn 2 triệu	254

Bởi vì các địa chỉ của mạng Internet thường được gán theo kích thước này dẫn đến tình trạng lãng phí. Trường hợp bạn cần 100 địa chỉ, bạn sẽ được cấp một địa chỉ lớp C. Như vậy còn 154 địa chỉ không được sử dụng. Chính điều này dẫn đến trình trạng thiếu địa chỉ IP cho mạng Internet. Theo thống kê, chỉ có khoảng 3% số địa chỉ đã được cấp phát được sử dụng đến. Chính vì thế sơ đồ đánh địa chỉ mới CIDR ra đời để khắc phục tình trạng trên.

4.2.5.4Vấn đề vượt quá khả năng chứa đựng của các bảng chọn đường

Khi số lượng mạng trên mạng Internet tăng cũng đồng nghĩa với việc tăng số lượng router trên mạng. Trong những năm gần đây, người ta dự đoán rằng các router đường trục của mạng Internet đang nhanh chóng tiến đến mức ngưỡng tối đa số lượng router mà nó có thể chấp nhận được. Thậm chí với những công nghệ hiện đại dùng để sản xuất các router thì về mặt lý thuyết kích thước tối đa của một bảng chọn đường cũng chỉ đến 60.000 mục từ (đường đi). Nếu không có những cải tiến thì các router đường trục sẽ đạt đến con số này và như thế không thể mở rộng mạng Internet hơn nữa. Để giải quyết hai vấn đề trên, cộng đồng Internet đã đưa ra các giải pháp sau :

- Sửa đổi lại cấu trúc cấp phát địa chỉ IP để tăng hiệu quả.
- Kết hợp việc chọn đường có cấu trúc để giảm tối đa số lượng các mục từ trong bảng chọn đường.

4.2.5.5Sửa đổi lại cấu trúc cấp phát địa chỉ IP

CIDR được sử dụng để thay thế cho sơ đồ cấp phát cũ với việc qui định các lớp A, B, C. Thay vì phần nhận dạng mạng được giới hạn với 8, 16 hoặc 24 bits, CIDR sử dụng phần nhận dạng mạng có tính tổng quát từ 13 đến 27 bits. Chính vì thế các khối địa chỉ có thể được gán cho mạng nhỏ nhất với 32 máy tính đến mạng lớn nhất hơn 500.000 máy tính. Điều này đáp ứng gần đúng yêu cầu đánh địa chỉ của các tổ chức khác nhau.

4.2.5.6Địa chỉ CIDR

Một địa chỉ theo cấu trúc CIDR, gọi tắt tắt địa chỉ CIDR, bao gồm 32 bits của địa chỉ IP chuẩn cùng với một thông tin bổ sung về số lượng các bit được sử dụng cho phần nhận dạng mạng.

Ví dụ: Với địa chỉ CIDR 206.13.01.48/25 thì chuỗi số "/25" chỉ ra rằng 25 bits đầu tiên trong địa chỉ IP được dùng để nhận dạng duy nhất một mạng, số bits còn lại dùng để nhận dạng một máy tính trong mạng.

Bảng sau so sánh giữa sơ đồ đánh địa chỉ theo kiểu CIDR và sơ đồ đánh địa chỉ theo chuẩn phân lớp hoàn toàn

Số bits nhận dạng mạng trong địa chỉ CIDR	Lớp tương ứng trong chuẩn phân lớp hoàn toàn	Số lượng máy tính trong mạng
/27	1/8 lớp C	32
/26	¼ lớp C	64
/25	½ lớp C	128

/24	1 lớp C	256
/23	2 lớp C	512
/22	4 lớp C	1.024
/21	8 lớp C	2.048
/20	16 lớp C	4.096
/19	32 lớp C	8.192
/18	64 lớp C	16.384
/17	128 lớp C	32.768
/16	256 lớp C (= 1 lớp B)	65.536
/15	512 lớp C	131.072
/14	1,024 lớp C	262.144
/13	2,048 lớp C	524.288

Kết hợp việc chọn đường có cấu trúc để giảm tối đa số lượng các mục từ trong bảng chọn đường.

Sơ đồ đánh địa chỉ theo theo CIDR cũng cho phép kết hợp các đường đi, ở đó mục từ trong bảng chọn đường ở mức cao có thể đại diện cho nhiều router ở mức thấp hơn trong các bảng chọn đường tổng thể.

Sơ đồ này giống như hệ thống mạng điện thoại ở đó mạng được thiết lập theo kiến trúc phân cấp. Một router ở mức cao (quốc gia), chỉ quan tâm đến mã quốc gia trong số điện thoại, sau đó nó sẽ vạch đường cho cuộc gọi đến router đường trục phụ trách mạng quốc gia tương ứng với mã quốc gia đó. Router nhận được cuộc gọi nhìn vào phần đầu của số điện thoại, mã tỉnh, để vạch đường cho cuộc gọi đến một mạng con tương ứng với mã tỉnh đó, và cứ như thế. Trong sơ đồ này, các router đường trục chỉ lưu giữ thông tin về mã quốc gia cho mỗi mục từ trong bảng chọn đường của mình, mỗi mục từ như thế đại diện cho một số khổng lồ các số điện thoại riêng lẽ chứ không phải là một số điện thoại cụ thể.

Thông thường, các khối địa chỉ lớn được cấp cho các nhà cung cấp dịch vụ Internet (Internet Service Providers) lớn, sau đó họ lại cấp lại các phần trong khối địa chỉ của họ cho các khách hàng của mình.

Hiện tại, mạng Internet sử dụng cả hai sơ đồ cấp phát địa chỉ Classfull standard và CIDR. Hầu hết các router mới đều hỗ trợ CIDR và những nhà quản lý Internet thì khuyến khích người dùng cài đặt sơ đồ đánh địa chỉ CIDR

Tham khảo thêm về CIDR ở địa chỉ http://www.rfc-editor.org/rfcsearch.html với các RFC liên quan sau:

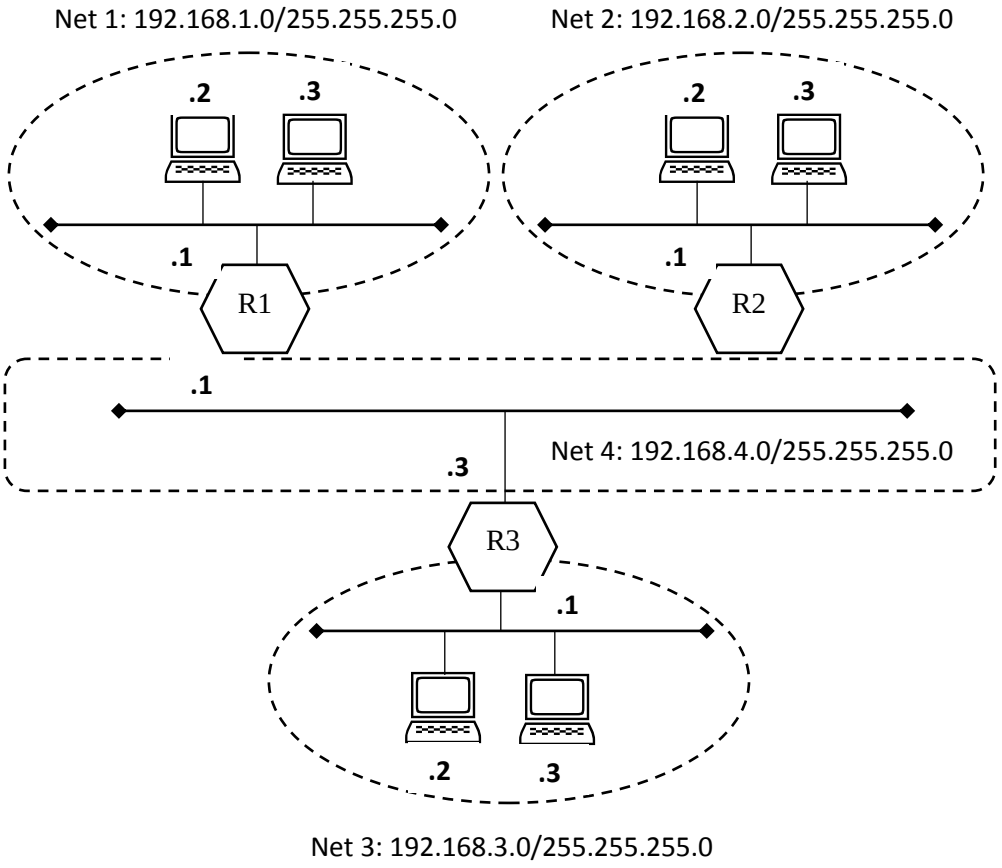
- RFC 1517: *Applicability Statement for the Implementation of CIDR*
- RFC 1518: *An Architecture for IP Address Allocation with CIDR*
- RFC 1519: *CIDR: An Address Assignment and Aggregation Strategy*
- RFC 1520: *Exchanging Routing Information Across Provider Boundaries in the CIDR Environment*

4.2.6 Vạch đường trong giao thức IP

Cho ba mạng Net1, Net2 và Net3 nối lại với nhau nhờ 3 router R1, R2 và R3. Mạng Net4 nối các router lại với nhau. Công việc đầu tiên trong thiết kế mạng liên mạng IP là chọn địa chỉ mạng cho các nhánh mạng. Trong trường hợp này chọn mạng lớp C cho 4 mạng như sau:

Mạng	Địa chỉ mạng	Mặt nạ mạng
Net 1	192.168.1.0	255.255.255.0
Net 2	192.168.2.0	255.255.255.0
Net 3	192.168.3.0	255.255.255.0
Net 4	192.168.4.0	255.255.255.0

Kế tiếp, gán địa chỉ cho từng máy tính trong mạng. Ví dụ trong mạng Net1, các máy tính được gán địa chỉ là 192.168.1.2 (Ký hiệu **.2** là cách viết tắt của địa chỉ IP để mô tả phần nhận dạng máy tính) và 192.168.1.3. Mỗi router có hai giao diện tham gia vào hai mạng khác nhau. Ví dụ, giao diện tham gia vào mạng NET1 của router R1 có địa chỉ là 192.168.1.1 và giao diện tham gia vào mạng NET4 có địa chỉ là 192.168.4.1.



Hình 4.9 ví dụ vềmột liên mạng sử dụng giao thức IP

Để máy tính của các mạng có thể giao tiếp được với nhau, cần phải có thông tin về đường đi. Bảng chọn đường của router có thể tạo ra thủ công hoặc tự động. Đối với mạng nhỏ, nhà quản trị mạng sẽ nạp đường đi cho các router thông qua các lệnh được cung cấp bởi hệ điều hành của router. Bảng chọn đường trong giao thức IP có 4 thông tin quan trọng là :

- Địa chỉ mạng đích
- Mặt nạ mạng đích
- Router kế tiếp sẽ nhận gói tin *(Next Hop)*
- Giao diện chuyển gói tin đi

Trong ví dụ trên, các router sẽ có bảng chọn đường như sau :

R1-Routing table		
Network/Netmask	**NextHop**	**Interface**
192.168.1.0/255.255.255.0	Local	Local
192.168.2.0/255.255.255.0	192.168.4.2	192.168.4.1
192.168.3.0/255.255.255.0	192.168.4.3	192.168.4.1
192.168.4.0/255.255.255.0	Local	Local

R2-Routing table		
Network/Netmask	**NextHop**	**Interface**
192.168.1.0/255.255.255.0	192.168.4.1	192.168.4.2
192.168.2.0/255.255.255.0	Local	Local
192.168.3.0/255.255.255.0	192.168.4.3	192.168.4.2
192.168.4.0/255.255.255.0	Local	Local

R3-Routing table		
Network/Netmask	**NextHop**	**Interface**
192.168.1.0/255.255.255.0	192.168.4.1	192.168.4.3
192.168.2.0/255.255.255.0	192.168.4.2	192.168.4.2
192.168.3.0/255.255.255.0	Local	Local
192.168.4.0/255.255.255.0	Local	Local

Các máy tính cũng có bảng chọn đường. Dưới đây là bảng chọn đường của máy tính có địa chỉ 192.168.3.3

192.168.3.3 – Routing table		
Network/Netmask	**NextHop**	**Interface**
192.168.3.0/255.255.255.0	Local	Local

default	192.168.3.1	Local

Mạng đích default ý nói rằng ngoài những đường đi đến các mạng đã liệt kê phía trên, các đường đi còn lại thì gửi cho NextHop của mạng default này. Như vậy, để gửi gói tin cho bất kỳ một máy tính nào nằm bên ngoài mạng 192.168.3.0 thì máy tính 192.168.3.3 sẽ chuyển gói tin cho router 3 ở địa chỉ 192.168.3.1.

4.2.6.1 Đường đi của gói tin

Để hiểu rõ có chế hoạt động của giao thức IP, ta hãy xét hai trường hợp gửi gói tin: Trường hợp máy tính gửi và nhận nằm trong cùng một mạng và trường hợp máy tính gửi và máy tính nhận nằm trên hai mạng khác nhau.

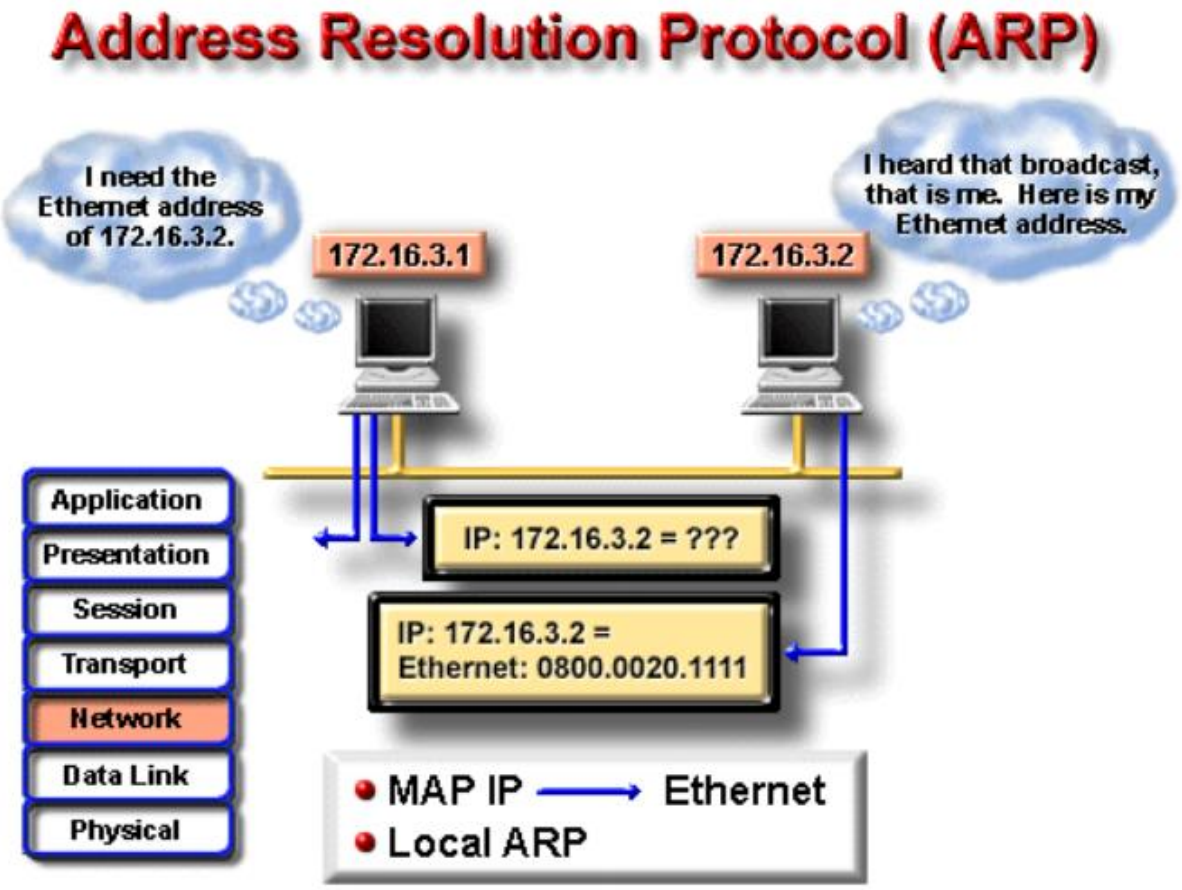
Giả sử máy tính có địa chỉ 192.168.3.3 gởi một gói tin cho máy tính 192.168.3.2. Tầng hai của máy gửi sẽ đặt gói tin vào một khung với địa chỉ nhận là địa chỉ vật lý của máy nhận và gửi khung lên đường truyền NET3, trên đó máy tính nhận sẽ nhận được gói tin. Bây giờ ta xét trường hợp máy tính có địa chỉ 192.168.3.3 trên mạng NET3 gởi gói tin cho máy tính có địa chỉ 192.168.1.2 trên mạng NET1. Theo như bảng chọn đường của máy gửi, các gói tin có địa chỉ nằm ngoài mạng 192.168.3.0 sẽ được chuyển đến router R3 (địa chỉ 192.168.3.1).

Chính vì thế, máy tính gửi sẽ đặt gói tin vào một khung với địa chỉ nhận là địa chỉ vật lý của giao diện 192.168.3.1 và đưa lên đường truyền NET3. Nhận được gói tin, R3 phân tích địa chỉ IP của máy nhận để xác định đích đến của gói tin Bảng chọn đường cho thấy, với đích đến là mạng 192.168.1.0 thì cần phải chuyển gói tin cho router R1 ở địa chỉ 192.168.4.1 thông qua giao diện 192.168.4.3. Vì thế R3 đặt gói tin vào một khung với địa chỉ nhận là địa chỉ vật lý của giao diện 192.168.4.1 của router R1 và đưa lên đường truyền NET4. Tương tự, R1 sẽ chuyển gói tin cho máy nhận 192.168.1.2 bằng một khung trên đường truyền NET1.

Ta nhận thấy rằng, để đi đến được máy nhận, gói tin được chuyển đi bởi nhiều khung khác nhau. Mỗi khung sẽ có địa chỉ nhận khác nhau, tuy nhiên địa chỉ của gói tin thì luôn luôn không đổi.

4.2.6.2Giao thức phân giải địa chỉ ARP(Address Resolution Protocol)

Nếu một máy tính muốn truyền một gói tin IP nó cần đặt gói tin này vào trong một khung trênđường truyền vật lý mà nó đang nối kết vào. Để có thể truyền thành công khung, máy tính gửi cần thiết phải biết được địa chỉ vật lý (MAC) của máy tính nhận. Điều này có thể thực hiện được bằng cách sử dụng một bảng để ánh xạ các địa chỉ IP về địa chỉ vật lý. Giao thức IP sử dụng giao thức ARP (Address Resolution Protocol) để thực hiện ánh xạ từ một địa chỉ IP về một địa chỉ MAC.



Hình 4.10 Giao thức ARP

Một máy tính xác định địa chỉ vật lý của nó vào lúc khởi động bằng cách đọc thiết bị phần cứng và xác định địa chỉ IP của nó bằng cách đọc tập tin cấu hình, sau đó lưu thông tin về mối tương ứng giữa địa chị IP và MAC của nó vào trong vùng nhớ tạm (ARP cache). Khi nhận được một địa chỉ IP mà ARP không thể tìm ra được địa chỉ vật lý tương ứng dựa vào vùng nhớ tạm hiện tại, nó sẽ thực hiện một khung quảng bá có định dạng như sau:

Tổng quát	Các trường	Kích thức (byte)	Các giá trị
Ethernet Header	Ethernet Destination Address	6	Địa chỉ máy nhận, trong trường hợp này là một địa chỉ quảng bá
	Ethernet Source Address	6	Địa chỉ của máy gởi thông điệp
	Frame Type	2	Kiểu khung, có giá trị là 0x0806 khi ARP yêu cầu và 0x8035 khi ARP trả lời
ARP request/reply	Hardware Type	2	Giá trị là 1 cho mạng Ethernet
	Protocol Type	2	Có giá trị là 0x0800 cho địa chỉ IP
	Hardware Address Size in bytes	1	Chiều dài của địa chỉ vật lý, có giá trị là 6 cho mạng Ethernet

	Protocol Address Size in bytes	1	Chiều dài của địa chỉ giao thức, có giá trị là 4 cho giao thức IP
	Operation	2	Là 1 nếu là khung yêu cầu, là 2 nếu là khung trả lời
	Sender Ethernet Address	6	-
	Sender IP Address	4	-
	Destination Ethernet Address	6	Không sử dụng đến trong yêu cầu của ARP
	Destination IP Address	4	-

Nhờ vào việc gửi các yêu cầu này, một máy tính có thể bổ sung thông tin cho vùng cache của giao thức ARP, nhờ đó cập nhật kịp thời mọi sự thay đổi của sơ đồ mạng. Thông thường thời gian quá hạn (Time-out) cho một thông tin trong vùng cache là 20 phút. Một yêu cầu ARP cho một máy tính không tồn tại trên nhánh mạng được lặp lại một vài lần xác định nào đó.

Nếu một máy tính được nối kết vào nhiều hơn một mạng bằng giao diện mạng, khi đó sẽ tồn tại những vùng cache ARP riêng cho từng giao diện mạng.

Lưu ý: ARP trên một máy tính chỉ thực hiện việc xác định địa chỉ vật lý cho các địa chỉ cùng địa chỉ mạng/mạng con với nó mà thôi. Đối với các gói tin gởi cho các máy tính có địa chỉ IP không cùng một mạng/mạng con với máy gửi sẽ được chuyển hướng cho một router nằm cùng mạng với máy gửi để chuyển đi tiếp.

Vì các yêu cầu ARP được quảng bá rộng rãi, cho nên bất kỳ một máy tính nào đang duy trì một vùng cache đều có thể theo dõi tất cả các yều cầu được quảng bá này để lấy thông tin về địa chỉ vật lý và địa chỉ IP của máy gửi yêu cầu và bổ sung vào vùng cache của nó khi cần thiết. Khi một máy tính khởi động, nó gửi một yêu cầu ARP (có thể cho chính nó) như để thông báo với các máy tính khác về sự xuất hiện của nó trong mạng cục bộ.

Có thể gán nhiều hơn một địa chỉ IP cho một địa chỉ vật lý. Chú ý rằng, định dạng của yêu cầu ARP thì được thiết kế để có thể hỗ trợ được cho các giao thức khác ngoài IP và Ethernet.

4.2.6.3Giao thức phân giải địa chỉ ngược RARP

(Reverse Address Resolution Protocol)

Ngày nay, các trạm làm việc không đĩa cứng *(Diskless workstation)* được sử dụng rộng rãi. Mỗi máy tính chỉ cần bộ xử lý và bộ nhớ, tất cả không gian lưu trữ được cung cấp từ một máy chủ *(Server)* sử dụng một hệ thống tập tin mạng theo một chuẩn nào đó. Do không có các tập tin cấu hình, tiến trình khởi động của các máy tính này thường sử dụng một giao thức truyền tải tập tin rất đơn giản như TFTP. Tuy nhiên, trước khi có thể nối kết đến được server, các trạm làm việc cần phải biết được địa chỉ IP của nó. Giao thức RARP được dùng trong trường hợp này. RARP sử dụng cùng định dạng yêu cầu của ARP nhưng trường Operation có giá trị là 3 cho yêu cầu và 4

cho trả lời. Trên server duy trì một bảng mô tả mối tương quan giữa địa chỉ vật lý và địa chỉ IP của các máy trạm. Khi nhận được yêu cầu RARP, server tìm trong bảng địa chỉ và trả về địa chỉ IP tương ứng cho máy trạm đã gửi yêu cầu.

4.2.6.4Giao thức thông điệp điều khiển Internet ICMP (Internet Control Message Protocol)

Giao thức ICMP được cài đặt trong hầu hết tất cả các máy tính TCP/IP. Các thông điệp của giao thức được gởi đi trong các gói tin IP và được dùng để gửi đi các báo lỗi hay các thông tin điều khiển.

ICMP tạo ra nhiều loại thông điệp hữu ích như :

- Đích đến không tới được (Destination Unreachable)
- Thăm hỏi và trả lời (Echo Request and Reply)
- Chuyển hướng (Redirect)
- Vượt quá thời gian (Time Exceeded)
- Quảng bá bộ chọn đường (Router Advertisement)
- Cô lập bộ chọn đường (Router Solicitation)

Nếu một thông điệp không thể phân phát được thì nó sẽ không được gởi lại. Điều này để tránh tình trạng di chuyển không bao giờ dừng của các thông điệp ICMP.

Nếu một thông điệp *«Đích đến không tới được»* được gởi đi bởi một router, điều đó có nghĩa rằng router không thể gởi gói tin đến đích được. Khi đó router sẽ xóa gói tin ra khỏi hàng đợi của nó. Có hai nguyên nhân làm cho một gói tin không thể đi đến nơi được. Phần lớn là máy gởi mô tả một địa chỉ nhận mà nó không tồn tại trên thực tế. Trường hợp ít hơn là router không biết đường đi đến nơi nhận gói tin.

Thông điệp đích đến không tới được được chia thành bốn loại cơ bản là :

- Mạng không đến được *(Network unreachable)*: Có nghĩa là có sự cố trong vấn đề vạch đường hoặc địa chỉ nhận của gói tin.
- Máy tính không đến được *(Host unreachable):* Thông thường dùng để chỉ trục trặc trong vấn đề phân phát, như là sai mặt nạ mạng con chẳng hạn.
- Giao thức không đến được *(Protocol unreachable):* Máy nhận không hỗ trợ giao thức ở tầng cao hơn như gói tin đã mô tả.
- Cổng không đến được *(Port unreachable):* Socket của giao thức TCP hay cổng không tồn tại.

Một thông điệp *«Thăm hỏi và trả lời»* được tạo ra bởi lệnh ping từ một máy tính để kiểm tra tính liên thông trên liên mạng. Nếu có một thông điệp trả lời, điều đó biểu hiện rằng giữa máy gửi và máy nhận có thể giao tiếp được với nhau.

Một thông điệp *«Chuyển hướng»* được gửi bởi một router đến máy đã gửi gói tin để khuyến cáo về một đường đi tốt hơn. Router hiện tại vẫn chuyển tiếp gói tin mà nó nhận được. Thông điệp chuyển hướng giữ cho bảng chọn đường của các máy tính được nhỏ bởi vì chúng chỉ cần chứa địa chỉ của một router mà thôi, thậm chí router đó cung cấp đường đi không phải là tốt nhất. Đôi khi sau khi nhận được thông điệp chuyển hướng, thiết bị gởi vẫn sử dụng đường đi cũ. Một thông điệp *«Vượt quá thời hạn»* được gửi bởi một router nếu thời gian sống *(Time-to-live)* của gói tin, tính bằng

số router hay giây, có giá trị là 0. Thời gian sống của gói tin giúp phòng ngừa trường hợp gói tin được gởi đi lòng vòng trên mạng và không bao giờ đến nơi nhận. Router sẽ bỏ đi các gói tin đã hết thời gian sống.

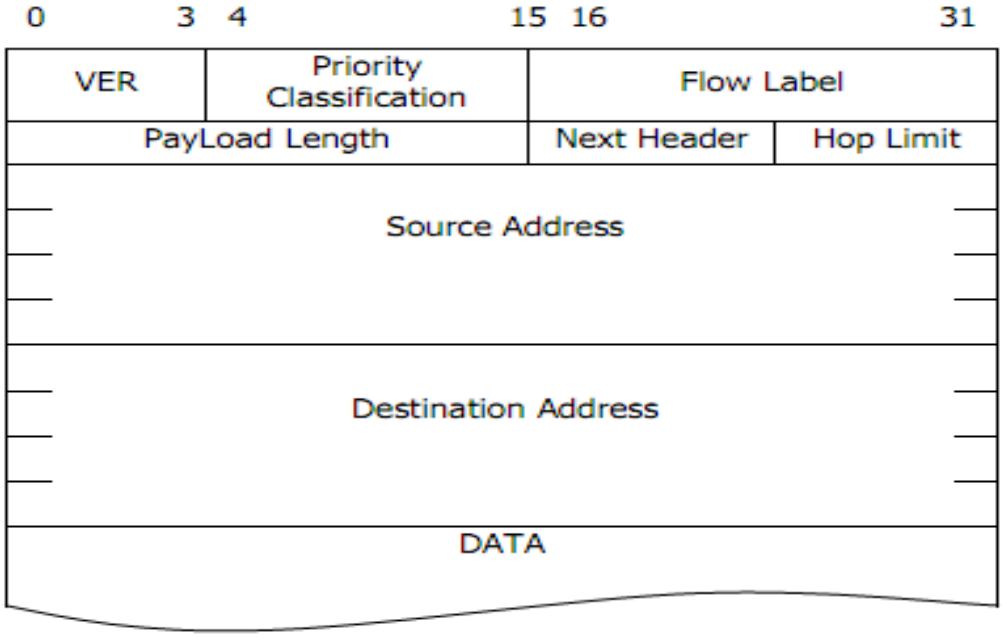
4.2.7 Phiên bản IPv6

Với sự phát triển nhanh chóng của internet thì địa chỉ IPv4 (32 bit) không thể đáp ứng được nhu cầu sử dụng Internet. Để khắc phục điều này phiên bản IPv6 (IP Next Generation) được phát triển. Phiên bản IPv6 có các thay đổi như sau:

- Sử dụng 128 bit địa chỉ mạng thay cho 32 bit địa chỉ như IPv4.
- Mở rộng phần header cho ứng dụng và lựa chọn của khung tin.
- Hỗ trợ các loại dữ liệu audio và video.
- Có các giao thức mở rộng: Cho phép bổ sung nhiều thông tin vào một datagram.

Khung tin IPv6

Phần Header của các khung tin IP đã được thay đổi so với phiên bản IPv4. Phần lớn sự thay đổi của IP là địa chỉ IP 128 bit và bỏ các trường không cần thiết. Cấu tạo của khung tin IP như sau:



Hình 4.11 Cấu trúc gói tin IPv6

TỔNG KẾT CHƯƠNG

Các điểm quan trọng bạn cần nắm được trong chương này:

1. Đặc điểm của giao thức liên mạng IPv4
2. So sánh mô hình TCP và OSI
3. Đặc điểm của các giao thức ARP, RARP, ICMP.
4. Vai trò, chức năng, phương pháp chia mạng con.
5. Cho IP như sau 00001011.01000010.00100110.00000001 và 172.168.12.1

   a. Địa chỉ IP thuộc lớp nào?

   b. Cho biết đâu là NetID và HostID trong địa chỉ mạng trên.

6. Cho 4 địa chỉ host như sau:

   A: 192.168.25.30/27

   B: 192.168.25.34/27

   C: 192.168.25.61/27

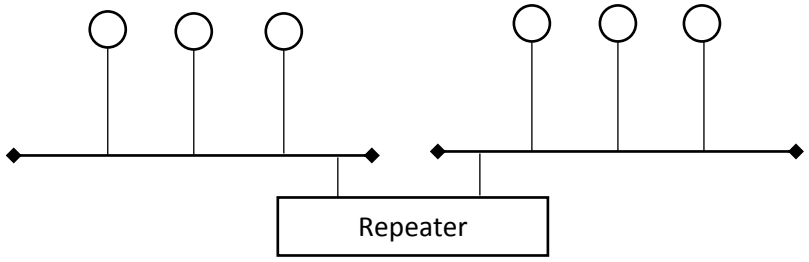
   D: 192.168.25.66/27

   a. Các địa chỉ trên thuộc lớp địa chỉ nào? Nêu rõ cách xác định?
   b. Trong những địa chỉ trên, hãy cho biết những địa chỉ nào cùng một mạng con với nhau.
   c. Liệt kê dãy địa chỉ (địa chỉ mạng, địa chỉ host, địa chỉ broadcast) của nhóm địa chỉ có cùng mạng con vừa tìm được ở câu b?

CHƯƠNG 5
CÁC THIẾT BỊ NỐI KẾTMẠNG

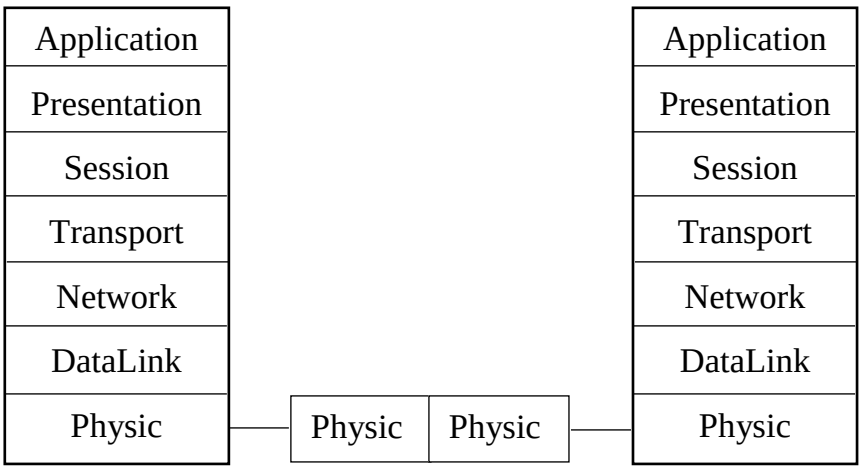
5.1 BỘ KHUYẾCH ĐẠI TÍN HIỆU – REPEATER

- Làm việc với tầng thứ nhất của mô hình OSI - tầng vật lý.
- Repeater có hai cổng. Nó thực hiện việc chuyển tiếp tất cả các tín hiệu vật lý đến từ cổng này ra cổng khác sau khi đã khuyếch đại. Tất cả các LAN liên kết với nhau qua repeater trở thành một LAN.
- Nó chỉ có khả năng liên kết các LAN có cùng một chuẩn công nghệ.



Hình 5.1 Mô hình liên kết mạng sử dụng Repeater

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



Hình 5.2 Hoạt động của Repeater trong mô hình OSI

Hiện nay có 2 loại Repeater đang được sử dụng là Repeater điện và Repeater điện quang.

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

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

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

5.2 BỘ TẬP TRUNG – HUB

- Là tên gọi của Repeater nhiều cổng. Nó thực hiện việc chuyển tiếp tất cả các tín hiệu vật lý đến từ một cổng tới tất cả các cổng còn lại sau khi đã khuyếch đại.
- Tất cả các LAN liên kết với nhau qua Hub sẽ trở thành một LAN
- Hub không có khả năng liên kết các LAN khác nhau về giao thức truyền thông ở tầng liên kết dữ liệu.

Một Hub thông thường có nhiều cổng nối với người sử dụng để gắn máy tính và các thiết bị ngoại vi. Mỗi cổng hỗ trợ một bộ kết nối dùng cặp dây xoắn 10BASET từ mỗi trạm của mạng. Khi tín hiệu được truyền từ một trạm tới hub, nó được lặp lại trên khắp các cổng khác của Hub. Các hub thông minh có thể định dạng, kiểm tra, cho phép hoặc không cho phép bởi người điều hành mạng từ trung tâm quản lý hub.

Hình 5.3 Thiết bị kết nối mạng Hub

Nếu phân loại theo phần cứng thì có 3 loại Hub:

- *Hub đơn (stand alone hub)*
- *Hub module* rất phổ biến cho các hệ thống mạng vì nó có thể dễ dàng mở rộng và luôn có chức năng quản lý, modular có từ 4 đến 14 khe cắm, có thể lắp thêm các modun Ethernet 10BASE-T.
- *Hub phân tầng (Stackable hub)* là lý tưởng cho những cơ quan muốn đầu tư tối thiểu ban đầu nhưng lại có kế hoạch phát triển LAN sau này.

Nếu phân loại theo khả năng ta có 2 loại:

- *Hub bị động (Passive Hub):* Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng.

- *Hub chủ động (Active Hub):* Hub chủ động có các linh kiện điện tử có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng.

Quá trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động. Về cơ bản, trong mạng Ethernet, hub hoạt động như một repeater có nhiều cổng.

5.3 CẦU NỐI – BRIDGE

Cầu nối là một thiết bị hoạt động ở tầng liên kết dữ liệu. Dùng để nối hai hoặc nhiều đoạn (segment) của mạng LAN khác nhau.

Hình 5.4 Cầu nối

a) Chức năng của cầu nối

- Mở rộng khoảng cách của các phân đoạn mạng, tăng số lượng máy tính trên mạng.
- Lọc những gói dữ liệu để gửi đi (hay không gửi) cho đoạn nối hoặc gửi trả lại nơi xuất phát.
- Phân chia một mạng lớn thành 2 mạng nhỏ nhằm cô lập lưu lượng, tăng tốc độ mạng. Nếu lưu lượng từ một nhóm máy tính trở nên quá tải và làm giảm hiệu suất toàn mạng thì cầu nối có thể cô lập máy tính hoặc bộ phận này.
- Làm giảm hiện tượng tắc nghẽn do số lượng máy tính nối vào mạng quá lớn: Cầu nối có thể tiếp nhận một mạng quá tải và chia nhỏ nó ra thành hai mạng riêng biệt, nhằm giảm bớt lưu lượng truyền trên mỗi đoạn mạng và do đó mỗi mạng sẽ hoạt động hiệu quả hơn.
- Kết nối các phương tiện truyền dẫn khác nhau, như cáp xoắn đôi và cáp quang.
- Kết nối các đoạn mạng sử dụng phương thức truy nhập đường truyền khác nhau, chẳng hạn CSMA/CD và chuyển thẻ bài.

b) Nguyên lý hoạt động

- Cầu nối không phân biệt giữa giao thức này với giao thức khác, chỉ có nhiệm vụ chuyển lưu lượng của tất cả các giao thức dọc theo mạng. Vì giao thức nào cũng di chuyển ngang qua cầu nối, nên tùy thuộc vào từng máy tính quyết định chúng có thể nhận diện được giao thức nào.
- Cầu nối hoạt động trên nguyên tắc mỗi nút mạng có một địa chỉ riêng. Cầu nối chuyển gói dữ liệu dựa trên địa chỉ của nút đích (địa chỉ MAC). Khi dữ liệu truyền

qua cầu nối, thông tin địa chỉ của máy tính được lưu trong RAM của cầu nối dùng để xây dựng bảng địa chỉ dựa trên địa chỉ nguồn của gói tin.

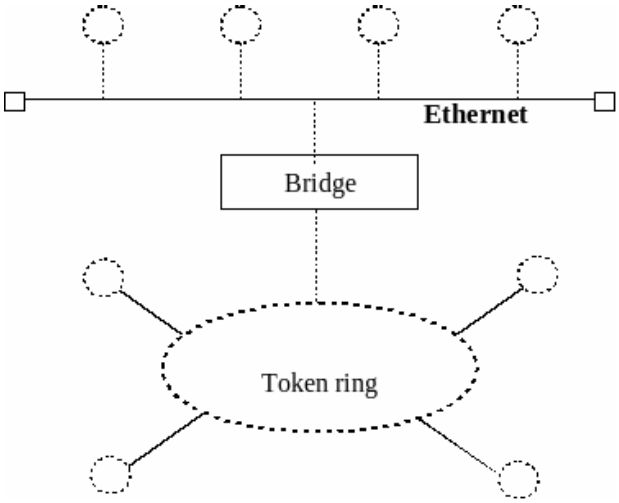
Giao diện Bridge chỉ chứa tầng 1 và tầng con MAC, có chức năng chuyển đổi khuôn dạng của các đơn vị dữ liệu (frame) của các giao thức khác nhau và gửi chúng tới các mạng cục bộ có đính kèm theo phối hợp tốc độ.

Hiện nay có 2 loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch.

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

Ví dụ: Bridge biên dịch nối một mạng Ethernet và một mạng Token ring. Khi đó cầu nối thực hiện như một nút token ring trên mạng Token ring và một nút Enthernet trên mạng Ethernet.

Cầu nối có thể chuyền một gói tin theo chuẩn đang sử dụng trên mạng Enthernet sang chuẩn đang sử dụng trên mạng Token ring. Tuy nhiên chú ý ở đây cầu nối không thể chia một gói tin ra làm nhiều gói tin cho nên phải hạn chế kích thước tối đa các gói tin phù hợp với cả hai mạng. Ví dụ như kích thước tối đa của gói tin trên mạng Ethernet là 1500 bytes và trên mạng Token ring là 6000 bytes do vậy nếu một trạm trên mạng token ring gửi một gói tin cho trạm trên mạng Ethernet với kích thước lớn hơn 1500 bytes thì khi qua cầu nối số lượng byte dư sẽ bị chặt bỏ.



Hình 5.5 Bridge biên dịch

5.4 BỘ CHUYỂN MẠCH - SWITCH

- Làm việc như một Bridge nhiều cổng. Khác với HUB nhận tín hiệu từ một cổng rồi chuyển tiếp tới tất cả các cổng còn lại, Switch nhận tín hiệu vật lý, chuyển đổi thành dữ liệu, từ một cổng, kiểm tra địa chỉ đích rồi gửi tới một cổng tương ứng.

- Nhiều node mạng có thể gửi thông tin đến cùng một node khác tại cùng một thời điểm mở rộng dải thông của LAN. Switch được thiết kế để liên kết các cổng của nó với dải thông rất lớn (vài trăm Mbps đến hàng Gbps).
- Dùng để vượt qua hạn chế về bán kính hoạt động của mạng gây ra bởi số lượng repeater được phép sử dụng giữa hai node bất kỳ của một LAN.
- Là thiết bị lý tưởng dùng để chia LAN thành nhiều LAN "con" làm giảm dung lượng thông tin truyền trên toàn LAN.
- Hỗ trợ công nghệ Full Duplex dùng để mở rộng băng thông của đường truyền mà không có repeater hoặc Hub nào dùng được.
- Hỗ trợ mạng đa dịch vụ (âm thanh, video, dữ liệu)

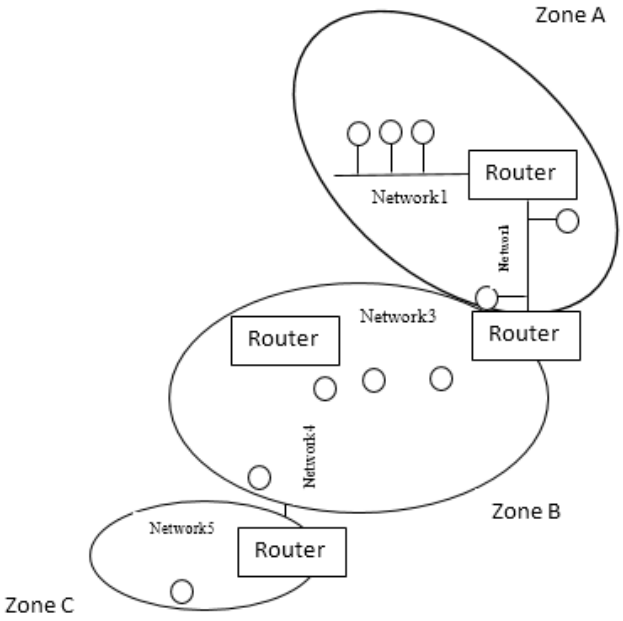
Các bộ chuyển mạch là loại thiết bị mạng hiện đang được sử dụng rộng rãi vì Switch cho phép chuyển sang chế độ truyền không đồng bộ ATM.

5.5 BỘ DẪN ĐƯỜNG –ROUTER

Trong môi trường gồm nhiều đoạn mạng với giao thức và kiến trúc mạng khác nhau, cầu nối không thể bảo đảm truyền thông nhanh trong tất cả các đoạn mạng. Mạng có độ phức tạp như vậy cần một thiết bị không những biết địa chỉ của mỗi đoạn mạng mà còn quyết định định tuyến đường đi tốt nhất để truyền dữ liệu và lọc lưu lượng quảng bá trên các đoạn mạng cục bộ. Thiết bị như vậy gọi là bộ định tuyến.

Chức năng của bộ định tuyến:

- Làm việc trên tầng network của mô hình OSI.
- Thường có nhiều hơn 2 cổng. Nó tiếp nhận tín hiệu vật lý từ một cổng, chuyển đổi về dạng dữ liệu, kiểm tra địa chỉ mạng rồi chuyển dữ liệu đến cổng tương ứng.
- Dùng để liên kết các LAN có thể khác nhau về chuẩn LAN nhưng cùng giao thức mạng ở tầng network.
- Có thể liên kết hai mạng ở rất xa nhau

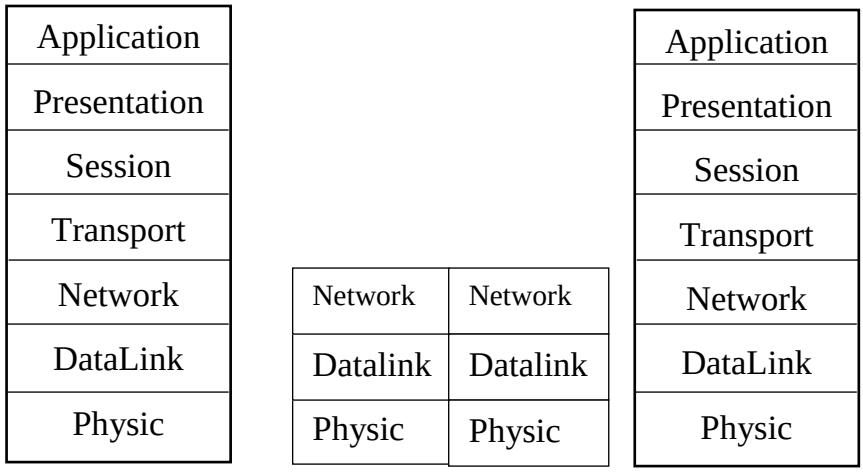


Hình 5.6 Hoạt động của Router

Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong gói tin đó phải chứa các thông tin khác về đích đến) và khi gói tin đến Router thì Router mới xử lý và gửi tiếp. Khi xử lý một gói tin Router phải tìm được đường đi của gói tin qua mạng. Để làm được điều đó Router phải tìm được đường đi tốt nhất trong mạng dựa trên các thông tin nó có về mạng, thông thường trên mỗi Router có một bảng chỉ đường *(Router table)*. Dựa trên dữ liệu về Router gần đó và các mạng trong liên mạng, Router tính được bảng chỉ đường (Router table) tối ưu dựa trên một thuật toán xác định trước.

Người ta phân chia Router thành hai loại là Router có phụ thuộc giao thức *(The protocol dependentrouters)* vàRouterkhông phụ thuộcvào giao thức *(The protocol independent router)* dựa vào phương thức xử lý các gói tin khi qua Router.

- Router có phụ thuộc giao thức: Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác chứ không chuyển đổi phương cách đóng gói của gói tin cho nên cả hai mạng phải dùng chung một giao thức truyền thông.
- Router không phụ thuộc vào giao thức: có thể liên kết các mạng dùng giao thức truyền thông khác nhau và có thể chuyển đổi gói tin của giao thức này sang gói tin của giao thức kia, Router cũng chấp nhận kích thước các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).



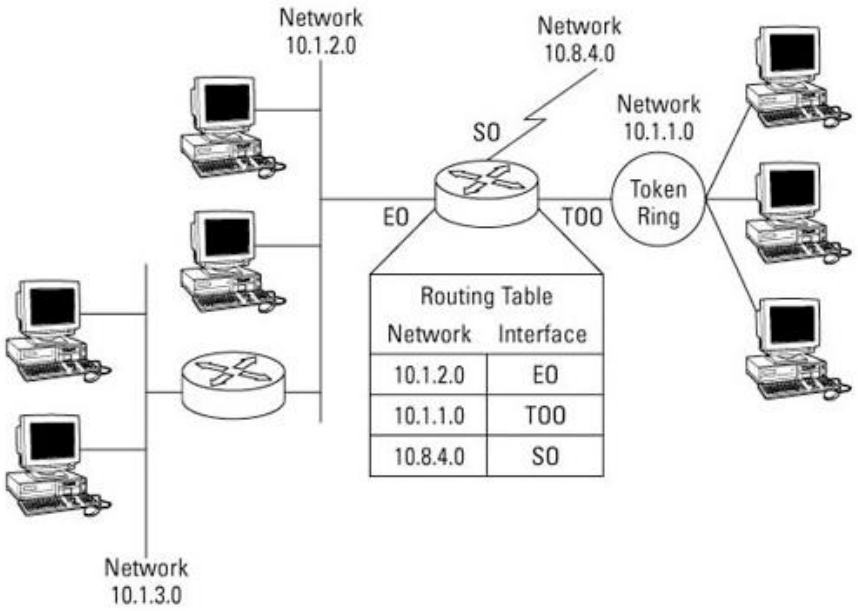
Hình 5.7 Hoạt động của Router trong mô hình OSI

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

Các lý do sử dụng Router :

- Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin muốn đi qua Router cần phải gửi trực tiếp đến nó nên giảm được số lượng gói tin qua nó. Router thường được sử dụng trong khi nối các mạng thông qua các đường dây thuê bao đắt tiền do nó không truyền dư lên đường truyền.
- Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.
- Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.

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



Hình 5.8 Ví dụ về bảng định tuyến của Router

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

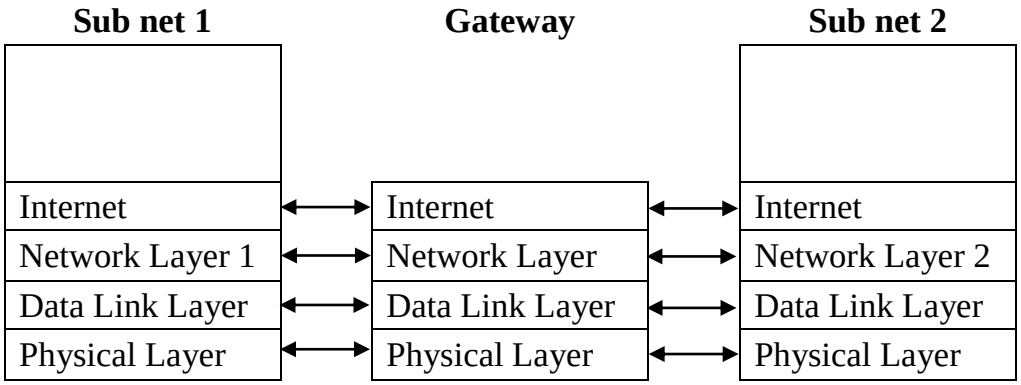
- Phương thức véc-tơ khoảng cách: mỗi Router luôn luôn truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.
- Phương thức trạng thái tĩnh: Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng vàchỉ khi đó các Routerkhác tự cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

** Một số giao thức hoạt động chính của Router*

- RIP*(Routing Information Protocol)* được phát triển bởi Xerox Network system sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc-tơ khoảng cách.
- NLSP *(Netware Link Service Protocol)* được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương thức véc-tơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng chỉ đường giảm đi.
- OSPF *(Open Shortest Path First)* là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...
- IS-IS *(Open System Interconnection Intermediate System to Intermediate System)* là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

5.6 CỔNG GIAO TIẾP – GATEWAY

Hoạt động ở mức mạng, thực hiện ghép nối với WAN. Nguyên lý chung của nối kết này là tạo ra 1 tầng *"liên mạng"* (internet) chung trong tất cả các kiến trúc của mạng con tham gia nối kết. Tầng liên mạng thường là tầng con nằm trên tầng 3 của mô hình OSI.



Hình 5.10 Sơ đồ kiến trúc của gateway trong mô hình OSI

Tầng con internet được cài đặt trong tất cả các trạm cũng như trong các giao diện kết nối (gateway), tầng này cung cấp dịch vụ truyền thông liên mạng với 2 chức năng chính:

- Chuyển đổi các đơn vị dữ liệu của giao thức (Protocol Data Unit – PDU)
- Chọn đường đi cho các PDU này.

Các gói tin ở tầng con Internet lưu thông trong mạng theo phương pháp *"gói/bóc" (encapsulation/decasulation)*. Khi một datagram được truyền từ mạng con này sang mạng con khác thông qua gateway thì nó được bổ sung thêm vào (hoặc tách ra) các phần thông tin điều khiển cần thiết tương ứng với các mạng con.

TỔNG KẾT CHƯƠNG

Các điểm quan trọng bạn cần nắm trong chương này:

1. Vai trò và đặc điểm của các thiết bị nối kết mạng.
2. Nguyên lý hoạt động của cầu nối.
3. Phạm vi hoạt động của các thiết bị nối kết mạng trong mô hình OSI.

CHƯƠNG 6
GIỚI THIỆU CÁC DỊCH VỤ MẠNG

6.1 DỊCH VỤ TÊN (DNS – DOMAIN NAME SYSTEM)

Cho đến bây giờ, chúng ta vẫn dùng địa chỉ để định danh các host. Trong khi rất thuận tiện cho việc xử lý của các router, các địa chỉ số không thân thiện với người dùng. Vì lý do này, các host thường được gán cho một cái tên thân thiện và dịch vụ tên được sử dụng để ánh xạ từ cái tên thân thiện với người dùng này sang địa chỉ số vốn rất thân thiện với các router. Dịch vụ như vậy thường là ứng dụng đầu tiên được cài đặt trong một mạng máy tính do nó cho phép các ứng dụng khác tự do định danh các host bằng tên thay vì bằng địa chỉ. Dịch vụ tên thường được gọi là phần trung gian (middleware) vì nó lấp đầy khoảng cách giữa các ứng dụng khác và lớp mạng phía dưới.

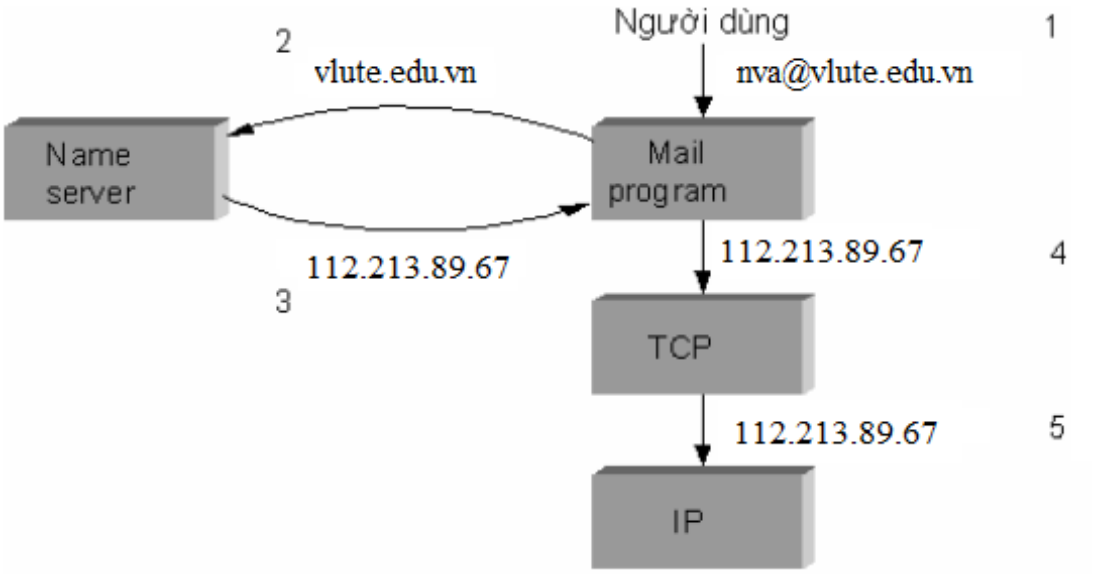
Tên host và địa chỉ host khác nhau ở hai điểm quan trọng. Thứ nhất, tên host thường có độ dài thay đổi và dễ gợi nhớ, vì thế nó giúp người dùng dễ nhớ hơn. Thứ hai, tên thường không chứa thông tin gì để giúp mạng định vị host.

Trước khi đi vào chi tiết cách thức đặt tên cho các host trong mạng như thế nào, chúng ta đi định nghĩa một số thuật ngữ trước:

- *Không gian tên*(name space) định nghĩa tập các tên có thể có. Một không gian tên có thể là phẳng (flat) – một tên không thể được chia thành các thành phần nhỏ hơn hoặc phân cấp.
- Hệ thống tên duy trì một *tập các ánh xạ(collection of bindings)* từ tên sang giá trị. Giá trị có thể là bất cứ thứ gì chúng ta muốn hệ thống tên trả về khi ta cấp cho nó một tên để ánh xạ; trong nhiều trường hợp giá trị chính là địa chỉ host.
- Một *cơ chế phân giải(resolution mechanism)* là một thủ tục mà khi được gọi với tham số là một tên, sẽ trả về một giá trị tương ứng.
- Một *server tên(name server)* là một kết quả cài đặt cụ thể của một cơ chế phân giải luôn sẵn dùng trên mạng và có thể được truy vấn bằng cách gởi đến nó một thông điệp.

Mạng Internet đã có sẵn một hệ thống đặt tên được phát triển tốt, gọi *là hệ thống tên miền (domain name system – DNS).* Vì thế chúng ta sẽ dùng DNS làm cơ sở để thảo luận về vấn đề đặt tên cho các host.

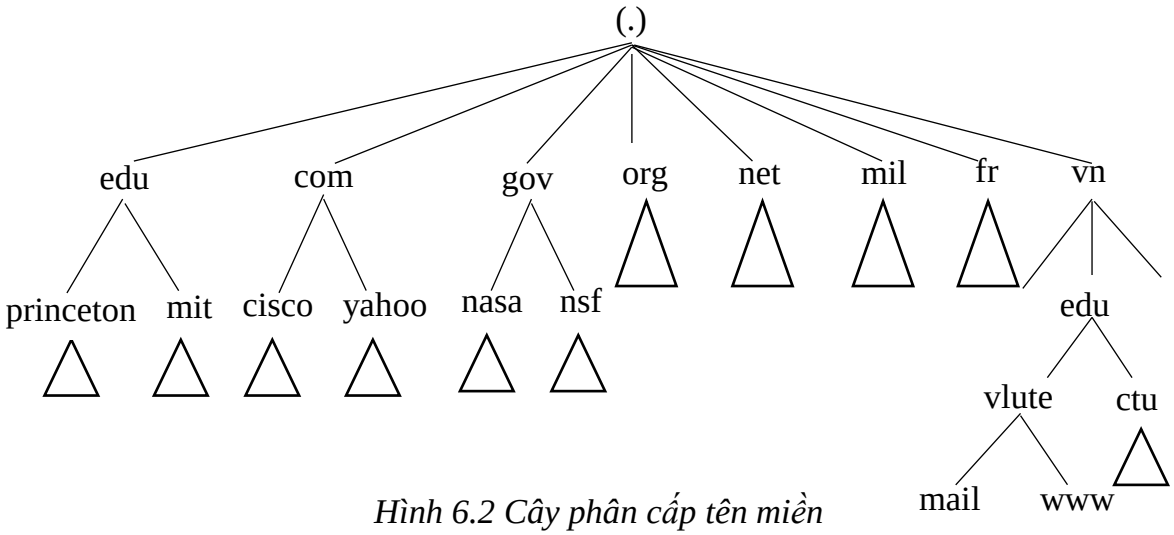
Khi người dùng đưa một tên host đến một ứng dụng (có thể tên host đó là một phần của một tên hỗn hợp như địa chỉ email chẳng hạn), ứng dụng này sẽ liên hệ với hệ thống tên để dịch tên host sang địa chỉ host. Sau đó ứng dụng liền tạo một nối kết đến host đó thông qua giao thức TCP chẳng hạn. Hiện trạng được mô tả trong hình 6.1.



Hình 6.1 Tên máy được dịch sang địa chỉ,
các số từ 1-5 thể hiện trình tự các bước xử lý

6.1.1 Miền phân cấp

DNS cài đặt không gian tên phân cấp dùng cho các đối tượng trên Internet. Các tên DNS được xử lý từ phải sang trái, sử dụng các dấu chấm (.) làm ký tự ngăn cách. (Mặc dù các tên DNS được xử lý từ phải qua trái, người dùng thường đọc chúng từ trái sang phải). Ví dụ tên miền của một host là ***mail.vlute.edu.vn***. Chú ý rằng các tên miền được sử dụng để đặt tên các đối tượng trên Internet, không phải chỉ được dùng để đặt tên máy. Ta có thể mường tượng cấu trúc phân cấp DNS giống như hình dáng cây. Hình 6.2 là một ví dụ.



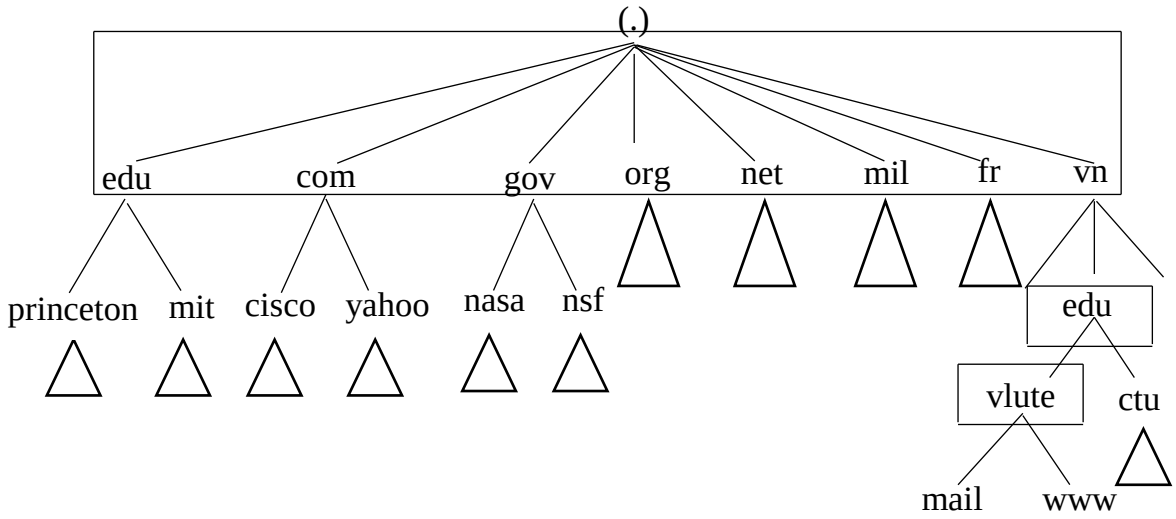
Hình 6.2 Cây phân cấp tên miền

Có thể thấy rằng, cây phân cấp không quá rộng ở mức đầu tiên. Mỗi quốc gia có một tên miền, ngoài ra còn có 6 miền lớn khác gồm: **edu**, **com**, **gov**, **mil**, **org** và **net**. Sáu miền lớn này nằm ở Mỹ. Những tên miền không chỉ ra tên nước một cách tường minh thì mặc nhiên là nằm ở Mỹ.

6.1.2 Các server phục vụ tên

Một cấu trúc tên miền phân cấp hoàn chỉnh chỉ tồn tại trong ý niệm. Vậy thì trong thực tế cấu trúc phân cấp này được cài đặt như thế nào? Bước đầu tiên là chia cấu trúc

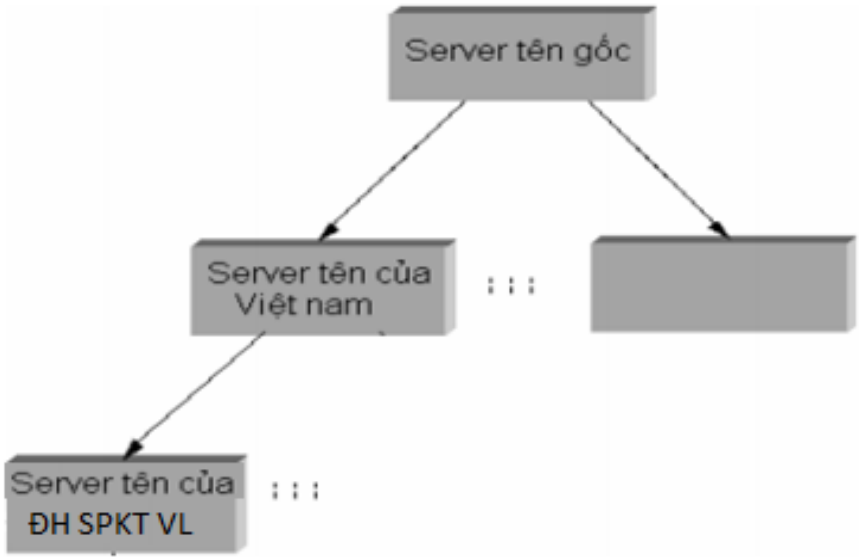
này thành các cây con gọi là các ***vùng*** (zone). Ví dụ, hình 6.3 chỉ ra cách thức cấu trúc phân cấp trong hình 6.2 được chia thành các vùng như thế nào.



Hình 6.3 Cấu trúc miền phân cấp được chia thành các vùng

Mỗi một vùng có thể được xem là đơn vị quản lý một bộ phận của toàn hệ thống phân cấp. Ví dụ, vùng cao nhất của hệ thống phân cấp được quản lý bởi NIC *(Network Information Center)*, vùng **vlute** được quản lý bởi Trường Đại học SPKT Vĩnh Long.

Một vùng luôn có mối liên hệ đến các đơn vị cài đặt cơ bản trong DNS - các server tên. Thông tin chứa trong một vùng được thiết lập tại hai hoặc nhiều server tên. Mỗi server tên có thể truy xuất được qua mạng Internet. Client gởi yêu cầu đến server tên, server tên sẽ trả lời cho yêu cầu đó. Câu trả lời đôi khi chứa thông tin cuối cùng mà client cần, đôi khi lại chứa chỉ điểm đến một server tên khác mà client nên gởi câu hỏi đến đó. Vì thế, theo cách nhìn thiên về cài đặt, người ta có thể nghĩ về DNS được cài đặt bằng cấu trúc phân cấp các server tên hơn là bằng cấu trúc phân cấp các miền.



Hình 6.4 Cấu trúc phân cấp của các server tên

Để ý rằng mỗi vùng được cài đặt trong hai hoặc nhiều server tên với lý do dự phòng; nghĩa là nếu một server bị chết sẽ còn các server khác thay thế. Mặt khác, một server tên cũng có thể được dùng để cài đặt nhiều hơn một vùng.

Mỗi server tên quản lý thông tin về một vùng dưới dạng một tập các mẫu tin tài nguyên *(resource record)*. Mỗi mẫu tin tài nguyên là một ánh xạ từ tên sang giá trị *(name to value binding)*, cụ thể hơn là một mẫu tin gồm 5 trường:

(Tên, Giá trị, Kiểu, Lớp, TTL)

Các trường *Tên*và *Giá trị*là những gì chúng ta muốn có, ngoài tra trường *Kiểu*chỉ ra cách thức mà *Giá trị*được thông dịch. Chẳng hạn, trường *Kiểu = A*chỉ ra rằng *Giá trị*là một địa chỉ IP. Vì thế các mẫu tin kiểu *A*sẽ cài đặt kiểu ánh xạ từ tên miền sang địa chỉ IP. Ví dụ như mẫu tin: *(ns.vlute.edu.vn, 112.213.89.67, A, IN)* chỉ ra rằng địa chỉ IP của host có tên*ns.vlute.edu.vn* là *112.213.89.67*.

Ngoài ra còn có những kiểu khác:

- NS:Trường *Giá trị*chỉ ra tên miền của máy tính đang chạy dịch vụ tên và dịch vụ đó có khả năng thông dịch các tên trong một miền cụ thể.

  Ví dụ mẫu tin*:(vlute.edu.vn, ns.vlute.edu.vn, NS, IN)* chỉ ra rằng server tên của miền vlute.edu.vn có tên là ns.vlute.edu.vn.

- CNAME:Trường *Giá trị*chỉ ra một cái tên giả của một host nào đó. Kiểu này được dùng để đặt thêm bí danh cho các host trong miền.

- MX:Trường *Giá trị*chỉ ra tên miền của host đang chạy chương trình mail server mà server đó có khả năng tiếp nhận những thông điệp thuộc một miền cụ thể.

Ví dụ mẫu tin *(vlute.edu.vn, mail.vlute.edu.vn, MX, IN)* chỉ ra rằng host có tên mail.vlute.edu.vn là mail server của miền vlute.edu.vn.

Trường *Lớp* được sử dụng nhằm cho phép thêm vào những thực thể mạng không do NIC quản lý. Ngày nay, lớp được sử dụng rộng rãi nhất là loại được Internet sử dụng; nó được ký hiệu là *IN*. Cuối cùng trường *TTL*chỉ ra mẫu tin tài nguyên này sẽ hợp lệ trong bao lâu. Trường này được sử dụng bởi những server đang trữ tạm các mẫu tin của server khác; khi trường *TTL*hết hạn, các mẫu tin chứa trường *TTL*hết hạn đó sẽ bị các server xóa khỏi cache của mình.

Để hiểu rõ hơn cách thức các mẫu tin tài nguyên được thể hiện trong cấu trúc phân cấp, xem ví dụ được vẽ trong hình 6.3. Để đơn giản hóa vấn đề, chúng ta bỏ qua trường *TTL*và cung cấp thông tin tương ứng cho một server tên làm nhiệm vụ quản lý một vùng.

Đầu tiên, server tên gốc (root name server) sẽ chứa một mẫu tin *NS*cho mỗi server cấp hai. Nó cũng chứa một mẫu tin *A* để thông dịch từ một tên server cấp hai sang địa chỉ IP của nó. Khi được ghép với nhau, hai mẫu tin này cài đặt một cách hiệu quả một con trỏ từ server gốc đến mỗi server cấp hai của nó.

(edu.vn, dns1.vnnic.net.vn, NS, IN);

thông tin về miền con edu.vn lưu ở máy dns1.vnnic.net.vn
(dns1.vnnic.net.vn, 203.162.57.105, A, IN);

máy dns1.vnnic.net.vn có địa chỉ 203.162.57.105

(cisco.com, ns1.cisco.com, NS, IN)

Kế tiếp, miền edu.vn có một server tên hiện hữu tại máy dns1.vnnic.net.vn và server này lại chứa các mẫu tin sau:

(vlute.edu.vn, ns.vlute.edu.vn, NS, IN)
(ns.vlute.edu.vn, 203.162.41.166, A, IN)
▪
▪
▪

Cuối cùng server ns.vlute.edu.vn lại chứa thông tin về các máy tính của trường Đại Học SPKT Vĩnh Long cũng như các miền con của Trường Đại Học SPKT Vĩnh Long

(cit.vlute.edu.vn, ns.cit.vlute.edu.vn, NS, IN)
(ns.cit.vlute.edu.vn, 112.213.89.67*, A, IN)*
(vlute.edu.vn, mail.vlute.edu.vn, MX, IN)
(mail.vlute.edu.vn, 112.213.89.67*, A, IN)*
(www.vlute.edu.vn, mail.vlute.edu.vn, CNAME, IN)
▪
▪
▪

Chú ý rằng trên lý thuyết các mẫu tin có thể được dùng để định nghĩa bất kỳ kiểu đối tượng nào, DNS lại thường được sử dụng để định danh các host và site. DNS không được dùng để định danh cá nhân con người hoặc các đối tượng khác như tập tin hay thư mục, việc định danh này được thực hiện trong các hệ thống phục vụ tên khác. Ví dụ X.500 là hệ thống định danh của ISO được dùng để định danh con người bằng cách cung cấp thông tin về tên, chức vụ, số điện thoại, địa chỉ,…. X.500 đã chứng tỏ là quá phức tạp nên không được hỗ trợ bởi các search engine nổi tiếng hiện nay. Tuy nhiên nó lại là nguồn gốc phát sinh ra chuẩn LDAP *(Lightweight Directory Access Protocol).* LDAP vốn là thành phần con của X.500 được thiết kế để làm phần front-end cho X.500. Ngày nay LDAP đang trở nên phổ biến nhất là ở cấp độ công ty, tổ chức lớn, đóng vai trò là hệ thống học và quản lý thông tin về người dùng của nó.

6.1.3 Phương pháp phân tích tên

Với một hệ thống phân cấp các server tên đã trình bày, bây giờ chúng ta đi tìm hiểu cách thức một khách hàng giao tiếp với các server này để phân tích cho được một tên miền thành địa chỉ. Giả sử một khách hàng muốn phân tích tên miền *www.vlute.edu.vn*, đầu tiên khách hàng này sẽ gởi yêu cầu chứa tên này đến server tên gốc. Server gốc không thể so khớp tên theo yêu cầu với các tên mà nó chứa, liền trả lời cho khách hàng một mẫu tin kiểu NS chứa edu.vn. Server gốc cũng trả về tất cả các mẫu tin có liên quan đến mẫu tin NS vừa nói, trong đó có mẫu tin kiểu A chứa địa chỉ của dns1.vnnic.vnn.vn. Khách hàng chưa có thông tin cuối cùng mà nó muốn, tiếp tục gởi yêu cầu đến server tên tại địa chỉ 203.162.57.105. Server tên thứ hai này lại không thể so khớp tên theo yêu cầu với các tên mà nó chứa, tiếp tục trả lời cho khách hàng một mẫu tin loại NS chứa tên ctu.edu.vn cùng với mẫu tin kiểu A tương ứng với tên server là ns.ctu.edu.vn. Khách hàng lại tiếp tục gởi yêu cầu đến server tên tại địa chỉ 112.213.89.67và lần này nhận được câu trả lời cuối cùng có kiểu A cho tên *www.vlute.edu.vn*.

Ví dụ trên chắc chắn sẽ để lại nhiều câu hỏi về quá trình phân giải tên. Câu hỏi thường được đặt ra là: Lúc khởi đầu, làm sao khách hàng có thể định vị được server

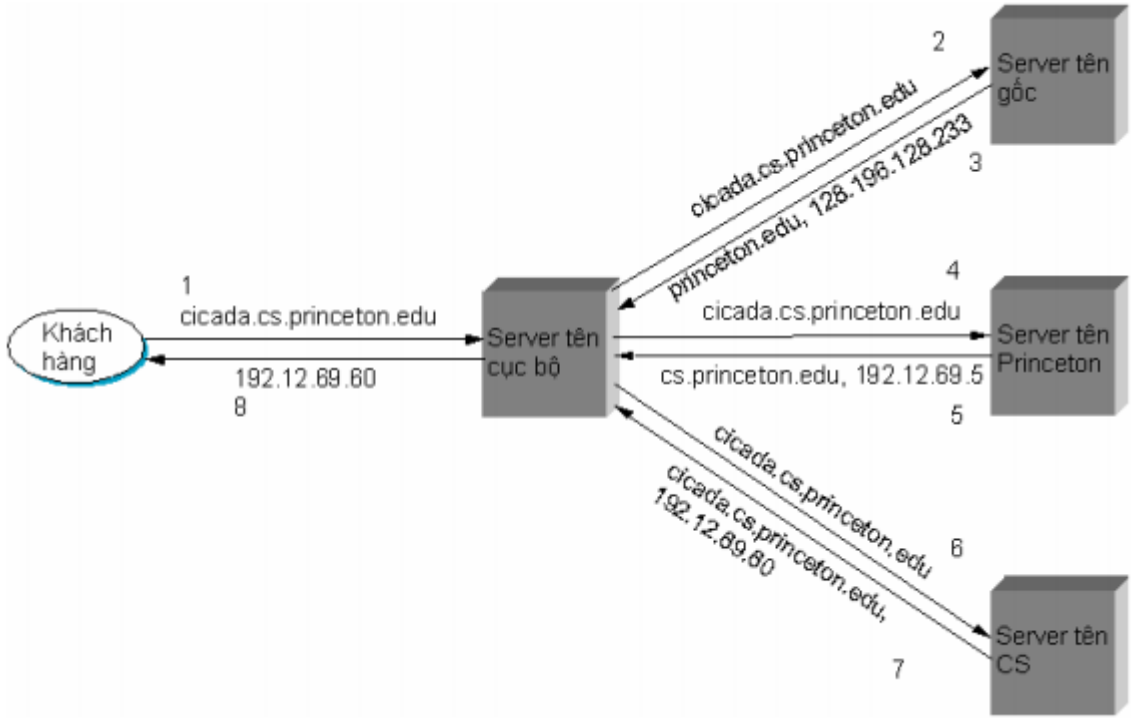
gốc. Đây là bài toán cơ bản đặt ra cho mọi hệ thống phục vụ tên và câu trả lời là: hệ thống phải tự thân vận động để có được thông tin về các server gốc. Trong tình huống của hệ thống DNS, ánh xạ từ tên sang địa chỉ của một hay nhiều server gốc được phổ biến cho mọi người, nghĩa là ánh xạ đó được loan báo thông qua các phương tiện truyền thông khác nằm ngoài hệ thống tên.

Tuy nhiên, trong thực tế không phải tất cả khách hàng đều biết về các server gốc. Thay vào đó, chương trình khách hàng chạy trên mỗi host trong Internet được khởi động với các địa chỉ lấy từ server tên cục bộ. Ví dụ, tất cả các host trong Khoa Công Nghệ Thông Tin của Trường Đại Học SPKT Vĩnh Long đều biết server tên nội bộ đang chạy trên máy ns.fit.vlute.edu.vn. Đến lượt server tên cục bộ này lại chứa các mẫu tin tài nguyên cho một hoặc nhiều server gốc của nó, ví dụ:

(. , a.root-servers.net, NS, IN)
(a.root-server.net, 198.41.0.4, A, IN)

Trong ví dụ trên, server tên cục bộ có thông tin về một server tên gốc của nó (chú ý miền gốc được ký hiệu bằng dấu chấm) là a.root-servers.net, địa chỉ IP tương ứng của server gốc này là 198.41.0.4.

Từ đó, việc phân giải một tên miền bắt đầu từ câu truy vấn của khách hàng đến server cục bộ. Nếu server cục bộ không có sẵn câu trả lời, nó sẽ gởi câu hỏi đến server từ xa dùm cho khách hàng. Chuỗi hành động trên có thể được mô tả trong hình 6.5



Hình 6.5 Quá trình phân giải tên trong thực tế, các số 1 đến 8 chỉ ra trình tựthực hiện

6.2 ELECTRONIC MAIL (SMTP, MIME, POP3, IMAP)

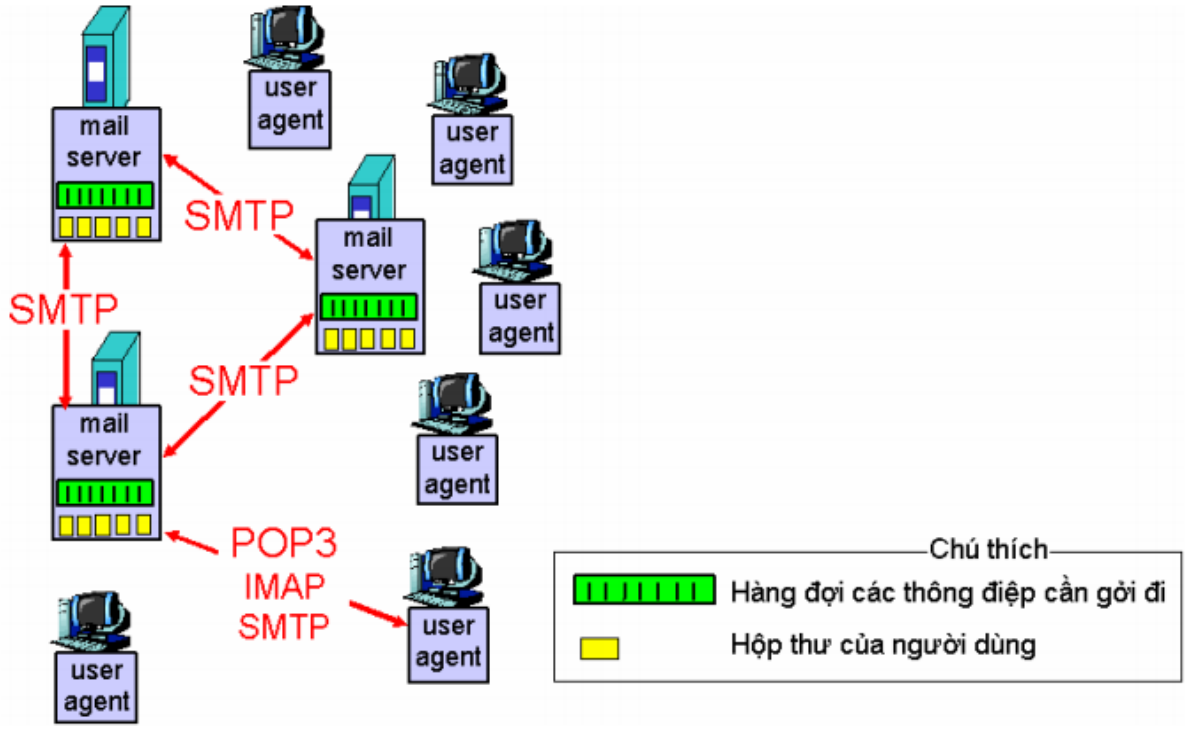
Email là một trong những ứng dụng mạng lâu đời nhất nhưng lại phổ dụng nhất. Thử nghĩ khi bạn muốn gởi thông điệp đến một người bạn ở đầu kia của thế giới, bạn muốn mang thư chạy bộ qua đó hay chỉ đơn giản lên máy tính gõ ít hàng và nhấn nút Send. Thật ra, những bậc tiền bối của mạng ARPANET đã không tiên đoán được email sẽ là ứng dụng then chốt chạy trên mạng này, mục tiêu chính của họ là thiết kế hệ thống

cho phép truy cập tài nguyên từ xa. Hệ thống email ra đời không mấy nổi bật, để bây giờ lại được sử dụng hằng ngày bởi hàng triệu người trên thế giới. Mục tiêu của phần này là chỉ ra những nhân vật hoạt động trong hệ thống email, vai trò của họ, giao thức mà họ sử dụng và khuôn dạng thông điệp mà họ trao đổi với nhau.

6.2.1 Các thành phần của hệ thống email

Một hệ thống email thường có 3 thành phần chính: Bộ phận trợ giúp người dùng (User Agent), Mail Server và các giao thức mà các thành phần này dùng để giao tiếp với nhau. Người ta phân loại các giao thức như sau:

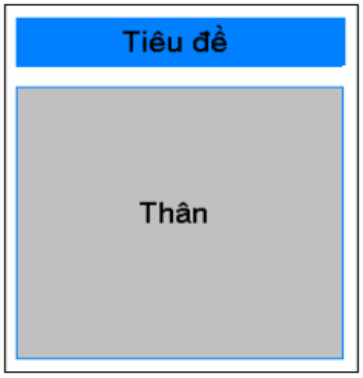
- Giao thức giữa các mail servers bao gồm:
  - ✓ SMTP (Simple Mail Transfer Protocol): được các server dùng để chuyển thư qua lại với nhau. Ví dụ nôm na, nó giống như cách thức mà các trạm bưu điện dùng để chuyển các thùng thư của khách hàng cho nhau. Thông tin chi tiết về giao thức này được mô tả trong tài liệu RFC 822.
- Giao thức giữa mail server và user agent bao gồm:
  - ✓ POP3 *(Post Offic Protocol version 3 [RFC 1939])*: được user agent sử dụng để lấy thư về từ hộp thư của nó trên server.
  - ✓ SMTP: Được user agent sử dụng để gởi thư ra server.
  - ✓ IMAP: *(Internet Mail Access Protocol [RFC 1730])*: Có nhiều tính năng vượt trội hơn POP3. Ngoài ra IMAP còn cho phép gởi mail.



Hình 6.6Giao thức giữa mail server và user agent

6.2.2 Khuôn dạng của một email

RFC 822 định nghĩa một email gồm có hai phần: phần tiêu đề (header) và phần thân (body).



Hình 6.8 Khuôn dạng của email

Cả hai phần đều được thể hiện dưới dạng ký tự ASCII. Lúc đầu, phần thân được qui định có khuôn dạng văn bản đơn giản. Sau này người ta đề nghị một chuẩn mới gọi là MIME, có thể cho phép phần thân của email chứa bất kỳ loại dữ liệu nào.

Phần tiêu đề bao gồm nhiều dòng thông tin, mỗi dòng kết thúc bằng hai ký tự <CRLF>. Phần tiêu đề được chia khỏi phần thân bởi một hàng rỗng. Mỗi một hàng tiêu đề chứa một cặp "tên" và "giá trị", cách nhau bởi dấu hai chấm (:). Người dùng có thể rất quen với nhiều hàng tiêu đề vì họ thường phải điền thông tin vào đấy. Ví dụ

Tên	Giá trị
From:	Địa chỉ người gởi
To:	Địa chỉ của người nhận
Subject:	Chủ đề thư
Date:	Ngày gởi

RFC 822 được mở rộng năm 1993 (và được cập nhật lại năm 1996) để cho phép email mang được nhiều loại dữ liệu: audio, video, hình ảnh, tài liệu Word, … MIME *(Multipurpose Internet Mail Extensions)* về cơ bản có ba phần. Phần đầu tiên là tập các dòng header dùng để bổ túc cho phần header cũ của RFC 822. Theo nhiều cách, những dòng header này mô tả dữ liệu chứa trong phần thân. Cụ thể như sau:

Tên	Giá trị
MIME-Version:	Phiên bản MIME đang sử dụng
Content-Description:	Mô tả trong thư đang có dữ liệu gì
Content-Type:	Mô tả kiểu dữ liệu đang nằm trong thư
Content-Transfer-Encoding:	Mô tả cách thức mã hóa dữ liệu trong thư

Phần thứ hai là các định nghĩa cho một tập các kiểu nội dung (và kiểu con nếu có). Ví dụ một số kiểu mà MIME định nghĩa:

Kiểu	Ý nghĩa
image/gif	Ảnh dạng gif
image/jpeg	Ảnh dạng jpeg
text/plain	Văn bản đơn giản

text/richtext	Văn bản mở rộng (có đặt font chữ, được định dạng đậm, nghiêng hoặc gạch dưới …)
application	Dữ liệu trong thư được xuất ra từ một ứng dụng nào đó. Chẳng hạn: *application/postscript*: tài liệu Postscript (.ps) *application/msword*: tài liệu Microsoft Word (.doc)

MIME cũng định nghĩa kiểu multipartđể chỉ ra cách mà phần thân của thư mang nhiều loại dữ liệu khác nhau như thế nào. Chỉ có một kiểu con của multipartlà mixedvới ý nói rằng trong phần thân của thư có nhiều mảnh dữ liệu khác nhau, độc lập với nhau và được sắp xếp theo một trình tự cụ thể. Mỗi mảnh dữ liệu sẽ có phần tiêu đề riêng để mô tả kiểu dữ liệu của mảnh đó. Phần thứ ba mô tả cách thức mã hóa các kiểu dữ liệu nói trên để có thể truyền chúng dưới dạng ASCII. Lý do để mọi bức thư phải chứa các ký tự ASCII là vì để đi được đến đích, bức thư đó có thể phải trung chuyển qua nhiều gateway, mà các gateway này đều coi mọi bức thư dưới dạng ASCII. Nếu trong thư chứa bất kỳ ký tự nào khác ASCII thì thư sẽ bị đứt gãy nội dung. MIME sử dụng phương pháp mã hóa trực tiếp dữ liệu nhị phân thành các ký tự nhị phân, gọi là base64. Ý tưởng của base64là ánh xạ 3 bytes dữ liệu nhị phân nguyên thủy thành 4 ký tự ASCII. Giải thuật đơn giản như sau: tập hợp 3 bytes dữ liệu nhị phân lại thành 24 bits, sau đó chia 24 bits này thành 4 cụm, một cụm 6 bits. Một cụm 6 bits được ánh xạ vào một trong 64 ký tự ASCII hợp lệ; ví dụ 0 ánh xạ thành A, 1 ánh xạ thành B…Nếu nhìn vào bức thư đã được mã hóa dạng base64, người dùng sẽ thấy chỉ có 52 chữ cái cả hoa lẫn thường, 10 chữ số từ 0 đến 9 và các ký tự đặc biệt + và /. Đối với những người dùng chỉ sử dụng trình đọc thư hỗ trợ duy nhất kiểu ký tự thì việc đọc những bức thư có kiểu base64 sẽ rất là khó. Vì lý do đó, MIME còn hỗ trợ kiểu mã hóa ký tự thường được gọi là 7-bit. 7-bitsẽ giữ nguyên dạng ký tự mà người ta nhập vào.

Tổng hợp lại, ví dụ một bức thư có 2 loại dữ liệu: văn bản thường, một ảnh JPEG, sẽ có hình dáng như sau:

```
From: nva@cit.vlute.edu.vn
To: TH31@cit.vlute.edu.vn
Subject: Picture of students.
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=”—98766789”

--98766789
Content-Transfer-Encoding: 7bit
Content-Type: text/plain

Hi,
Please find a picture of you.
--98766789
Content-Transfer-Encoding: base64
Content-Type: image/jpeg

base64 encoded data .....
.....
.....base64 encoded data
--98766789--
```

6.2.3 Chuyển thư

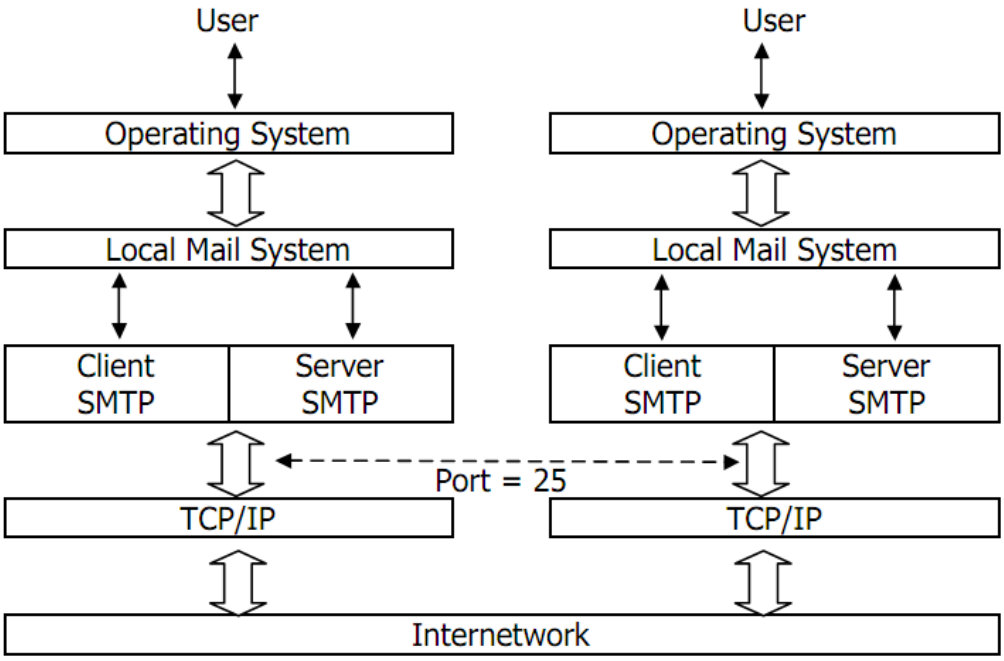
Kế đến, chúng ta sẽ xem xét giao thức SMTP – giao thức được dùng để chuyển thư từ máy này đến máy kia. Để đặt SMTP vào đúng ngữ cảnh, chúng ta nên nhắc lại các nhân vật then chốt trong hệ thống email. Đầu tiên, người dùng tương tác với trình đọc thư (hay còn gọi là user agent) để soạn, lưu, tìm kiếm và đọc thư của họ. Hiện trên thị trường có nhiều phần mềm đọc thư, cũng giống như hiện cũng đang có nhiều loại trình duyệt Web vậy. Thứ hai, có trình xử lý thư (hay còn gọi là mail server) chạy trên một máy nào đó trong mạng nội bộ của người dùng. Có thể xem mail server như một bưu điện: Người dùng trao cho mail server các bức thư mà họ muốn gởi cho người dùng khác, mail server sử dụng giao thức SMTP trên TCP để chuyển bức các thư này đến mail server bên đích. Mail server bên đích nhận các thư đến và đặt chúng vào hộp thư của người dùng bên đích. Do SMTP là giao thức mà rất nhiều người có thể tự cài đặt, vì thế sẽ có rất nhiều sản phẩm mail server hiện có trên thị trường. Sản phẩm mail server thường được sử dụng nhất là sendmail, ban đầu được cài đặt trong hệ điều hành Berkeley Unix.

Tất nhiên mail server bên máy gởi có thể kết nối SMTP/TCP trực tiếp tới mail server bên máy nhận, nhưng trong thực tế, một bức thư có thể đi ngang qua vài mail gateways trước khi đến đích. Cũng giống như máy đích, mỗi mail gateway cũng chạy một mail server. Không phải ngẫu nhiên mà các nút chuyển thư trung gian được gọi là mail gateway. Công việc của chúng cũng giống như các IP gateway là lưu tạm và chuyển phát tiếp các bức thư của người dùng. Điểm khác nhau duy nhất giữa chúng là, mail gateway trữ tạm các bức thư trong đĩa, trong khi các IP gateway trữ tạm các gói tin IP trong bộ nhớ.

Bạn có thể đặt câu hỏi: tại sao lại cần đến các mail gateways? Tại sao không dùng phương pháp nối kết SMTP/TCP trực tiếp từ bên gởi sang bên nhận? Lý do thứ nhất, người gởi không muốn kèm trong thư địa chỉ của máy đích. Ví dụ, riêng việc nhập vào trong thư địa chỉ đích nva@cit.vlute.edu.vnđã mất công rồi, không ai thấy thoải mái khi phải nhập thêm địa chỉ máy đích là cntt.cit.vlute.edu.vn. Thứ hai, không chắc lúc bên gởi thiết lập nối kết đến bên nhận, người dùng bên nhận đã bật sẵn máy! Thành thử chỉ cần địa chỉ thư bên nhận là đủ. Khi bức thư đến được mail gateway của Khoa Công Nghệ Thông Tin – Đại học SPKT Vĩnh Long, nếu người dùng nvađang mở máy, mail gateway sẽ chuyển thư cho anh ta ngay, nếu không mail gateway sẽ trữ tạm thư trên đĩa của nó đến khi nvabật máy lên và kiểm tra thư.

Dù có bao nhiêu mail gateways trung gian trên đường đến đích vẫn không đáng lo lắng, bởi vì mỗi mail gateway trung gian sẽ nỗ lực sử dụng một kết nối SMTP độc lập đến gateway kế tiếp trên đường đi nhằm chuyển thư càng ngày càng đến gần người nhận.

*SMTP (Simple Mail Transfer Protocol)*là một giao thức đơn giản dùng các ký tự ASCII. Sau khi thiết lập nối kết TCP đến cổng 25 của máy đích (được coi là server), máy nguồn (được coi là client) chờ nhận kết quả trả về từ server. Server khởi đầu cuộc đối thoại bằng cách gởi một dòng văn bản đến client thông báo danh tính của nó và khả năng tiếp nhận thư. Nếu server không có khả năng nhận thư tại thời điểm hiện tại, client sẽ hủy bỏ nối kết và thử thiết lập lại nối kết sau.



Hình 6.7 Mối quan hệ giữa SMTP và hệ thống Mail cục bộ

Các lệnh của giao thức SMTP:

Lệnh	**Ý nghĩa**
HELLO	Xưng danh với SMTP bên nhận, báo cho bên nhận biết bên gửi là ai. SMTP bên gửi gửi lệnh này đầu tiên cho SMTP bên nhận.
MAIL	Khởi động một cuộc giao dịch mail mà mục đích cuối cùng là chuyển giao các mail tới một hay nhiều Mailbox (nơi chứa Mail nhận được) khác nhau.
RCPT	Nói rõ người nhận mail là ai?
DATA	Các dòng lệnh DATA là dữ liệu của Mail. Đới với SMTP, chuỗi ký tự "CRLF.CRLF" báo nhận biết kết thúc nội dung Mail.
RSET	Bỏ (Reset) cuộc giao dịch hiện tại.
NOOP	Yêu cầu SMTP bên nhận không làm gì ngoài việc trả về câu trả lời OK (dùng để kiểm tra).
QUIT	Yêu cầu SMTP nhận trả lời OK và kết thúc phiên giao dịch hiện tại.
VRFY	Yêu cầu SMTP bên nhận kiểm tra người nhận là đúng, xác nhận các tham số gửi theo dòng lệnh.
SEND	Khởi động một cuộc giao dịch mà mail sẽ được gửi tới một hay nhiều thiết bị đầu cuối chứ không phải qua Mailbox.
SOML	Khởi động một cuộc giao dịch mà mail sẽ được gửi tới một hay nhiều thiết bị đầu cuối hay Mailbox.
SAML	Khởi động một cuộc giao dịch mà mail sẽ được gửi tới một hay nhiều thiết bị đầu cuối hay Mailbox.
HELP	Yêu cầu SMTP bên nhận gửi thông tin giúp đỡ cho SMTP bên phát.

EXPN	Yêu cầu SMTP bên nhận gửi về danh sách những người nhận mail để có thể mở rộng việc chuyển mail cho các user khác.
TURN	Yêu cầu SMTP bên nhận gửi OK và đổi vai trò trở thành SMTP gửi.

Nếu server sẵn sàng nhận thư, client sẽ thông báo lá thư đó từ đâu đến và ai sẽ là người nhận. Nếu người nhận đó tồn tại, server sẽ thông báo cho client tiếp tục gởi thư. Sau đó client gởi thư và server báo nhận cho thư đó. Sau khi cả hai bên hoàn tất phiên truyền nhận, kết nối sẽ được đóng lại.

Ví dụ một phiên truyền nhận được cho ngay dưới đây. Những dòng bắt đầu bằng C:là của phía client gởi đi; bằng S:là các câu trả lời của server.

S: 220 vlute.edu.vn
C: HELO cit.vlute.edu.vn
S: 250 vlute.edu.vn says hello to cit.vlute.edu.vn
C: MAIL FROM: <nva@cit.vlute.edu.vn>
S: 250 Sender ok
C: RCPT TO: <lhly@yale.edu>
S: 250 Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Subject: It’s Xmast!
C: So I hope you a merry Xmas and a happy new year!
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 Bye - Bye

LỆNH CỦA CLIENT	
Lệnh	**Ý nghĩa**
HELO	Câu chào và xưng danh của client
MAIL FROM	Địa chỉ email của người gởi
RCPT TO	Địa chỉ email của người nhận
DATA	Bắt đầu truyền nội dung của thư
QUIT	Hủy nối kết
TRẢ LỜI CỦA SERVER	
Trả lời	**Ý nghĩa**
250	Yêu cầu hợp lệ
550	Yêu cầu không hợp lệ, không tồn tại hộp thư như client đã chỉ ra
354	Cho phép bắt đầu nhập thư vào. Kết thúc thư bằng <CRLF>.<CRLF>
221	Server đang đóng kết nối TCP

Vẫn còn nhiều lệnh và mã trả lời chưa được trình bày, tham khảo tài liệu RFC 822 để có được đầy đủ thông tin.

6.2.4 Phân phát thư

Như đã trình bày, khi đứng về góc độ người dùng thư, họ sẽ dùng user agent để gởi và nhận thư cho họ. User agent dùng giao thức SMTP để gởi thư đi, dùng giao thức POP3 hoặc IMAP để nhận thư về.

6.2.4.1POP3

Một phiên làm việc theo giao thức POP3 bắt đầu tại user agent. User agent khởi động một nối kết TCP đến cổng 110 của mail server. Khi kết nối thực hiện xong, phiên làm việc POP3 sẽ trải qua theo thứ tự ba kỳ:

1. Chứng thực.
2. Giao dịch dữ liệu.
3. Cập nhật.

Kỳ chứng thực buộc người dùng thực hiện thủ tục đăng nhập bằng cách nhập vào hai lệnh sau:

Lệnh	Ý nghĩa
USER <*tên người dùng*>	Khai báo tên người dùng.
PASS <*mật khẩu*>	Khai báo mật khẩu.

Báo trả của mail server sẽ là một trong hai câu sau:

Trả lời	Ý nghĩa
+OK <*chú thích*>	Khai báo của người dùng là đúng.
+ERR <*chú thích*>	Khai báo của người dùng là sai và lời giải thích.

Trong kỳ giao dịch, người dùng có thể xem danh sách thư chưa nhận về, nhận thư về và xóa thư trong hộp thư của mình khi cần thiết. Các lệnh mà người dùng thường sử dụng để giao dịch với server là:

Lệnh	Ý nghĩa
LIST [<*số thứ tự thư*>]	Nếu dùng LIST không tham số, server sẽ trả về toàn bộ danh sách các thư chưa nhận. Nếu có tham số là số thứ tự thư cụ thể, server sẽ trả về thông tin của chỉ bức thư đó thôi.
RETR <*số thứ tự thư*>	Tải lá thư có số thứ tự <*số thứ tự thư*> về.
DELE <*số thứ tự thư*>	Xóa lá thứ số <*số thứ tự thư*> khỏi hộp thư.
QUIT	Hoàn tất giai đoạn giao dịch và hủy nối kết TCP

Các trả lời của server có thể là các số liệu mà client yêu cầu hoặc các thông báo +OK, -ERR như trong phần đăng nhập.

Sau đây là dàn cảnh một phiên làm việc ví dụ giữa người dùngnvakhi anh ta đăng nhập và làm việc trên hộp thư của mình tại server có địa chỉ **mail.vlute.edu.vn**.

Client	Server	Giải thích
	+OK POP3 server ready	Server sẵn sàng phục vụ client
USER ptphi		
	+OK	Server xác nhận người dùng hợp lệ
PASS godblessus		
	+OK login successfully	Chứng thực thành công
LIST		nva kiểm tra hộp thư
	+OK 1 1024 2 2550	Hộp thư của ptphi còn hai thư chưa nhận về, thư thứ nhất có kích thước 1024 bytes, thư thứ hai có kích thước 2550 bytes
RETR 1		ptphi tải thư thứ nhất về
	+OK	server gởi thư thứ 1 cho ptphi
DELE 1		nva xóa thư thứ nhất trong hộp thư
	+OK	server xoá thư thứ 1 thành công
QUIT		nva hủy nối kết
	+OK Bye-Bye	server hủy nối kết

6.2.4.2 IMAP

Với những người dùng có một tài khoản email trên một ISP và người dùng này thường truy cập email trên một PC thì giao thức POP3 hoạt động tốt. Tuy nhiên, một sự thật trong ngành công nghệ máy tính, khi một thứ gì đó đã hoạt động tốt, người ta lập tức đòi hỏi thêm nhiều tính năng mới. Điều đó cũng xảy ra đối với hệ thống email. Ví dụ, người ta chỉ có một tài khoản email nhưng họ lại muốn ngồi đâu cũng truy cập được nó. POP3 cũng làm được việc này bằng cách đơn giản là tải hết tất cả các email xuống máy PC mà người dùng này đang ngồi làm việc. Và dĩ nhiên là thư của người dùng này nằm rải rác khắp nơi.

Sự bất tiện này khơi mào cho sự ra đời của giao thức phân phối thư mới, IMAP *(Internet Message Access Protocol)*, được định nghĩa trong RFC 2060. Không giống như POP2, IMAP coi các thông điệp mặc nhiên nằm trên server vô hạn và trên nhiều hộp thư. IMAP còn đưa ra cơ chế cho phép đọc các thông điệp hoặc một phần của thông điệp, một tính năng hữu ích khi người dùng kết nối đến server bằng đường truyền tốc độ chậm như điện thoại nhưng lại đọc các email có âm thanh, hình ảnh…Với quan niệm cho rằng người dùng không cần tải thư về lưu trên PC, IMAP cung cấp các cơ chế cho phép tạo, xóa và sửa đổi nhiều hộp thư trên server.

Cung cách làm việc của IMAP cũng giống như POP3, ngoài trừ trong IMAP có rất nhiều lệnh. IMAP server sẽ lắng nghe trên cổng 143. Cũng nên chú ý rằng, không phải mọi ISP đều hỗ trợ cả hai giao thức POP3 và IMAP.
Bảng sau so sánh các tính năng của POP3 và IMAP

Tính năng	POP3	IMAP
Giao thức được định nghĩa ở đâu?	RFC 1939	RFC 2060
Cổng TCP được dùng	110	143

Email được lưu ở đâu	PC của người dùng	Server
Email được đọc ở đâu	Off-line	On-line
Thời gian nối kết	Ít	Nhiều
Sử dụng tài nguyên của server	Tối thiểu	Nhiều hơn
Nhiều hộp thư	Không	Đúng
Ai lưu phòng hờ các hộp thư	Người dùng	ISP
Tốt cho người dùng di động	Không	Có
Kiểm soát của người dùng đối với việc tải thư về	Ít	Tốt
Tải một phần thư	Không	Có
Quota đĩa có là vấn đề không?	Không	Thỉnh thoảng
Dễ cài đặt	Có	Không
Được hỗ trợ rộng rãi	Có	Đang phát triển

6.3 WORLD WIDE WEB (HTTP- Hyper Text Transfer Protocol)

Ứng dụng Web đã rất thành công, giúp cho nhiều người có thể truy cập Internet đến nỗi Web được hiểu đồng nghĩa với Internet!. Có thể hiểu Web như là một tập các client và server hợp tác với nhau và cùng nói chung một ngôn ngữ: HTTP (Hyper Text Transfer Protocol). Đa phần người dùng tiếp xúc với Web thông qua chương trình client có giao diện đồ họa, hay còn gọi là trình duyệt Web (Web browser). Các trình duyệt Web thường được sử dụng nhất là Netscape Navigator (của Netscape) và Internet Explorer (của Microsoft). Hình 6.8 thể hiện trình duyệt Explorer đang trình bày trang chủ của Trường Đại Học SPKT Vĩnh Long:

Hình 6.8 Trình duyệt Web Internet Explorer

Bất kỳ trình duyệt Web nào cũng có chức năng cho phép người dùng "mở một URL". Các URL (Uniform Resource Locators) cung cấp thông tin về vị trí của các đối tượng trên Internet; chúng thường trông giống như sau:
http://www.vlute.edu.vn/index.html

Nếu người dùng mở URL trên, trình duyệt Web sẽ thiết lập một kết nối TCP đến Web Server tại địa chỉ **www.vlute.edu.vn** và ngay lập tức tải tập tin **index.html** về và thể hiện nó. Hầu hết các tập tin trên Web chứa văn bản và hình ảnh, một số còn chứa audio và video clips. Chúng còn có thể chứa các liên kết đến các tập tin khác – được gọi là các liên kết siêu văn bản (hypertext links). Khi người dùng yêu cầu trình duyệt Web mở ra một liên kết siêu văn bản (bằng cách trỏ chuột và click lên liên kết đó), trình duyệt sẽ mở một nối kết mới, tải về và hiển thị một tập tin mới. Vì thế, rất dễ để duyệt từ server này đến server khác trên khắp thế giới để có được hết những thông tin mà người dùng cần.

Khi người dùng chọn xem một trang Web, trình duyệt Web sẽ nạp trang Web đó từ Web server về sử dụng giao thức HTTP chạy trên TCP. Giống như SMTP, HTTP là giao thức hướng ký tự. Về cốt lõi, một thông điệp HTTP có khuôn dạng tổng quát sau:

START_LINE <CRLF>
MESSAGE_HEADER <CRLF>
<CRLF>
MESSAGE_BODY <CRLF>

Hàng đầu tiên chỉ ra đấy là thông điệp yêu cầu hay trả lời. Nó sẽ chỉ ra "thủ tục cần được thực hiện từ xa" (trong tình huống là thông điệp yêu cầu) hoặc là "trạng thái trả về" (trong tình huống là thông điệp trả lời). Tập hợp các hàng kế tiếp chỉ ra các tùy chọn hoặc tham số nhằm xác định cụ thể tính chất của yêu cầu hoặc trả lời. Phần MESSAGE_HEADER có thể không có hoặc có một vài hàng tham số và được kết thúc bằng một hàng trống. HTTP định nghĩa nhiều kiểu header, một số liên quan đến các thông điệp yêu cầu, một số liên quan đến các thông điệp trả lời và một số lại liên quan đến phần dữ liệu trong thông điệp. Ở đây chỉ giới thiệu một số kiểu thường dùng. Cuối cùng, sau hàng trống là phần nội dung của thông điệp trả lời (MESSAGE_BODY), phần này thường là rỗng trong thông điệp yêu cầu.

6.3.1 Các thông điệp yêu cầu

Hàng đầu tiên của một thông điệp yêu cầu HTTP sẽ chỉ ra 3 thứ: thao tác cần được thực thi, trang Web mà thao tác đó sẽ áp lên và phiên bản HTTP được sử dụng. Bảng sau sẽ giới thiệu một số thao tác phổ biến.

Hành động	Mô tả
OPTIONS	Yêu cầu thông tin về các tùy chọn hiện có.
GET	Lấy về tài liệu được xác định trong URL
HEAD	Lấy về thông tin thô về tài liệu được xác định trong URL
POST	Cung cấp thông tin cho server
PUT	Tải tài liệu lên server và đặt ở vị trí được xác định trong URL
DELETE	Xóa tài liệu nằm ở vị trí URL trên server
TRACE	Phản hồi lại thông điệp yêu cầu

CONNECT	Được sử dụng bởi các proxy

Hai thao tác thường được sử dụng nhiều nhất là GET (lấy một trang Web về) và HEAD (lấy về thông tin của một trang Web). GET thường được sử dụng khi trình duyệt muốn tải một trang Web về và hiển thị nó cho người dùng. HEAD thường được sử dụng để kiểm tra tính hợp lệ của một liên kết siêu văn bản hoặc để xem một trang nào đó có bị thay đổi gì không kể từ lần tải về trước đó.

Ví dụ, dòng START_LINE GET http://www.vlute.edu.vn/index.html HTTP/1.1 nói rằng: người dùng muốn tải về trên server www.vlute.edu.vn trang Web có tên index.html và hiển thị nó. Ví dụ trên dùng URL tuyệt đối. Ta cũng có thể sử dụng URL tương đối như sau:

GET /index.html HTTP/1.1
Host: www.vlute.edu.vn

Ở đây, Host là một trong các trường trong MESSAGE_HEADER.

6.3.2 Các thông điệp trả lời

Giống như các thông điệp yêu cầu, các thông điệp trả lời bắt đầu bằng một hàng START_LINE. Trong trường hợp này, dòng START_LINE sẽ chỉ ra phiên bản HTTP đang được sử dụng, một mã 3 ký số xác định yêu cầu là thành công hay thất bại và một chuỗi ký tự chỉ ra lý do của câu trả lời này.

Ví dụ: dòng START_LINEHTTP/1.1 202 Accepted chỉ ra server đã có thể thõa mãn yêu cầu của người dùng. Còn dòngHTTP/1.1 404 Not Found chỉ ra rằng server đã không thể tìm thấy tài liệu như được yêu cầu. Có năm loại mã trả lời tổng quát với ký số đầu tiên xác định loại mã.

Mã	Loại	Lý do
1xx	Thông tin	Đã nhận được yêu cầu, đang tiếp tục xử lý
2xx	Thành công	Thao tác đã được tiếp nhận, hiểu được và chấp nhận được
3xx	Chuyển hướng	Cần thực hiện thêm thao tác để hoàn tất yêu cầu được đặt ra
4xx	Lỗi client	Yêu cầu có cú pháp sai hoặc không thể được đáp ứng
5xx	Lỗi server	Server thất bại trong việc đáp ứng một yêu cầu hợp lệ

Cũng giống như các thông điệp yêu cầu, các thông điệp trả lời có thể chứa một hoặc nhiều dòng trong phần MESSAGE_HEADER. Những dòng này cung cấp thêm thông tin cho client. Ví dụ, dòng header Locationchỉ ra rằng URL được yêu cầu đang có ở vị trí khác. Vì thế, nếu trang Web của Khoa Công Nghệ Thông Tin được di chuyển từ địa chỉ http://www.fit.vlute.edu.vn/index.html sang địa chỉ
http://www.vlute.edu.vn/cit/index.htmlmà người dùng lại truy cập vào URL cũ, thì Web server sẽ trả lời như sau
HTTP/1.1 301 Moved Permanently
Location: http://www.vlute.edu.vn/cit/index.html

Trong tình huống chung nhất, thông điệp trả lời cũng sẽ mang theo nội dung trang Web được yêu cầu. Trang này là một tài liệu HTML, nhưng vì nó có thể chứa dữ liệu không phải dạng văn bản (ví dụ như ảnh GIF), dữ liệu này có thể được mã hóa theo dạng MIME. Một số hàng trong phần MESSAGE_HEADER cung cấp thêm thông tin

về nội dung của trang Web, bao gồm ContentLength(số bytes trong phần nội dung), Expires(thời điểm mà nội dung trang Web được xem như lỗi thời), và Last-Modified(thời điểm được sửa đổi lần cuối cùng).

6.3.3 Các kết nối TCP

Nguyên tắc chung của giao thức HTTP là client nối kết đến cổng TCP số 80 tại server, server luôn lắng nghe trên cổng này để sẵn sàng phục vụ client. Phiên bản đầu tiên (HTTP/1.0) sẽ thiết lập một nối kết riêng cho mỗi hạng mục dữ liệu cần tải về từ server. Không khó để thấy rằng đây là cơ chế không mấy hiệu quả: Các thông điệp dùng để thiết lập và giải phóng nối kết sẽ phải được trao đổi qua lại giữa client và server và khi mà tất cả client muốn lấy thông tin mới nhất của một trang Web, server sẽ bị quá tải.

Cải tiến quan trọng nhất trong phiên bản HTTP/1.1 là nó cho phép các kết nối lâu dài – client và server sẽ trao đổi nhiều thông điệp yêu cầu/trả lời trên cùng một kết nối TCP. Kết nối lâu dài có hai cái lợi. Thứ nhất, nó làm giảm thiểu chi phí cho việc thiết lập/giải phóng nối kết. Thứ hai, do client gởi nhiều thông điệp yêu cầu qua một kết nối TCP, cơ chế điều khiển tắc nghẽn của TCP sẽ hoạt động hiệu quả hơn.

Tuy nhiên, kết nối lâu dài cũng có cái giá phải trả. Vấn đề phát sinh ở chỗ: không ai trong client và server biết được kết nối đó sẽ kéo dài bao lâu. Điều này thực sự gây khó khăn cho phía server bởi vì tại mỗi thời điểm, nó phải đảm bảo duy trì kết nối đến cả ngàn client. Giải pháp cho vấn đề này là: server sẽ mãn kỳ và cắt nối kết nếu nó không nhận được một yêu cầu cụ thể nào từ phía client trong một khoảng thời gian định trước. Ngoài ra, cả client và server phải theo dõi xem phía bên kia có chủ động cắt nối kết hay không và lấy đó làm cơ sở để tự cắt nối kết của mình. (Nhắc lại rằng, cả hai bên phải cắt nối kết thì nối kết TCP mới thực sự kết thúc).

6.3.4 Trữ đệm

Một trong những lĩnh vực nghiên cứu tích cực nhất hiện nay về Internet là làm sao để trữ tạm các trang Web một cách hiệu quả. Việc trữ tạm mang lại nhiều lợi ích. Từ phía client, việc nạp và hiển thị một trang Web từ bộ đệm gần đấy là nhanh hơn rất nhiều so với từ một server nào đó ở nửa vòng trái đất. Đối với server, có thêm một bộ đệm để can thiệp vào và phục vụ giúp yêu cầu của người dùng sẽ giảm bớt tải trên server.

Việc trữ đệm có thể được cài đặt tại nhiều nơi khác khau. Ví dụ, trình duyệt Web có thể trữ tạm những trang Web mới được nạp về gần đây, để khi người dùng duyệt lại những trang Web đó, trình duyệt sẽ không phải nối kết ra Internet để lấy chúng về mà dùng bản trữ sẵn. Ví dụ khác, một khu vực làm việc (site) có thể đề cử một máy làm nhiệm vụ trữ tạm các trang Web, để những người dùng sau có thể sử dụng các bản trữ sẵn của những người dùng trước. Yêu cầu của hệ thống này là mọi người dùng trong site phải biết địa chỉ của máy tính làm nhiệm vụ bộ trữ tạm, và họ chỉ đơn giản là liên hệ với máy tính này để tải các trang Web về theo yêu cầu. Người ta thường gọi máy tính làm nhiệm vụ trữ tạm các trang Web cho một site là *proxy*. Vị trí trữ đệm có thể di chuyển gần hơn đến phần lõi của Internet là các ISP. Trong tình huống này, các site nối kết tới ISP thường không hay biết gì về việc trữ tạm ở đây. Khi các yêu cầu HTTP từ các site được chuyển phát đến router của ISP, router liền kiểm tra xem URL được yêu cầu có giống với các URL được trữ sẵn hay không. Nếu có, router sẽ trả lời ngay. Nếu

không, router sẽ chuyển yêu cầu đến server thật sự và cũng không quên lưu vào bộ đệm của mình thông điệp trả lời từ phía server đó.

Việc trữ tạm là đơn giản. Tuy nhiên bộ đệm phải đảm bảo những thông tin trữ đệm trong đó không quá cũ. Để làm được việc này, các Web server phải gán "ngày hết hạn" (tức là trường Expirestrong header) cho mọi trang Web mà nó phục vụ cho client. Nhân đó, các bộ đệm cũng lưu lại thông tin này. Và từ đó, các bộ đệm sẽ không cần phải kiểm tra tính cập nhật của trang Web đó cho đến khi ngày hết hạn đến. Tại thời điểm một trang Web hết hạn, bộ đệm sẽ dùng lệnh HEAD hoặc lệnh GET có điều kiện (GET với trường If-Modified-Sincetrong phần header được đặt) để kiểm tra rằng nó có một phiên bản mới nhất của trang Web kia. Tổng quát hơn, cần phải có "các chỉ thị hướng dẫn" cho việc trữ đệm và các chỉ thị này phải được tuân thủ tại mọi bộ đệm. Các chỉ thị sẽ chỉ ra có nên trữ đệm một tài liệu hay không, trữ nó bao lâu, một tài liệu phải tươi như thế nào và vân vân.

6.4 TRUYỀN TẬP TIN (FTP- File Transfer Protocol)

Thông qua dịch vụ FTP, người dùng tại một máy tính có thể đăng nhập và thao tác lên hệ thống tập tin được chia sẻ của một máy tính từ xa.

Mục tiêu của dịch vụ FTP là:

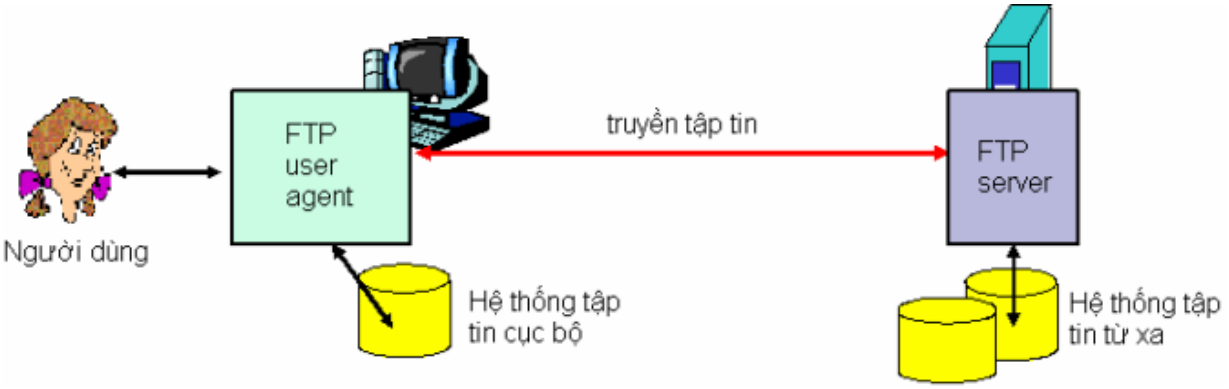
1) Đảm bảo việc chia sẻ tập tin (chương trình máy tính hoặc dữ liệu) trên mạng.

2) Khuyến khích việc sử dụng không trực tiếp (thông qua chương trình) tài nguyên trên các máy tính khác.

3) Người dùng không cần phải quan tâm đến sự khác nhau của các hệ thống tập tin trên mạng.

4) Truyền dữ liệu một cách tin cậy và hiệu quả.

6.4.1 Mô hình dịch vụ FTP



Hình 6.9 Mô hình dịch vụ FTP

Trong hệ thống này, người dùng sẽ ra lệnh cho FTP user agent. User agent sẽ nối kết tới FTP server để dàn xếp thủ tục làm việc, thực thi các tác vụ theo yêu cầu và trả kết quả về cho người dùng.

6.4.2 Quá trình làm việc FTP

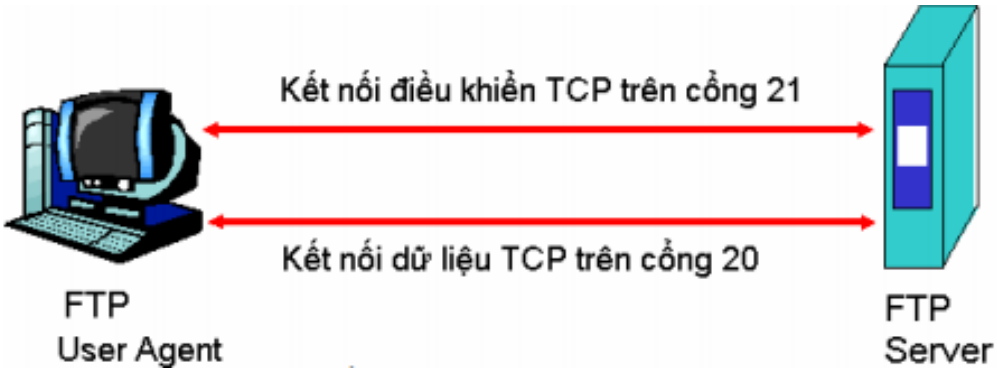
1) Truy nhập vào mạng TCP/IP từ máy trạm
2) Gõ lệnh: *ftp <Địa chỉ máy server>*
3) Làm việc với FTP

Khi một kết nối FTP được thiết lập, thực hiện các bước như sau:

- Duyệt tên và mật khẩu (ID) của người dùng
- Xác định thư mục bắt đầu làm việc
- Định nghĩa chế độ truyền tập tin
- Cho phép các lệnh của người dùng
- Hủy kết nối

6.4.3 Giao thức FTP

Đầu tiên, user agent thiết lập một kết nối điều khiển trên cổng 21 tới FTP server. Sau khi đã thỏa thuận các tham số truyền nhận, hai bên sẽ thiết lập một kênh dữ liệu chạy trên cổng 20. Dữ liệu của các tập tin được trao đổi qua lại giữa user agent và server sẽ chạy trên kênh dữ liệu này. Kênh dữ liệu là kênh hoạt động theo phương thức hai chiều và không nhất thiết phải luôn tồn tại.



Hình 6.10 Giao tiếp giữa Client và Server trong giao thức FTP

6.4.4 Các lệnh cơ bản

Sau đây là các lệnh cơ bản mà người dùng có thể sử dụng để thao tác lên hệ thống FTP

Lệnh FTP	Mô tả
FTP*host_name*	Nối kết đến FTP server có địa chỉ host-name
USER*user_name*	Cung cấp tên người dùng cho FTP server để thực hiện quá trình chứng thực
ascii	Chuyển sang chế độ truyền ACSII
bell	Âm thanh của chương trình sau khi truyền mỗi tập tin
binary	Chuyển sang chế độ truyền nhị phân
cd *dirctory*	Chuyển đổi thư mục hiện hành trên server
cdup	Lùi thư mục hiện hành về một cấp trước đó
close	Hủy kết nối
delete *filename*	Xóa một tập tin trên server
dir *directory*	Hiển thị thư mục directory của server
get *filename*	Truyền tập tin trên server về máy cục bộ
hash	Hiển thị/làm mất dấu # cho mỗi khối các ký tự đã truyền được

help	Hiển thị các trợ giúp
lcd *directory*	Chuyển đổi thư mục hiện hành trên máy cục bộ
ls *directory*	Xem danh sách các tập tin trong thư mục dicrectory trên server
mdelete *files*	Xóa nhiều tập tin trên máy server
mdir *directory*	Liệt kê các tập tin trong thư mục hiện hành của máy cục bộ
mget *files*	Lấy một số file trên server về thư mục hiện hành của máy tính cục bộ
mkdir *directory*	Tạo thư mục dirctory trên máy server
mput *files*	Gửi một số tập tin từ máy cục bộ lên máy Server
open *host*	Kết nối với server host từ xa
put *filename*	Truyền tập tin từ máy cục bộ lên máy server
pwd	Hiển thị thư mục hiện thời của server
status	Hiển thị trạng thái của FTP
rename *file1file2*	Đổi tên file1 trên Server thành file2
quote	Cung cấp một lệnh FTP một cách trực tiếp
quit	Chấm dứt kết nối và thoát khỏi FTP
?	Hiển thị danh sách lệnh

Để truyền một tập tin từ thư mục hiện hành trên máy Client đến máy Server dùng lệnh put, ngược lại muốn tải tập tin từ máy server về client, bạn dùng lệnh *get*.

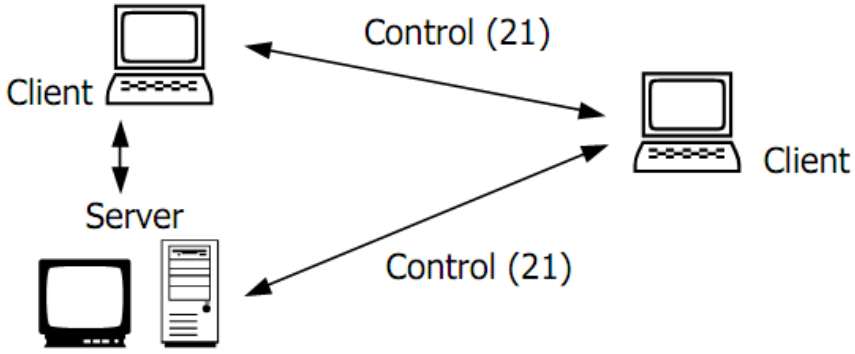
Cú pháp như sau:

ftp>put local_file remote_file

ftp>get remote_file local_file

Khi truy cập vào hệ thống nếu chưa có account, người sử dụng có thể sử dụng một name đặc biệt là *anonymous* để truy cập vào hệ thống. Acount này không có một khẩu.

FTP cho phép truyền các tập tin thông qua máy thứ 3, máy này nằm giữa client và server. Thủ tục nay được gọi là truyền tay ba điều này cần thiết để có được sự cho phép chính xác để truy cập vào máy ở xa. Hình sau mô tả thủ tục này.



Hình 6.11 Truyền các tập tin thông qua máy thứ 3

6.5 DỊCH VỤ TELNET

6.5.1 Căn bản về TELNET

Telnet là một ứng dụng cho phép người dùng ngồi trên một thiết bị đầu cuối có thể thông qua kết nối mạng đến một thiết bị từ xa để điều khiển nó bằng câu lệnh như là đang ngồi tại máy ở xa. Một máy trạm có thể thực hiện đồng thời nhiều phiên telnet đến nhiều địa chỉ IP khác nhau. Đồng thời đối với cùng một host đích ở xa, có thể telnet đến các cổng khác nhau (ví dụ cổng 80 của web; cổng 20, 21 của FTP).

6.5.2 Hoạt động của TELNET

Telnet hoạt động theo phiên, mỗi phiên là một kết nối truyền dữ liệu theo giao thức TCP với cổng 23.

Telnet hoạt động theo mô hình client server trong đó client là một phần mềm chạy trên máy trạm tại chỗ mà người dùng sử dụng, phần mềm này sẽ cung cấp giao diện hiển thị để người dùng gõ lệnh điều khiển.

Phần server là dịch vụ chạy trên máy từ xa lắng nghe và xử lý các kết nối và câu lệnh được gửi đến từ máy trạm tại chỗ.

Câu lệnh ở máy trạm tại chỗ (terminal) sẽ được đóng gói bằng giao thức TCP và truyền đến địa chỉ IP của máy ở xa. Máy ở xa sẽ bóc tách gói tin đó và đọc ra câu lệnh để thực hiện. Kết quả trả về sẽ được máy từ xa đóng gói lại và gửi cho máy tại chỗ. Các câu lệnh điều khiển từ xa của telnet do vậy sẽ được đóng gói và truyền song song với dữ liệu trên một mạng máy tính. Các gói tin của telnet do đó cũng được định tuyến như các gói dữ liệu để đến được máy đích và ngược lại.

Đường truyền của telnet là fullduplex, cho phép cả client và server có thể truyền dữ liệu đồng thời.

Telnet cho phép kết nối và điều khiển nhiều thiết bị của các hãng khác nhau, thậm chí chạy các hệ điều hành khác nhau chỉ cần giữa 2 máy đó có một kết nối IP thông suốt. Để có kết nối IP đó các máy phải trong cùng một mạng hoặc ở các mạng khác nhau nhưng có thể định tuyến đến nhau được. Các thiết bị lớp 3 (router, switch layer 3 hoặc gateway sẽ xây dựng tuyến đường giữa 2 thiết bị) trên đó, câu lệnh sẽ được đóng gói và gửi một cách tin cậy bằng giao thức TCP.

Số câu lệnh telnet có thể thực hiện được phụ thuộc vào dịch vụ được máy từ xa cung cấp. Dịch vụ telnet của router Cisco cho phép máy trạm tại chỗ có thể nhập vào và gửi đi tất cả các câu lệnh như khi cấu hình trực tiếp trên router. Một số thiết bị khác và hệ điều hành khác thì chỉ cho phép thực hiện các câu lệnh giới hạn mà thôi.

6.5.3 Các bước thực hiện phiên TELNET

Ta có thể bật các dịch vụ telnet trên các thiết bị khác nhau (PC, router, switch, modem, gateway…) của các hãng sản xuất khác nhau (Microsoft, Cisco, Zoom…). Phần này tìm hiểu các bật dịch vụ telnet cho router của Cisco

6.5.4 Các bước để bật dịch vụ TELNET trong router

1. Truy cập vào router (bằng đường console hoặc telnet), sau khi truy cập thành công, dấu nhắc dòng lệnh trên router sẽ hiện ra như sau:

   Router>

2. Vào mức previlidge

Router>enable
Router#

3. Vào mức cấu hình global (config global)

Router#config terminal

4. Vào mức cấu hình telnet

Router(config)#line vty 0 4

0 và 4 là số hiệu phiên telnet, như vậy bằng câu lệnh này có thể thực hiện 5 phiên telnet vào router với số hiệu từ phiên 0 đến phiên 4.

5. Trong mức cấu hình telnet, đặt password cho truy cập

Router(config-line)#password cisco
Router(config-line)#login

Ở máy trạm tại chỗ phải có phần mềm telnet client. Đơn giản nhất là sử dụng câu lệnh telnet của dòng lệnh cmd trong windows.

Ví dụ: telnet 192.168.1.250 sẽ thiết lập phiên telnet với thiết bị có địa chỉ IP là 192.168.1.250.

Một số phần mềm telnet khác là Hyper terminal, SecureCRT. Việc cài đặt rất đơn giản, các thông số nhập vào trong một phiên telnet thường chỉ là địa chỉ IP và số port.

6.6 DỊCH VỤ GOPHER

Trước khi Web ra đời Gopher là dịch vụ rất được ưa chuộng. Gopher là một dịch vụ chuyển tệp tương tự như FTP, nhưng nó hỗ trợ người dùng trong việc cung cấp thông tin về tài nguyên. Client Gopher hiển thị một thực đơn, người dùng chỉ việc lựa chọn cái mà mình cần. Kết quả của việc lựa chọn được thể hiện ở một thực đơn khác.

Gopher bị giới hạn trong kiểu dữ liệu. Nó chỉ hiển thị dữ liệu dưới dạng mã ASCII mặc dù có thể chuyển dữ liệu dạng nhị phân và hiển thị nó bằng một phần mềm khác.

6.7 DỊCH VỤ WAIS

WAIS (Wide Area Information Serves) là một dịch vụ tìm kiếm dữ liệu. WAIS thường xuyên bắt đầu việc tìm kiếm dữ liệu tại thư mục của máy chủ, nơi chứa toàn bộ danh mục của các máy phục vụ khác. Sau đó WAIS thực hiện tìm kiếm tại máy phục vụ thích hợp nhất. WAIS có thể thực hiện công việc của mình với nhiều loại dữ liệu khác nhau như văn bản ASCII, PostScript, GIF, TIFF, điện thư …

TỔNG KẾT CHƯƠNG

Các điểm quan trọng bạn cần nắm trong chương này:

1. Khảo sát cấu trúc và hoạt động của dịch vụ DNS.
2. Khảo sát cấu trúc và hoạt động của giao thức SNMP.
3. Khảo sát cấu trúc và hoạt động của giao thức HTTP.
4. Đặc điểm của các dịch vụ mạng.
5. Tìm hiểu giao thức DHCP.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Thúc Hải (1997), ***Mạng máy tính và các hệ thống mở***, NXB Giáo dục.

[2] Lê Văn Sơn (1998), ***Giáo trình Mạng máy tính***, Trường ĐH Bách Khoa Đà Nẵng.

[3] Ngô Bá Hùng – Phạm Thế Phi (2005), ***Giáo trình Mạng máy tính***, Trường Đại học Cần Thơ.

[4] Nguyễn Hồng Sơn (2002), ***Giáo trình hệ thống mạng máy tính CCNA***, Nhà xuất bản Lao Động.

[5] Stallings w.(1995), ***Data and computer communications***, Macmillan Publishing.

[6] Tanenbaum Andrew S., ***Computer Network***, Prentice Hall.

[7] Ed Taylor, ***TCP/IP complete***, McGraw-Hill.

[8] Pujolle (2003), ***Les rDseaux***, Eyrolles.

MỤC LỤC