Chương 1

Tổng quan về thiết kế và cài đặt mạng

Mục đích

Chương này nhằm giới thiệu cho người đọc những vấn đề sau :

- Các bước cần phải thực hiện để xây dựng một mạng máy tính và các vấn đề liên quan
- Nhắc lại mô hình OSI

1.1 Tiến trình xây dựng mạng

Ngày nay, mạng máy tính đã trở thành một hạ tầng cơ sở quan trọng của tất cả các cơ quan xí nghiệp. Nó đã trở thành một kênh trao đổi thông tin không thể thiếu được trong thời đại công nghệ thông tin. Với xu thế giá thành ngày càng hạ của các thiết bị điện tử, kinh phí đầu tư cho việc xây dựng một hệ thống mạng không vượt ra ngoài khả năng của các công ty xí nghiệp. Tuy nhiên, việc khai thác một hệ thống mạng một cách hiệu quả để hỗ trợ cho công tác nghiệp vụ của các cơ quan xí nghiệp thì còn nhiều vấn đề cần bàn luận. Hầu hết người ta chỉ chú trọng đến việc mua phần cứng mạng mà không quan tâm đến yêu cầu khai thác sử dụng mạng về sau. Điều này có thể dẫn đến hai trường hợp: lãng phí trong đầu tư hoặc mạng không đáp ứng đủ cho nhu cầu sử dụng.

Có thể tránh được điều này nếu ta có kế hoạch xây dựng và khai thác mạng một cách rõ ràng. Thực tế, tiến trình xây dựng mạng cũng trải qua các giai đoạn như việc xây dựng và phát triển một phần mềm. Nó cũng gồm các giai đoạn như: Thu thập yêu cầu của khách hàng (công ty, xí nghiệp có yêu cầu xây dựng mạng), Phân tích yêu cầu, Thiết kế giải pháp mạng, Cài đặt mạng, Kiểm thử và cuối cùng là Bảo trì mạng.

Phần này sẽ giới thiệu sơ lược về nhiệm vụ của từng giai đoạn để ta có thể hình dung được tất cả các vấn đề có liên quan trong tiến trình xây dựng mạng.

1.1.1 Thu thập yêu cầu của khách hàng

Mục đích của giai đoạn này là nhằm xác định mong muốn của khách hàng trên mạng mà chúng ta sắp xây dựng. Những câu hỏi cần được trả lời trong giai đoạn này là:

- Bạn thiết lập mạng để làm gì? sử dụng nó cho mục đích gì?
- Các máy tính nào sẽ được nối mạng?
- Những người nào sẽ được sử dụng mạng, mức độ khai thác sử dụng mạng của từng người / nhóm người ra sao?
- Trong vòng 3-5 năm tới bạn có nối thêm máy tính vào mạng không, nếu có ở đâu, số lượng bao nhiêu ?

Phương pháp thực hiện của giai đoạn này là bạn phải phỏng vấn khách hàng, nhân viên các phòng mạng có máy tính sẽ nối mạng. Thông thường các đối tượng mà bạn phỏng vấn không có chuyên môn sâu hoặc không có chuyên môn về mạng. Cho nên bạn nên tránh sử dụng những thuật ngữ chuyên môn để trao đổi với họ. Chẳng hạn nên hỏi khách hàng " Bạn có muốn người trong cơ quan bạn gởi mail được cho nhau không?", hơn là hỏi " Bạn có muốn cài đặt Mail server cho mạng không? ". Những câu trả lời của khách hàng thường không có cấu trúc, rất lộn xộn, nó xuất phát từ góc nhìn của người sử dụng, không phải là góc nhìn của kỹ sư mạng. Người thực hiện phỏng vấn phải có kỹ năng và kinh nghiệm trong lĩnh vực này. Phải biết cách đặt câu hỏi và tổng hợp thông tin.

Một công việc cũng hết sức quan trọng trong giai đoạn này là "Quan sát thực địa" để xác định những nơi mạng sẽ đi qua, khoảng cách xa nhất giữa hai máy tính trong mạng, dự kiến đường đi của dây mạng, quan sát hiện trạng công trình kiến trúc nơi mạng sẽ đi qua. Thực địa đóng vai trò quan trọng trong việc chọn công nghệ và ảnh hưởng lớn đến chi phí mạng. Chú ý đến ràng buộc về mặt thẩm mỹ cho các công trình kiến trúc khi chúng ta triển khai đường dây mạng bên trong nó. Giải pháp để nối kết mạng cho 2 tòa nhà tách rời nhau bằng một khoảng không phải đặc biệt lưu ý. Sau khi khảo sát thực địa, cần vẽ lại thực

địa hoặc yêu cầu khách hàng cung cấp cho chúng ta sơ đồ thiết kế của công trình kiến trúc mà mạng đi qua.

Trong quá trình phỏng vấn và khảo sát thực địa, đồng thời ta cũng cần tìm hiểu yêu cầu trao đổi thông tin giữa các phòng ban, bộ phận trong cơ quan khách hàng, mức độ thường xuyên và lượng thông tin trao đổi. Điều này giúp ích ta trong việc chọn băng thông cần thiết cho các nhánh mạng sau này.

1.1.2 Phân tích yêu cầu

Khi đã có được yêu cầu của khách hàng, bước kế tiếp là ta đi phân tích yêu cầu để xây dựng bảng "Đặc tả yêu cầu hệ thống mạng", trong đó xác định rõ những vấn đề sau:

- Những dịch vụ mạng nào cần phải có trên mạng ? (Dịch vụ chia sẻ tập tin, chia sẻ máy in, Dịch vụ web, Dịch vụ thư điện tử, Truy cập Internet hay không?, ...)
- Mô hình mạng là gì? (Workgoup hay Client / Server? ...)
- Mức độ yêu cầu an toàn mạng.
- Ràng buộc về băng thông tối thiểu trên mạng.

1.1.3 Thiết kế giải pháp

Bước kế tiếp trong tiến trình xây dựng mạng là thiết kế giải pháp để thỏa mãn những yêu cầu đặt ra trong bảng Đặc tả yêu cầu hệ thống mạng. Việc chọn lựa giải pháp cho một hệ thống mạng phụ thuộc vào nhiều yếu tố, có thể liệt kê như sau:

- Kinh phí dành cho hệ thống mạng.
- Công nghệ phổ biến trên thị trường.
- Thói quen về công nghệ của khách hàng.
- Yêu cầu về tính ổn định và băng thông của hệ thống mạng.
- Ràng buộc về pháp lý.

Tùy thuộc vào mỗi khách hàng cụ thể mà thứ tự ưu tiên, sự chi phối của các yếu tố sẽ khác nhau dẫn đến giải pháp thiết kế sẽ khác nhau. Tuy nhiên các công việc mà giai đoạn thiết kế phải làm thì giống nhau. Chúng được mô tả như sau:

1.1.3.1 Thiết kế sơ đồ mạng ở mức luận lý

Thiết kế sơ đồ mạng ở mức luận lý liên quan đến việc chọn lựa mô hình mạng, giao thức mạng và thiết đặt các cấu hình cho các thành phần nhận dạng mạng.

Mô hình mạng được chọn phải hỗ trợ được tất cả các dịch vụ đã được mô tả trong bảng Đặc tả yêu cầu hệ thống mạng. Mô hình mạng có thể chọn là Workgroup hay Domain (Client / Server) đi kèm với giao thức TCP/IP, NETBEUI hay IPX/SPX.

Ví dụ:

- Một hệ thống mạng chỉ cần có dịch vụ chia sẻ máy in và thư mục giữa những người dùng trong mạng cục bộ và không đặt nặng vấn đề an toàn mạng thì ta có thể chọn Mô hình Workgroup.
- Một hệ thống mạng chỉ cần có dịch vụ chia sẻ máy in và thư mục giữa những người dùng trong mạng cục bộ nhưng có yêu cầu quản lý người dùng trên mạng thì phải chọn Mô hình Domain.

- Nếu hai mạng trên cần có dịch vụ mail hoặc kích thước mạng được mở rộng, số lượng máy tính trong mạng lớn thì cần lưu ý thêm về giao thức sử dụng cho mạng phải là TCP/IP.

Mỗi mô hình mạng có yêu cầu thiết đặt cấu hình riêng. Những vấn đề chung nhất khi thiết đặt cấu hình cho mô hình mạng là:

- Định vị các thành phần nhận dạng mạng, bao gồm việc đặt tên cho Domain, Workgroup, máy tính, định địa chỉ IP cho các máy, định cổng cho từng dịch vụ.
- Phân chia mạng con, thực hiện vạch đường đi cho thông tin trên mạng.

1.1.3.2 Xây dựng chiến lược khai thác và quản lý tài nguyên mạng

Chiến lược này nhằm xác định ai được quyền làm gì trên hệ thống mạng. Thông thường, người dùng trong mạng được nhóm lại thành từng nhóm và việc phân quyền được thực hiện trên các nhóm người dùng.

1.1.3.3 Thiết kế sơ đồ mạng ở vật lý

Căn cứ vào sơ đồ thiết kế mạng ở mức luận lý, kết hợp với kết quả khảo sát thực địa bước kế tiếp ta tiến hành thiết kế mạng ở mức vật lý. Sơ đồ mạng ở mức vật lý mô tả chi tiết về vị trí đi dây mạng ở thực địa, vị trí của các thiết bị nối kết mạng như Hub, Switch, Router, vị trí các máy chủ và các máy trạm. Từ đó đưa ra được một bảng dự trù các thiết bị mạng cần mua. Trong đó mỗi thiết bị cần nêu rõ: Tên thiết bị, thông số kỹ thuật, đơn vị tính, đơn giá,…

1.1.3.4 Chọn hệ điều hành mạng và các phần mềm ứng dụng

Một mô hình mạng có thể được cài đặt dưới nhiều hệ điều hành khác nhau. Chẳng hạn với mô hình Domain, ta có nhiều lựa chọn như: Windows NT, Windows 2000, Netware, Unix, Linux,... Tương tự, các giao thức thông dụng như TCP/IP, NETBEUI, IPX/SPX cũng được hỗ trợ trong hầu hết các hệ điều hành. Chính vì thế ta có một phạm vi chọn lựa rất lớn. Quyết định chọn lựa hệ điều hành mạng thông thường dựa vào các yếu tố như:

- Giá thành phần mềm của giải pháp.
- Sự quen thuộc của khách hàng đối với phần mềm.
- Sự quen thuộc của người xây dựng mạng đối với phần mềm.

Hệ điều hành là nền tảng để cho các phần mềm sau đó vận hành trên nó. Giá thành phần mềm của giải pháp không phải chỉ có giá thành của hệ điều hành được chọn mà nó còn bao gồm cả giá thành của các phầm mềm ứng dụng chạy trên nó. Hiện nay có 2 xu hướng chọn lựa hệ điều hành mạng: các hệ điều hành mạng của Microsoft Windows hoặc các phiên bản của Linux.

Sau khi đã chọn hệ điều hành mạng, bước kế tiếp là tiến hành chọn các phần mềm ứng dụng cho từng dịch vụ. Các phần mềm này phải tương thích với hệ điều hành đã chọn.

1.1.4 Cài đặt mạng

Khi bản thiết kế đã được thẩm định, bước kế tiếp là tiến hành lắp đặt phần cứng và cài đặt phần mềm mạng theo thiết kế.

1.1.4.1 Lắp đặt phần cứng

Cài đặt phần cứng liên quan đến việc đi dây mạng và lắp đặt các thiết bị nối kết mạng (Hub, Switch, Router) vào đúng vị trí như trong thiết kế mạng ở mức vật lý đã mô tả.

1.1.4.2 Cài đặt và cấu hình phần mềm

Tiến trình cài đặt phần mềm bao gồm:

- Cài đặt hệ điều hành mạng cho các server, các máy trạm
- Cài đặt và cấu hình các dịch vụ mạng.
- Tạo người dùng, phân quyền sử dụng mạng cho người dùng.

Tiến trình cài đặt và cấu hình phần mềm phải tuân thủ theo sơ đồ thiết kế mạng mức luận lý đã mô tả. Việc phân quyền cho người dùng pheo theo đúng chiến lược khai thác và quản lý tài nguyên mạng.

Nếu trong mạng có sử dụng router hay phân nhánh mạng con thì cần thiết phải thực hiện bước xây dựng bảng chọn đường trên các router và trên các máy tính.

1.1.5 Kiểm thử mạng

Sau khi đã cài đặt xong phần cứng và các máy tính đã được nối vào mạng. Bước kế tiếp là kiểm tra sự vận hành của mạng.

Trước tiên, kiểm tra sự nối kết giữa các máy tính với nhau. Sau đó, kiểm tra hoạt động của các dịch vụ, khả năng truy cập của người dùng vào các dịch vụ và mức độ an toàn của hệ thống.

Nội dung kiểm thử dựa vào bảng đặc tả yêu cầu mạng đã được xác định lúc đầu.

1.1.6 Bảo trì hệ thống

Mạng sau khi đã cài đặt xong cần được bảo trì một khoảng thời gian nhất định để khắc phục những vấn đề phát sinh xảy trong tiến trình thiết kế và cài đặt mạng.

1.2 Nội dung của giáo trình

Trong sáu giai đoạn cần thực hiện trong tiến trình xây dựng mạng ở trên, giáo trình này chủ yếu giới thiệu những vấn đề liên quan đến giai đoạn thiết kế mạng ở mức luận lý và vật lý. Đây chính là hai nội dung quan trọng trong tiến trình xây dựng mạng. Các vấn đề khác có thể tìm hiểu trong các môn học Mạng máy tính, Thực tập mạng máy tính.

1.3 Mô hình OSI.

Để dễ dàng cho việc nối kết và trao đổi thông tin giữa các máy tính với nhau, vào năm 1983, Tổ chức tiêu chuẩn thế giới ISO đã phát triển một mô hình cho phép hai máy tính có thể gởi và nhận dữ liệu cho nhau. Mô hình này dựa trên tiếp cận phân tầng (lớp), với mỗi tầng đảm nhiệm một số các chức năng cơ bản nào đó.

Để hai máy tính có thể trao đổi thông tin được với nhau cần có rất nhiều vấn đề liên quan. Ví dụ như cần có Card mạng, dây cáp mạng, điện thế tín hiệu trên cáp mạng, cách thức đóng gói dữ liệu, điều khiển lỗi đường truyền vv... Bằng cách phân chia các chức năng này vào những tầng riêng biệt nhau, việc viết các phần mềm để thực hiện chúng trở

nên dễ dàng hơn. Mô hình OSI giúp đồng nhất các hệ thống máy tính khác biệt nhau khi chúng trao đổi thông tin. Mô hình này gồm có 7 tầng:

Tầng 1: Tầng vật ký (Physical Layer)

Điều khiển việc truyền tải thật sự các bit trên đường truyền vật lý. Nó định nghĩa các thuộc tính về cơ, điện, qui định các loại đầu nối, ý nghĩa các pin trong đầu nối, qui định các mức điện thế cho các bit 0,1,….

Tầng 2: Tầng liên kết dữ liệu (Data-Link Layer)

Tầng này đảm bảo truyền tải các khung dữ liệu (Frame) giữa hai máy tính có đường truyền vật lý nối trực tiếp với nhau. Nó cài đặt cơ chế phát hiện và xử lý lỗi dữ liệu nhận.

Tầng 3: Tầng mạng (Network Layer)

Tầng này đảm bảo các gói tin dữ liệu (Packet) có thể truyền từ máy tính này đến máy tính kia cho dù không có đường truyền vật lý trực tiếp giữa chúng. Nó nhận nhiệm vụ tìm đường đi cho dữ liệu đến các đích khác nhau trong mạng.

Tầng 4: Tầng vận chuyển (Transport Layer)

Tầng này đảm bảo truyền tải dữ liệu giữa các quá trình. Dữ liệu gởi đi được đảm bảo không có lỗi, theo đúng trình tự, không bị mất mát, trùng lắp. Đối với các gói tin có kích thước lớn, tầng này sẽ phân chia chúng thành các phần nhỏ trước khi gởi đi, cũng như tập hợp lại chúng khi nhận được.

Tầng 5: Tầng giao dịch (Session Layer)

Tầng này cho phép các ứng dụng thiết lập, sử dụng và xóa các kênh giao tiếp giữa chúng (được gọi là giao dịch). Nó cung cấp cơ chế cho việc nhận biết tên và các chức năng về bảo mật thông tin khi truyền qua mạng.

Tầng 6: Tầng trình bày (Presentation Layer)

Tầng này đảm bảo các máy tính có kiểu định dạng dữ liệu khác nhau vẫn có thể trao đổi thông tin cho nhau. Thông thường các máy tính sẽ thống nhất với nhau về một kiểu định dạng dữ liệu trung gian để trao đổi thông tin giữa các máy tính. Một dữ liệu cần gởi đi sẽ được tầng trình bày chuyển sang định dạng trung gian trước khi nó được truyền lên mạng. Ngược lại, khi nhận dữ liệu từ mạng, tầng trình bày sẽ chuyển dữ liệu sang định dạng riêng của nó.

Tầng 7: Tầng ứng dụng (Application Layer)

Đây là tầng trên cùng, cung cấp các ứng dụng truy xuất đến các dịch vụ mạng. Nó bao gồm các ứng dụng của người dùng, ví dụ như các Web Browser (Netscape Navigator, Internet Explorer), các Mail User Agent (Outlook Express, Netscape Messenger, ...) hay các chương trình làm server cung cấp các dịch vụ mạng như các Web Server (Netscape Enterprise, Internet Information Service, Apache, ...), Các FTP Server, các Mail server (Send mail, MDeamon). Người dùng mạng giao tiếp trực tiếp với tầng này.

Về nguyên tắc, tầng n của một hệ thống chỉ giao tiếp, trao đổi thông tin với tầng n của hệ thống khác. Mỗi tầng sẽ có các đơn vị truyền dữ liệu riêng:

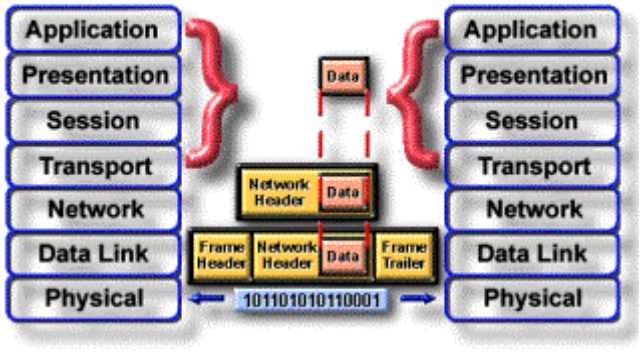
- Tầng vật lý: bit

- Tầng liên kết dữ liệu: Khung (Frame)
- Tầng Mạng: Gói tin (Packet)
- Tầng vận chuyển: Đoạn (Segment)

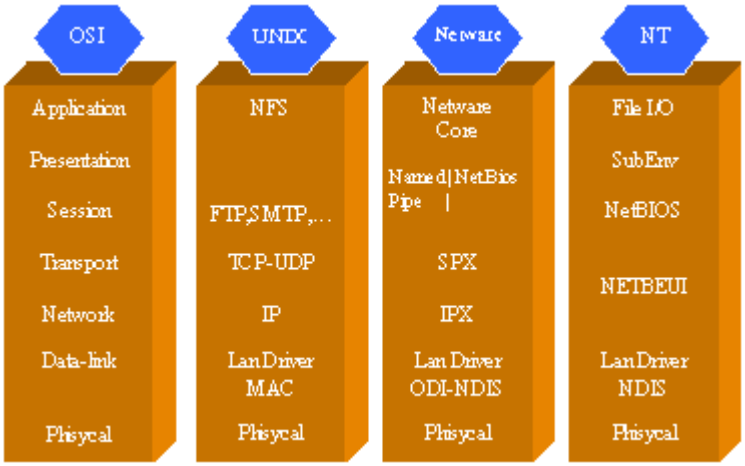
Trong thực tế, dữ liệu được gởi đi từ tầng trên xuống tầng dưới cho đến tầng thấp nhất của máy tính gởi. Ở đó, dữ liệu sẽ được truyền đi trên đường truyền vật lý. Mỗi khi dữ liệu được truyền xuống tầng phía dưới thì nó bị "gói" lại trong đơn vị dữ liệu của tầng dưới. Tại bên nhận, dữ liệu sẽ được truyền ngược lên các tầng cao dần. Mỗi lần qua một tầng, đơn vị dữ liệu tương ứng sẽ được tháo ra.

Đơn vị dữ liệu của mỗi tầng sẽ có một tiêu đề (header) riêng.

Hình 1.1 - Xử lý dữ liệu qua các tầng



OSI chỉ là mô hình tham khảo, mỗi nhà sản xuất khi phát minh ra hệ thống mạng của mình sẽ thực hiện các chức năng ở từng tầng theo những cách thức riêng. Các cách thức này thường được mô tả dưới dạng các chuẩn mạng hay các giao thức mạng. Như vậy dẫn đến trường hợp cùng một chức năng nhưng hai hệ thống mạng khác nhau sẽ không tương tác được với nhau. Hình dưới sẽ so sánh kiến trúc của các hệ điều hành mạng thông dụng với mô hình OSI.



Hình 1.2 - Kiến trúc của một số hệ điều hành mạng thông dụng

Để thực hiện các chức năng ở tầng 3 và tầng 4 trong mô hình OSI, mỗi hệ thống mạng sẽ có các protocol riêng:

- UNIX: Tầng 3 dùng giao thức IP, tầng 4 giao thức TCP/UDP
- Netware: Tầng 3 dùng giao thức IPX, tầng 4 giao thức SPX
- Giao thức NETBEUI của Microsoft cài đặt chức năng của cả hai tầng 3 và 4

Nếu chỉ dừng lại ở đây thì các máy tính UNIX, Netware, NT sẽ không trao đổi thông tin được với nhau. Với sự lớn mạnh của mạng Internet, các máy tính cài đặt các hệ

điều hành khác nhau đòi hỏi phải giao tiếp được với nhau, tức phải sử dụng chung một giao thức. Đó chính là bộ giao thức TCP/IP, giao thức của mạng Internet.

Chương 2

Các chuẩn mạng cục bộ

Mục đích

Chương này nhằm giới thiệu cho người đọc những vấn đề sau :

- Cách phân loại mạng chuyển mạch và mạng quảng bá
- Đặc điểm của mạng cục bộ
- Định nghĩa giao thức điều khiển truy cập đường truyền
- Các sơ đồ nối kết mạng LAN
- Các loại thiết bị sử dụng trong mạng LAN
- Các tổ chức chuẩn hóa về mạng
- Một số chuẩn mạng cục bộ phổ biến hiện nay như:
    - Ethernet: 10 BASE-5, 10BASE-2, 10 BASE-T
    - FAST Ethernet:100 BASE-TX, 100 BASE-T4,100BASE-FX
    - Token Ring

2.1 Phân loại mạng

Mạng cục bộ (LAN - Local Area Network) thường được biết đến như một mạng truyền dữ liệu tốc độ cao triển khai trong một phạm vi nhỏ như một phòng, một tòa nhà hay một khu vực. Trong khi mạng diện rộng (WAN – Wide Area Network) có phạm vi lớn hơn, có thể trải dài trên một quốc gia, một châu lục hay thậm chí cả hành tinh. Đây là cách phân loại mạng dựa trên tiêu chuẩn phân loại là phạm vi địa lý. Ngoài ra, ta có thể phân loại mạng dựa vào kỹ thuật truyền tải thông tin sử dụng trong mạng.

Mạng LAN sử dụng kỹ thuật mạng quảng bá (Broadcast network), trong đó các thiết bị cùng chia sẽ một kênh truyền chung. Khi một máy tính truyền tin, các máy tính khác đều nhận được thông tin. Ngược lại, mạng WAN sử dụng kỹ thuật Mạng chuyển mạch (Switching Network), có nhiều đường nối kết các thiết bị mạng lại với nhau. Thông tin trao đổi giữa hai điểm trên mạng có thể đi theo nhiều đường khác nhau. Chính vì thế cần phải có các thiết bị đặc biệt để định đường đi cho các gói tin, các thiết bị này được gọi là bộ chuyển mạch hay bộ chọn đường (router). Ngoài ra để giảm bớt số lượng đường nối kết vật lý, trong mạng WAN còn sử dụng các kỹ thuật đa hợp và phân hợp.

Chương này tập trung giới thiệu những vấn đề liên quan đến mạng cục bộ.

2.2 Mạng cục bộ và giao thức điều khiển truy cập đường truyền

Vì chỉ có một đường truyền vật lý trong mạng LAN, tại một thời điểm nào đó LAN chỉ cho phép một thiết bị được sử dụng đường truyền để truyền tin. Nếu có hai máy tính cùng gởi dữ liệu ở tại một thời điểm sẽ dẫn đến tình trạng đua tranh. Dữ liệu của hai thiết bị này sẽ bị phủ lấp lẫn nhau, không sử dụng được. Vì thế cần có một cơ chế để giải quyết sự cạnh tranh đường truyền giữa các thiết bị. Người ta gọi phương pháp giải quyết cạnh tranh đường truyền giữa các thiết bị trong một mạng cục bộ là **Giao thức điều khiển truy cập đường truyền** (Media Access Control Protocol hay MAC Protocol). Có hai giao thức chính thường được dùng trong các mạng cục bộ là: Giao thức CSMA/CD (Carrier Sense Multiple Access with Collision Detection) và Token Passing.

Trong các mạng sử dụng giao thức CSMA/CD như Ethernet chẳng hạn, các thiết bị mạng tranh nhau sử dụng đường truyền. Khi một thiết bị muốn truyền tin, nó phải lắng nghe xem có thiết bị nào đang sử dụng đường truyền hay không. Nếu đường truyền đang rãnh, nó sẽ truyền dữ liệu lên đường truyền. Trong quá trình truyền tải, nó đồng thời lắng nghe, nhận lại các dữ liệu mà nó đã gởi đi để xem có sự đụng độ với dữ liệu của các thiết bị khác hay không. Một cuộc đụng độ xảy ra nếu cả hai thiết bị cùng truyền dữ liệu một cách đồng thời. Khi đụng độ xảy ra, mỗi thiết bị sẽ tạm dừng một khoản thời gian ngẫu nhiên nào đó trước khi thực hiện truyền lại dữ liệu bị đụng độ. Khi mạng càng bận rộn thì tần suất đụng độ càng cao. Hiệu suất của mạng giảm đi một cách nhanh chóng khi số lượng các thiết bị nối kết vào mạng tăng lên.

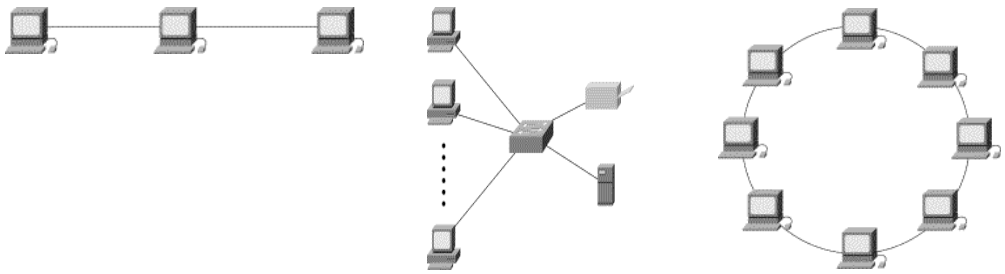
Trong các mạng sử dụng giao thức Token-passing như Token Ring hay FDDI, một gói tin đặc biệt có tên là thẻ bài (Token) được chuyển vòng quanh mạng từ thiết bị này đến thiết bị kia. Khi một thiết bị muốn truyền tải thông tin, nó phải đợi cho đến khi có được token. Khi việc truyền tải dữ liệu hoàn thành, token được chuyển sang cho thiết bị kế tiếp. Nhờ đó đường truyền có thể được sử dụng bởi các thiết bị khác. Tiện lợi lớn nhất của mạng Token-passing là ta có thể xác định được khoản thời gian tối đa một thiết bị phải chờ

để có được đường truyền và gởi dữ liệu. Chính vì thế mạng Token-passing thường được sử dụng trong các môi trường thời gian thực, như điều khiển thiết bị công nghiệp, nơi mà thời gian từ lúc phát ra một tín hiệu điều khiển cho đến khi thiết bị nhận được tín hiệu luôn đảm bảo phải nhỏ hơn một hằng số cho trước.

2.3 Các sơ đồ nối kết mạng LAN (LAN Topologies)

LAN topology định nghĩa cách thức mà ở đó các thiết bị mạng được tổ chức sắp xếp. Có ba sơ đồ nối kết mạng LAN phổ biến là: dạng thẳng (Bus), dạng hình sao (Star) và dạng hìng vòng (ring).

- Bus topology là một mạng với kiến trúc tuyến tính trong đó dữ liệu truyền tải của một trạm sẽ được lan truyền trên suốt chiều dài của đường truyền và được nhận bởi tất cả các thiết bị khác.
- Star topology là một kiến trúc mạng trong đó các máy trạm được nối kết vào một bộ tập trung nối kết, gọi là HUB
- Ring topology là một kiến trúc mạng mà nó bao gồm một loạt các thiết bị được nối lại với nhau trên một kênh truyền có hướng theo dạng vòng.



Bus topology **Star topology** **Ring topology**

Hình 2.1 – Topology thường sử dụng cho mạng LAN

2.4 Các loại thiết bị sử dụng trong mạng LAN

Để xây dựng mạng LAN, người ta thường dùng các thiết bị sau:

- Card giao tiếp mạng (NIC- Network Interface Card)
- Dây cáp mạng (Cable)
- Bộ khuyếch đại (Repeater)
- Bộ tập trung nối kết (HUB)
- Cầu nối (Brigde)
- Bộ chuyển mạch (Switch)
- Bộ chọn đường (Router)

2.5 Các tổ chức chuẩn hóa về mạng

Để các thiết bị phần cứng mạng của nhiều nhà sản xuất khác nhau có thể đấu nối, trao đổi thông tin được với nhau trong một mạng cục bộ thì chúng phải được sản xuất theo

cùng một chuẩn. Dưới đây là một số tổ chức chuẩn hóa quan trọng liên quan đến các thiết bị mạng:

- EIA (Electronic Industry Association)
- TIA (Telecom Industry Association)
- ISO (International Standard Organization)
- ANSI (American National Standard Institute)
- IEEE (Institute of Electrical and Electronics Engineers)

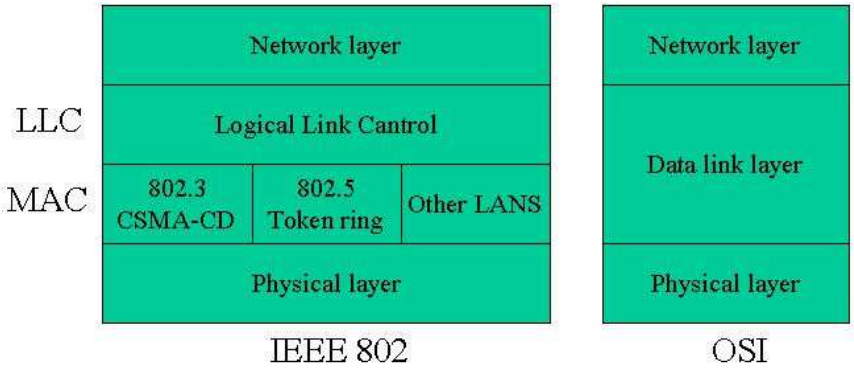
Trong đó hai tổ chức TIA và EIA kết hợp với nhau để đưa ra nhiều đặc tả cho các thiết bị truyền dẫn cũng như đưa ra nhiều sơ đồ nối dây.

IEEE có nhiều tiểu ban (Committee). Trong đó Tiểu ban 802 phụ trách về các chuẩn cho mạng cục bộ. Một số chuẩn mạng cục bộ quan trọng do tiểu ban này đưa ra như:

- 802.3: Chuẩn cho mạng Ethernet
- 802.4: Chuẩn cho mạng Token-Bus
- 802.5: Chuẩn mạng Token-Ring
- 802.11: Chuẩn mạng không dây.
- ....

Các chuẩn do IEEE 802 định nghĩa thực hiện chức năng của tầng 2 trong mô hình tham khảo OSI. Tuy nhiên, chúng chia tầng 2 thành hai tầng con (sublayer) là Tầng con điều khiển nối kết luận lý (LLC - Logical Link Control) và Tầng con điều khiển truy cập đường truyền (MAC – Medium Access Control).

Tầng con điều khiển truy cập đường truyền đảm bảo cung cấp dịch truyền nhận thông tin theo kiểu không nối kết. Trong khi tầng con điều khiển nối kết luận lý cung cấp dịch vụ truyền tải thông tin theo kiểu định hướng nối kết.



Hình 2.2 – Kiến trúc mạng cục bộ theo IEEE 802

2.6 Mạng Ethernet

Thuật ngữ Ethernet dùng để chỉ đến họ mạng cục bộ được xây dựng theo chuẩn IEEE 802.3 sử dụng giao thức CSMA/CD để chia sẻ đường truyền chung. Ethernet được xem như là kỹ thuật mạng cục bộ chủ đạo trên thị trường nối kết các máy tính cá nhân lại với nhau (chiếm khoảng 85% thị trường) bởi vì giao thức của nó có các đặc tính sau:

- Dễ hiểu, dễ cài đặt, quản trị và bảo trì
- Cho phép chi phí xây dựng mạng thấp
- Cung cấp nhiều sơ đồ nối kết mềm dẽo trong cài đặt
- Đảm bảo thành công việc liên nối kết mạng và vận hành của mạng cho dù các thiết bị được cung cấp bởi nhiều nhà sản xuất khác nhau.

2.6.1 Lịch sử hình thành

Mạng Ethernet đầu tiên được phát triển vào năm 1970 bởi công ty Xerox là một mạng thử nghiệm, sử dụng dây cáp đồng trục với tốc độ truyền tải dữ liệu 3 Mbps. Mạng sử dụng giao thức CSMA/CD.

Sự thành công của dự án này đã gây chú ý cho các nhà sản xuất thiết bị điện tử thời đó. Chính vì thế mà năm 1980, ba nhà sản xuất thiết bị điện tử hàng đầu là Digital Equipment Coperation, Intel Corporation và Xerox Corporation đã cùng nhau phát triển phiên bản Ethernet 1.0 với tốc độ truyền tải dữ liệu là 10 Mbps.

Năm 1983, chuẩn mạng IEEE 802.3 đã được soạn thảo với nội dung tương tự như chuẩn mạng Ethernet phiên bản 1.0. Đến năm 1985 thì IEEE 802.3 được chuẩn hóa. Sau đó nhiều chuẩn mạng cục bộ khác đã được phát triển dựa theo nguyền tắc chia sẻ đường truyền chung của giao thức CSMA/CD. Có thể liệt kê các chuẩn mạng sử dụng giao thức CSMA/CD như sau:

- Chuẩn mạng 802.3:
  - Có tên là mạng Ethernet
  - Tốc độ truyền tải dữ liệu là 10 Mbps
  - Hỗ trợ 4 chuẩn vật lý là 10Base-5 (cáp đồng trục béo), 10Base-2 (Cáp đồng trục gầy), 10Base-T (Cáp xoắn đôi) và 10Base-F (Cáp quang).
- Chuẩn mạng 802.3u
  - Có tên là mạng Fast Ethernet
  - Tốc độ truyền tải dữ liệu là 100 Mbps
  - Hỗ trợ 3 chuẩn vật lý là 100Base-TX (Cáp xoắn đôi), 100Base-T4 (Cáp xoắn đôi) và 100Base-FX (Cáp quang).
- Chuẩn mạng 802.3z:
  - Có tên là mạng Giga Ethernet
  - Tốc độ truyền tải dữ liệu là 1 Gbps
  - Hỗ trợ 3 chuẩn vật lý là 1000Base-LX, 1000Base-SX, 1000Base-CX. 1000Base-LX, 1000Base-SX sử dụng cáp quang. 1000Base-CX sử dụng dây cáp đồng bọc kim.
- Chuẩn mạng 802.3ab:
  - Có tên là mạng Giga Ethernet over UTP
  - Tốc độ truyền tải dữ liệu là 1 Gbps

- Hỗ trợ chuẩn vật lý 1000Base-TX sử dụng dây cáp xoắn đôi không bọc kim.

2.6.2 Card giao tiếp mạng (NIC-Network Interface Card)

Bởi vì các chức năng của mạng Ethernet chỉ liên quan đến tầng một và tầng hai trong mô hình tham khảo OSI, cho nên chúng thông thường được cài đặt trong Card giao tiếp mạng (NIC-Network Interface Card) được cắm vào bản mạch chính (motherboard) của máy tính. Khi chọn lựa một card mạng cần chú ý các vấn đề sau:

- Chuẩn khe cắm (slot) thiết bị ngoại vi được hỗ trợ bởi bản mạch chính: Các máy tính cá nhân hiện đại thông thường hỗ trợ loại khe cắm thiết bị ngoại vi theo chuẩn PCI. Các máy tính đời cũ có hỗ trợ chuẩn ISA. Khe cắm chuẩn ISA dài hơn so với khe cắm chuẩn PCI. Card mạng vì thế cũng có hai loại. Không thể sử dụng card mạng chuẩn PCI cắm vào khe cắm ISA và ngược lại. Chính vì thế khi mua card mạng cần lưu ý đến loại khe cắm.

NIC theo chuẩn PCI

NIC theo chuẩn ISA

Hình 2.3 – Một số loại giao diện mạng

- Loại đầu nối vào dây cáp: Mỗi chuẩn mạng thường qui định loại dây dẫn được sử dụng. Để nối card mạng vào dây dẫn cần có loại đầu nối riêng tùy thuộc vào từng loại dây dẫn. Ví dụ, để nối vào dây cáp đồng trục gầy trên card mạng cần có đầu nối BNC; để nối với dây cáp xoắn đôi card mạng cần có đầu nối UTP, ... Cần chọn card mạng có đầu nối theo đúng loại dây dẫn do chuẩn mạng qui định.

Card mạng là một thiết bị ngoại vi, vì thế bạn cần lưu ý đến các thông số xác định địa chỉ của nó như số hiệu ngắt (Interrupt), số hiệu cổng (port) và địa chỉ nền (Base address). Cần phải đặt chúng sao cho không trùng với các thiết bị khác đã có trên máy tính. Thông thường có phần mềm cài đặt (install/setup) đi kèm với card mạng khi mua, cho phép kiểm tra trạng thái của card mạng cũng như đặt lại các thông số trên.

Mỗi card mạng có một địa chỉ vật lý là một dãy số 48 bits (thường được viết dưới dạng 12 số thập lục phân), gọi là địa chỉ MAC. Một một card mạng có địa chỉ MAC riêng, không trùng lắp lẫn nhau. Chúng được các nhà sản xuất cài vào khi sản xuất.

2.6.3 Một số chuẩn mạng Ethernet phổ biến

2.6.3.1 Chuẩn mạng Ethernet 10BASE-5

Đây là chuẩn mạng Ethernet đầu tiên được phát triển. Nó bao gồm các thông số kỹ thuật sau:

- Sơ đồ mạng dạng BUS

- Sử dụng dây cáp đồng trục béo (thich coaxial cable), chiều dài tối đa của mỗi đoạn mạng (network segment) là 500 mét.
- Tốc độ truyền dữ liệu là 10 Mbps
- Khoảng cách gần nhất giữa hai nút / máy tính trên mạng là 2,5 mét
- Tối đa cho phép 100 nút / máy tính trên một đoạn mạng.
- Card mạng sử dụng đầu nối kiểu AUI.
- Chiều dài dây dẫn nối máy tính vào dây cáp đồng trục dài tối đa 50 mét
- Sử dụng hai thiết bị đầu cuối (Terminator) trở kháng 50 Ω để gắn vào mỗi đầu của dây cáp. Một trong hai đầu cuối này phải nối tiếp đất vào vỏ của máy tính.

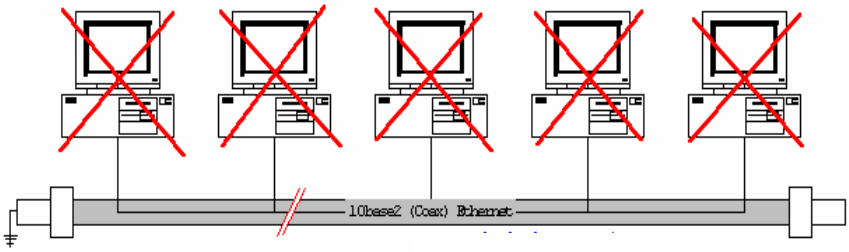
Thế mạnh lớn nhất của chuẩn mạng này là đường kính mạng (khoảng cách giữa hai máy tính trong mạng) lớn. Tuy nhiên việc thi công mạng khá phức tạp, tốc độ lại không cao, giá thành không phải là thấp so với các chuẩn mạng khác. Chính vì thế mà hiện nay nó không phải là chuẩn mạng được chọn lựa khi xây dựng các mạng LAN mới.

2.6.3.2 Chuẩn mạng Ethernet 10BASE-2

Chuẩn 10Base-2 có các thông số kỹ thuật sau:

- Sơ đồ mạng dạng Bus
- Sử dụng dây cáp đồng trục gầy (thin coaxial cable), chiều dài tối đa của mỗi đoạn mạng (network segment) là 185 mét.
- Tốc độ truyền dữ liệu là 10 Mbps
- Tối đa cho phép 30 nút / máy tính trên một đoạn mạng.
- Dây dẫn được cắt thành từng đoạn nhỏ để nối hai máy tính kế cận nhau với chiều dài tối thiểu là 0,5 mét. Mỗi đầu dây có một đầu nối BNC bấm vào.
- Card mạng sử dụng cần có đầu nối BNC để gắn đầu nối hình chữ T vào (T connector).
- Sử dụng hai thiết bị đầu cuối (Terminator) trở kháng 50Ω để gắn vào đầu nối hình chữ T của hai máy ở hai đầu dây mạng. Một trong hai đầu cuối này phải nối tiếp đất vào vỏ của máy tính.

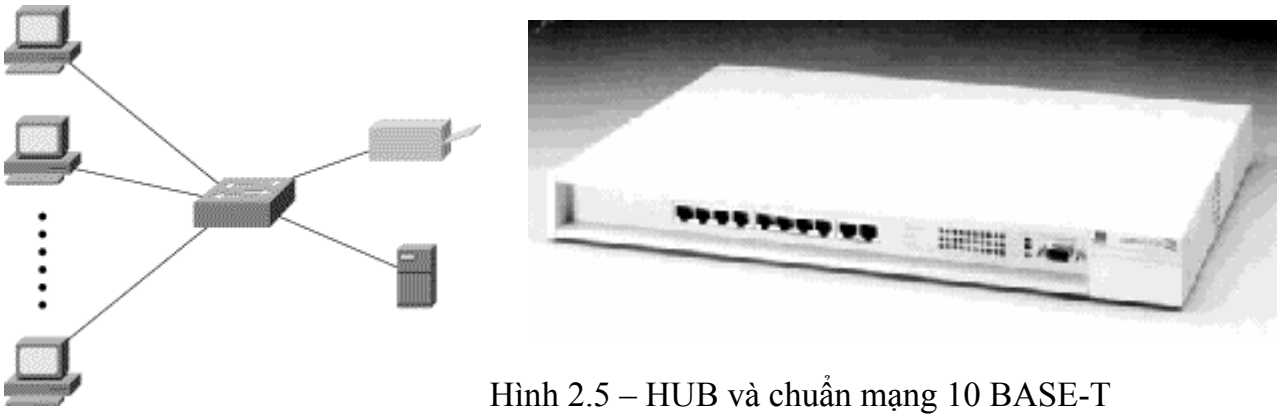
Mạng thiết kế theo chuẩn 10Base-2 có giá thành rẻ nhất khi so với các chuẩn khác. Tuy nhiên tính ổn định của nó không cao, các điểm nối dây rất dễ bị hỏng tiếp xúc. Chỉ cần một điểm nối dây trong mạng không tiếp xúc tốt sẽ làm cho các máy khác không thể vào mạng được.



Hình 2.4 – Yếu điểm của mạng 10BASE-2

2.6.3.3 Chuẩn mạng Ethernet 10BASE-T

Vào những năm 1990, cấu hình mạng hình sao trở nên được ưu chuộng. Trong mạng sử dụng một bộ khuếch đại nhiều cổng (port), được họi là HUB hay còn gọi là Bộ tập trung nối kết, để nối các máy tính lại với nhau.



Hình 2.5 – HUB và chuẩn mạng 10 BASE-T

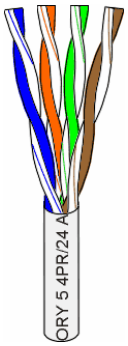
Với một HUB, người ta quan tâm đến số lượng cổng của nó. Bởi vì một cổng cho phép nối một máy tính vào mạng. Một HUB 24 cổng sẽ cho nối tối đa 24 máy tính lại với nhau. Trên thị trường thường tìm thấy các HUB 8,12,16, 24 cổng.

Chuẩn 10BASE-T sử dụng cáp xoắn đôi (Twisted Pair Cable) để nối máy tính vào HUB. Cáp xoắn đôi thường có hay loại là có vỏ bọc (STP - Shielded Twisted Pair) và loại không có vỏ bọc (UTP - Unshielded Twisted Pair).

Loại có vỏ bọc có tính năng chống nhiễu tốt hơn loại không có vỏ bọc. Nó được sử dụng trong những môi trường mà ở đó có các sóng điện từ mạnh (đài phát thanh, phát hình, ...). Tuy nhiên giá thành đắt hơn loại không có vỏ bọc. Đa số các mạng cục bộ sử dụng cho văn phòng ngày nay sử dụng cáp xoắn đôi không bọc kim (cáp UTP).

Cáp xoắn đôi được chia thành nhiều chủng loại (Caterogy), viết tắt là CAT. Mỗi chủng loại có băng thông tối đa khác nhau.

- CAT 1:2Mbps
- CAT 2:4 Mbps
- CAT 3:16Mbps
- CAT 4:20Mbps
- CAT 5:100Mbps
- CAT 5E: 1000Mbps
- CAT 6:1000Mbps

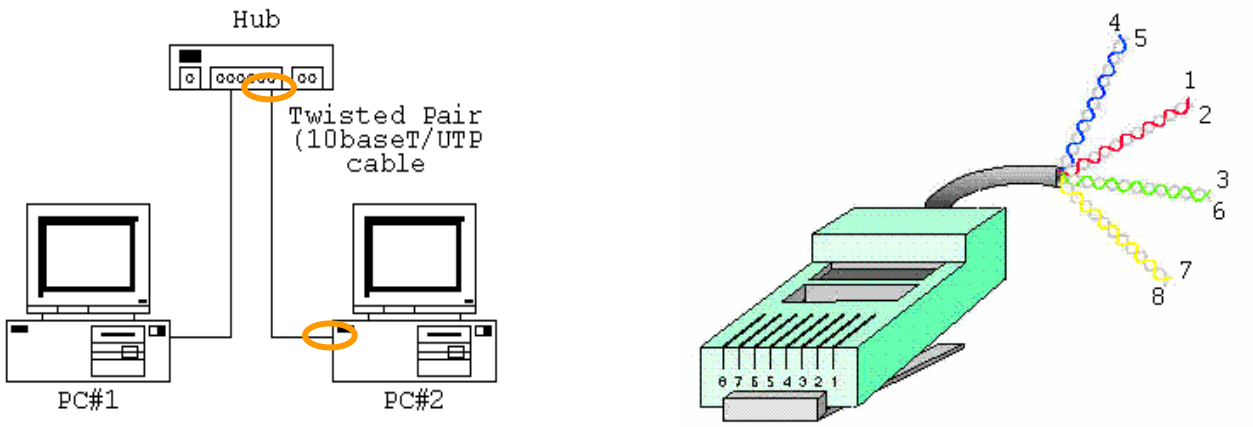


Hình 2.6 - Cáp xoắn đôi

Chuẩn 10 BASE-T có băng thông qui định là 10 Mbps, vì thế phải sử dụng cáp từ CAT 3 trở lên. Chiều dài tối đa của một sợi dây là 100 mét.

Cáp xoắn đôi có 8 sợi, xoắn lại với nhau từng đôi một tạo thành 4 đôi với bốn màu đặc trưng: Cam (Orange), xanh dương (Blue), xanh lá (Green) và nâu (Brown). Một đôi gồm một sợi được phủ màu hoàn toàn và một sợi màu trắng được điểm vào các đốm màu tương ứng.

Để có thể nối máy tính vào HUB, mỗi đầu của sợi cáp xoắn đôi đều phải được bấm đầu nối UTP (UTP Connector). Card mạng trong trường hợp này cũng phải hỗ trợ loại đầu nối UTP.



Hình 2.7 – Sử dụng đầu nối UTP với dây cáp xoắn đôi

Đâu nối UTP có 8 pin để tiếp xúc với 8 sợi của dây cáp xoắn đôi. Chuẩn 10 BASE-T chỉ sử dụng 4 trong 8 sợi của cáp xoắn đôi để truyền dữ liệu (Một cặp truyền, một cặp nhận). Bốn sợi còn lại không sử dụng. Tương ứng trên đầu nối UTP, chỉ có 4 pin 1,2,3,6 được sử dụng, các pin còn lại không dùng đến.

Câu hỏi kế tiếp là sợi dây màu nào của cáp xoắn đôi sẽ đi với pin số mấy của đầu nối UTP. Để thống nhất, EIA và TIA đã phối hợp và đưa ra 2 chuẩn bấm đầu dây là T568A và T568B

Chuẩn T568A qui định:

- Pin 1: White Green / Tx+
- Pin 2: Green / Tx-
- Pin 3: White Orange / Rx+
- Pin4: Blue
- Pin5: White Blue
- Pin 6: Orange / Rx-
- Pin 7: White Brown
- Pin 8: Brown

Chuẩn T568B qui định:

- Pin 1: White Orange / Tx +
- Pin 2: Orange / Tx-
- Pin 3: White Green / Rx+
- Pin4: Blue

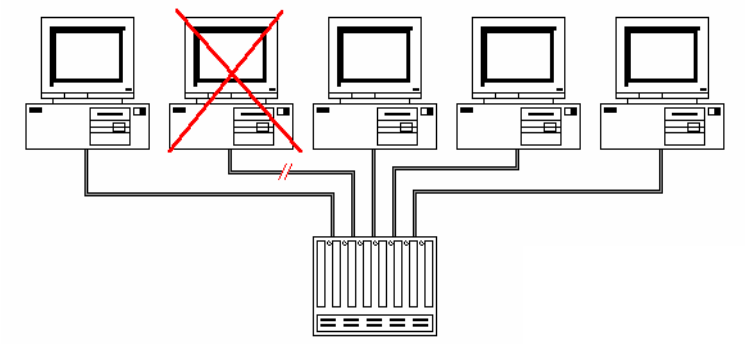
- Pin5: White Blue
- Pin 6: Green / Rx-
- Pin 7: White Brown
- Pin 8: Brown

Như vậy, sẽ dẫn đến 2 sơ đồ nối dây đối với một sợi cáp xoắn đôi:

- Sơ đồ nối dây thẳng (Straight through): hai đầu của một sơi cáp xoắn đôi đều được bấm đầu UTP theo cùng một chuẩn, tức hoặc cả hai cùng bấm theo chuẩn T568A hoặc cả hai cùng bấm theo chuẩn T568B.
- Sơ đồ nối dây chéo (Cross over): hai đầu của một sợi cáp xoắn đôi được bấm đầu UTP theo hai chuẩn khác nhau, tức một đầu bấm theo chuẩn T568A, đầu còn lại bấm theo chuẩn T568B.

Dây được bấm theo sơ đồ thẳng dùng để nối hai thiết bị khác loại lại với nhau. Ví dụ nối máy tính và Hub,Switch, router. Ngược lại, dây bấm theo sơ đồ chéo dùng để nối hai thiết bị cùng loại, ví dụ nối Hub với Hub, nối máy tính với máy tính, Hub với Router.

So với chuẩn 10 BASE-2, chuẩn 10 BASE-T đắt hơn, nhưng nó có tính ổn định cao hơn: sự cố trên một điểm nối dây không ảnh hưởng đến toàn mạng.

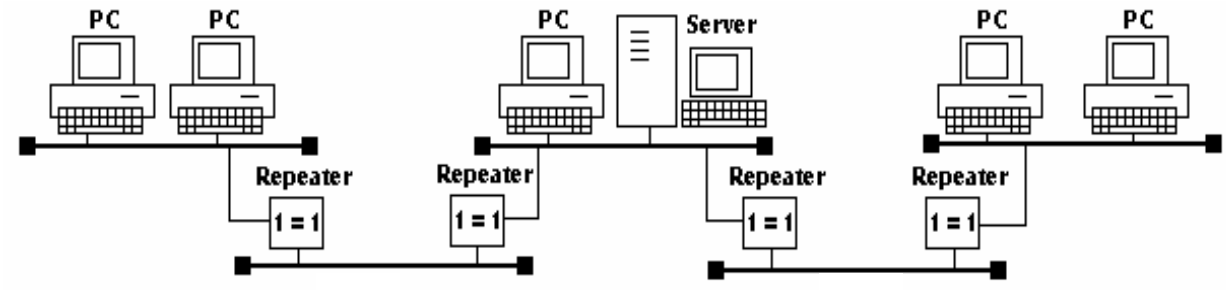


Hình 2.8 – Chuẩn 10BASE-T khắc phục nhược điểm của 10BASE-2

2.6.3.4 Vấn đề mở rộng mạng

2.6.3.4.1 Mở rộng mạng 10 BASE-2

Chuẩn 10BASE-2 ràng buộc số nút tối đa trên một nhánh mạng (segment) là 30. Nếu mạng có hơn 30 máy tính thì phải sử dụng ít nhất 2 nhánh mạng và nối chúng lại với nhau bằng một bộ khuếch đại (Repeater).



Hình 2.9 – Luật 5-4-3 khi sử dụng Repeater hay HUB

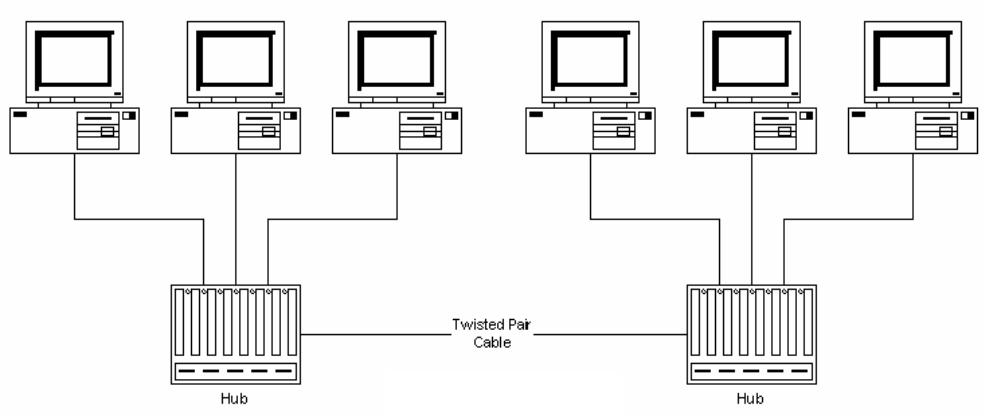
Tuy nhiên, để đảm bảo các máy tính có thể phát hiện được đụng độ khi truyền dữ liệu, số lượng tối đa các nhánh mạng được nối lại với nhau bằng các Repeater bị giới hạn bởi luật 5-4-3. Luật này qui định như sau:

- Chỉ có thể nối tối đa 5 nhánh mạng lại với nhau bằng các Repeater
- Chỉ có thể sử dụng tối đa 4 Repeater trong một mạng
- Chỉ cho phép tối đa 3 nhánh mạng có nhiều hơn 3 nút (Một nút có thể là một máy tính hoặc là một Repeater)

2.6.3.4.2 Mở rộng mạng Ethernet

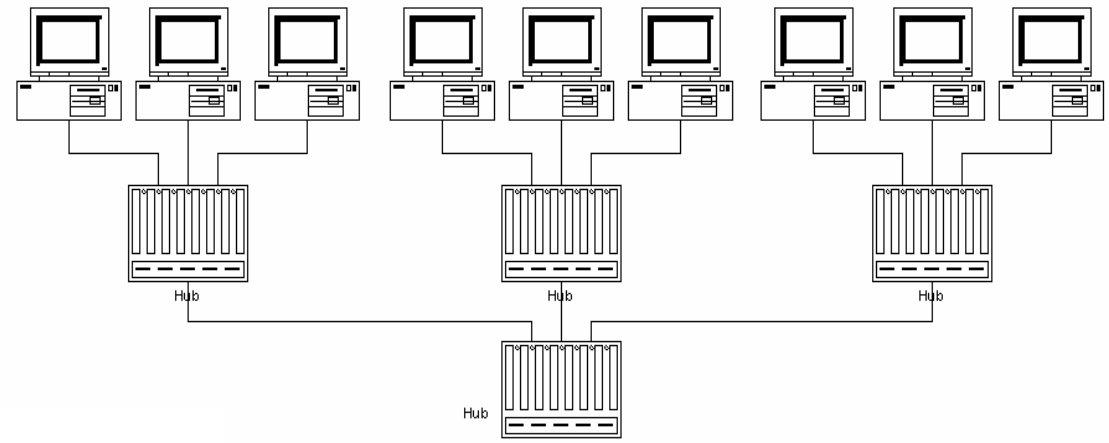
Mỗi cổng trên Hub cho phép nối một máy tính vào mạng. Thường số lượng cổng trên Hub là 8, 12, 16, 24. Nếu số lượng máy tính cần nối mạng vượt quá số lượng cổng mà một Hub có thể cung cấp, khi đó ta phải sử dụng nhiều Hub và nối chúng lại với nhau. Dưới đây là một vài sơ đồ thường được sử dụng để mở rộng mạng theo chuẩn 10BASE-T:

- Nối liên tiếp các Hub lại với nhau: Trong sơ đồ này cần tuân thủ luật 5-4-3, đảm bảo rằng tín hiệu đi từ máy tính này đến máy tính kia trong mạng không đi qua nhiều hơn 4 HUB.



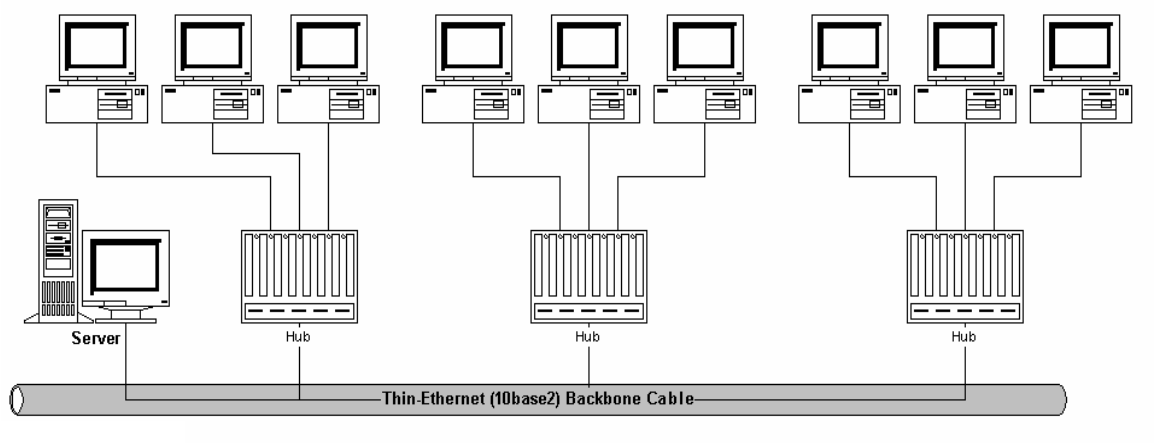
Hình 2.10 – Sơ đồ nối kết hai HUB

- Sử dụng một Hub làm xương sống: Sơ đồ này được sử dụng khi số lượng Hub nhiều hơn 4



Hình 2.11 – Sử dụng HUB để nối nhiều HUB

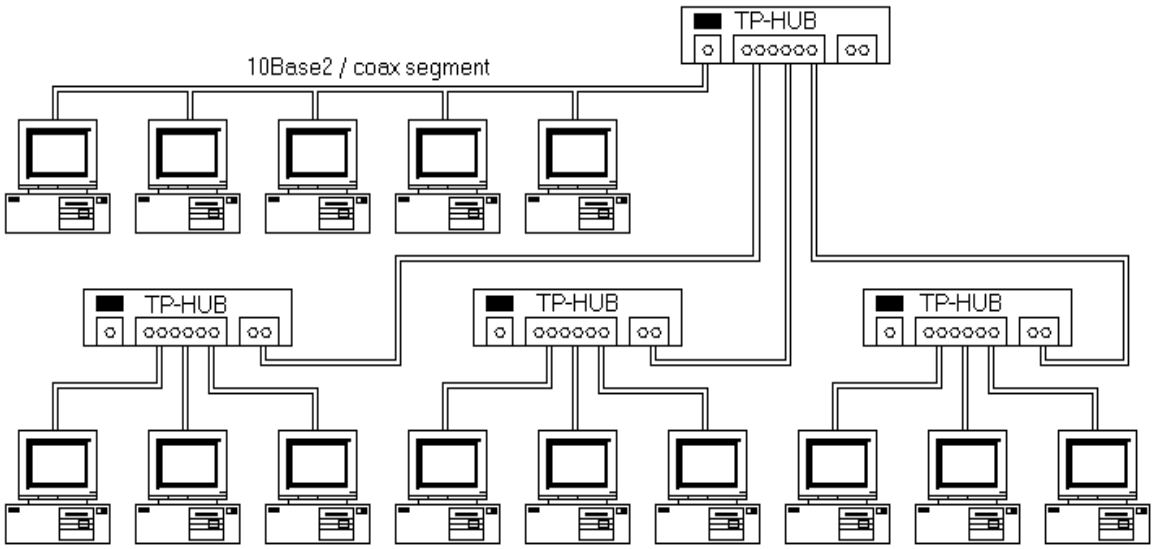
- Sử dụng một nhánh mạng 10BASE-2 làm xương sống: Trường hợp này phải chọn các Hub có môđun mở rộng (Add- in module) 10BASE-2.



Hình 2.12 – Nối kết các HUB bằng cáp đồng trục gầy

2.6.3.4.3 Sơ đồ hỗn hợp

Có thể nối các nhánh mạng 10Base-2 và 10Base-T theo sơ đồ sau:



Hình 2.13 – Nối mạng 10BASE-2 và 10BASE-T lại với nhau

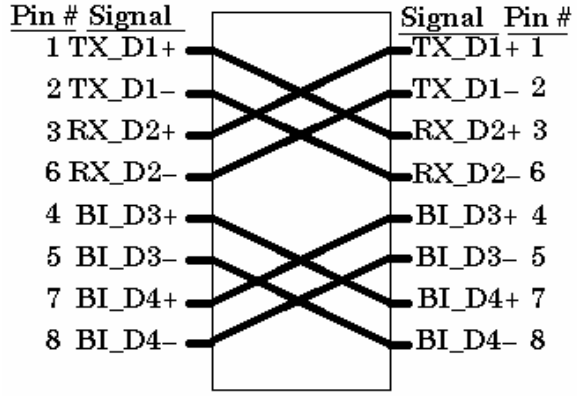
2.6.3.5 Mạng Fast Ethernet

Để tăng tốc độ truyền dữ liệu, chuẩn mạng Fast Ethernet đã được phát triển với tốc độ tăng gấp 10 lần sơ với chuẩn mạng Ethernet, tức 100 Mbps. Về cơ bản Fast Ethernet vẫn sử dụng giao thức CSMA/CD để chia sẻ đường truyền chung giữa các máy tính. Fast

Ethernet định nghĩa 3 chuẩn mạng ở tầng vật lý là 100Base-Tx, 100Base-T4 và 100Base-FX.

Chuẩn mạng 100Base-TX và 100 Base-T4 sử dụng topology dạng hình sao, với một Hub làm trung tâm, cùng các loại đầu nối UTP tương tự như chuẩn 10Base-T. Tuy nhiên chúng có các điểm khác nhau như:

- Chuẩn 100Base-TX sử dụng dây cáp xoắn đôi từ CAT 5 trở lên, chỉ sử dụng 2 đôi và có sơ đồ bấm dây giống như chuẩn 10Base-T.
- Chuẩn 100Base-T4 sử dụng cáp xoắn đôi từ CAT 3 trở lên. Điều này cho phép sử dụng lại hệ thống dây của các mạng 10Base-T. Tuy nhiên sơ đồ đầu dây trong chuẩn này có sự khác biệt. Dây phải được bấm đầu RJ45 theo sơ đồ sau:



Hình 2.14 – Sơ đồ bấm dây cho chuẩn mạng 100 BASE-T4

Chiều dài tối đa sợi cáp trong cả hai chuẩn vẫn là 100 mét.

- Chuẩn 100Base-FX được thiết kế để nối kết vào đường truyền cáp quang với chiều dài của sợi cáp lên đến 2000 mét, sử dụng loại đầu nối SC.

Hub trong chuẩn Fast Ethernet được phân thành 2 loại là Hub lớp 1(Class 1) và Hub lớp 2 (Class 2).

Hub lớp 2 chỉ cho phép hai nhánh mạng có cùng kiểu tín hiệu giao tiếp với nhau. Ví dụ như giữa nhánh 100Base-TX và 100Base-TX hay giữa nhánh mạng 100Base-T4 và 100Base-T4. Ta có thể nối 2 Hub lớp 2 lại với nhau với khoảng cách tối đa giữa chúng là 5m.

Hub lớp 1 cho phép hai nhánh mạng khác kiểu tín hiệu có thể giao tiếp được với nhau. Ví dụ giữa nhánh mạng 100Base-TX và 100Base-FX. Tuy nhiên chúng không cho phép nối các Hub lại với nhau.

Một điểm cần lưu ý nữa là card mạng sử dụng cũng phải chọn loại hỗ trợ chuẩn Fast Ethernet.

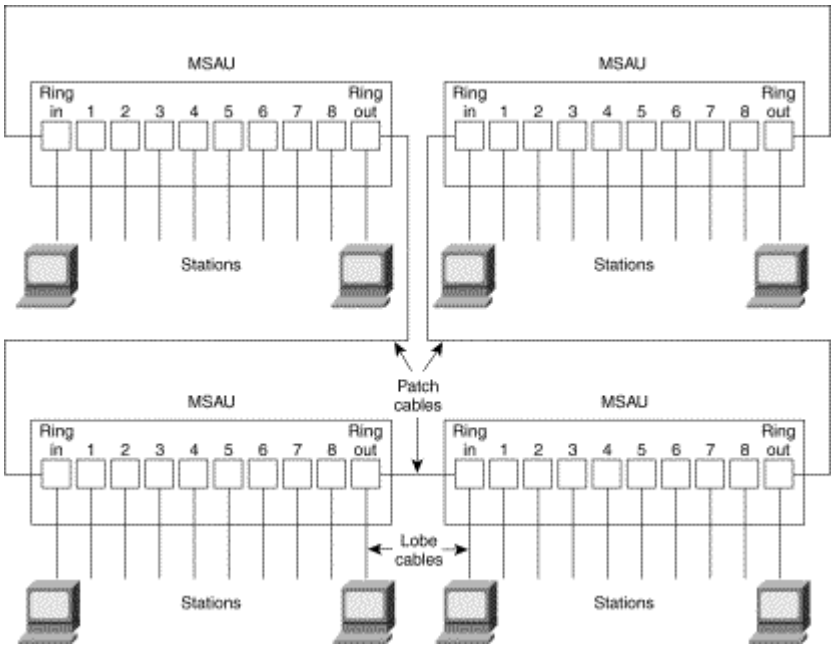
Hiện nay chuẩn mạng 100Base-TX được sử dụng nhiều nhất vì nó cung cấp tốc độ cao, ổn định, dễ thi công và không quá đắt tiền. Chuẩn 100Base-FX cũng được sử dụng đến trong trường hợp đường kính mạng vượt quá tầm của chuẩn 100Base-TX (Trong khoảng từ 100 đến 2.000 mét)

Một điểm cần lưu ý nữa là khả năng liên thông giữa chuẩn Ethernet và Fast Ethernet. Đa số Hub và card mạng thuộc chuẩn Fast Ethernet đều hỗ trợ thêm chức năng Auto-Sensing, nhờ đó có thể giao tiếp được với các thiết bị của chuẩn 10Base-T.

Ví dụ, nếu card mạng chuẩn 100Base-TX có tính năng Auto-Sensing nối kết vào một cổng 10Base-T thì nó sẽ tự động nhận biết và chuyển sang hoạt động theo chuẩn 10Base-T. Hay ngược lại, một card mạng chuẩn 10Base-T nối vào một cổng 100Base-TX của Hub có tính năng Auto-Sensing thì Hub sẽ tự động chuyển cổng sang hoạt động theo chuẩn 10Base-T.

2.6.3.6 Mạng Token Ring

Token Ring là mạng cục bộ được phát minh bởi IBM vào những năm 1970. Về sau, Token Ring được chuẩn hóa trong chuẩn IEEE 802.5. Các máy tính nối vào MSAU (MultiStation Access Unit) bằng dây cáp xoắn đôi. Các MSAU sau đó nối lại với nhau hình thành một vòng trong (Ring) như hình dưới đây:



Hình 2.15 – Sơ đồ nối kết mạng theo chuẩn mạng Token Ring

Chương 3

Cơ sở về cầu nối

Mục đích

Chương này nhằm giới thiệu cho người đọc những vấn đề sau:

- Các vấn đề về băng thông gặp phải khi thực hiện mở rộng mạng bằng các thiết bị như Repeater và HUB,
- Giải pháp khắc phục với cầu nối (Bridge)
- Giới thiệu cầu nối trong suốt và Giải thuật Backward Learning
- Vấn đề vòng quẩn và giải thuật Spanning tree
- Cầu nối xác định đường đi từ nguồn
- Cầu nối trộn lẫn

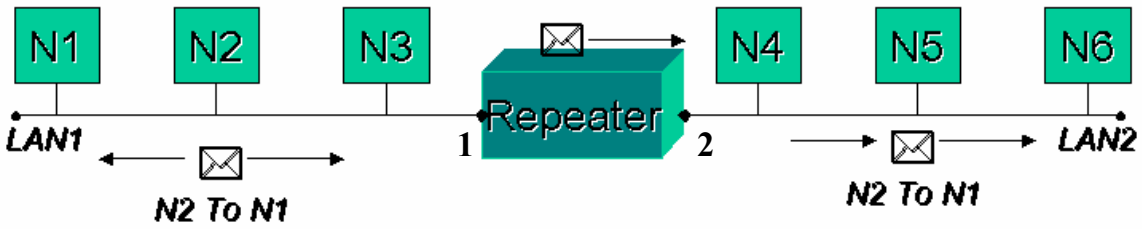
3.1 Giới thiệu về liên mạng

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. Người ta thực hiện liên mạng (Internetworking) để nối kết nhiều mạng lại với nhau nhờ đó mở rộng được phạm vi, số lượng máy tính trong mạng, cũng như cho phép các mạng được xây dựng theo các chuẩn khác nhau có thể giao tiếp được với nhau.

Liên mạng có thể được thực hiện ở những tầng khác nhau, tùy thuộc vào mục đích cũng như thiết bị mà ta sử dụng.

Tầng nối kết	**Mục đích**	**Thiết bị sử dụng**
Tầng vật lý	Tăng số lượng và phạm vi mạng LAN	HUB / Repeater
Tầng liên kết dữ liệu	Nối kết các mạng LAN có tầng vật lý khác nhau Phân chia vùng đụng độ để cải thiện hiệu suất mạng	Cầu nối (Bridge) Bộ hoán chuyển (Switch)
Tầng mạng	Mở rộng kích thước và số lượng máy tính trong mạng, hình thành mạng WAN	Router
Các tầng còn lại	Nối kết các ứng dụng lại với nhau	Gateway

Trong chương này ta sẽ xem xét các vấn đề liên quan đến việc liên mạng ở tầng 2, giới thiệu về cơ chế hoạt động, tính năng của cầu nối (Brigde).Nhược điểm của các thiết bị liên mạng ở tầng 1 (Repeater, HUB)



Hình 3.1 – Hạn chế của Repeater/HUB

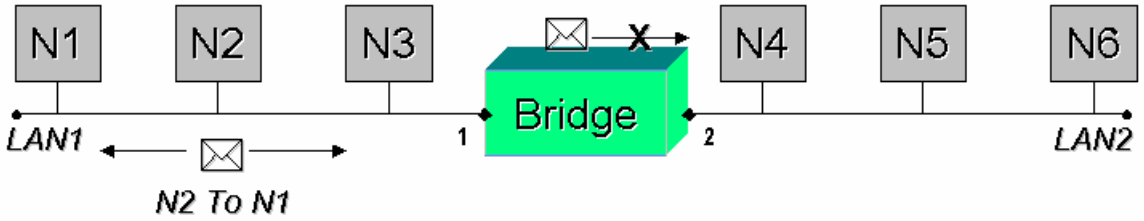
Xét một liên mạng gồm 2 nhánh mạng LAN1 và LAN2 nối lại với nhau bằng một Repeater. Giả sử máy N2 gởi cho N1 một Frame thông tin. Frame được lan truyền trên LAN1 và đến cổng 1 của Repeater dưới dạng một chuỗi các bits. Repeater sẽ khuếch đại chuỗi các bits nhận được từ cổng 1 và chuyển chúng sang cổng 2. Điều này vô tình đã chuyển cả khung N2 gởi cho N1 sang LAN2. Trên LAN1, N1 nhận toàn bộ Frame. Trên LAN2 không có máy trạm nào nhận Frame cả. Tại thời điểm đó, nếu N5 có nhu cầu gởi khung cho N4 thì nó sẽ không thực hiện được vì đường truyền đang bị bận.

Ta nhận thấy rằng, Frame N2 gởi cho N1 không cần thiết phải gởi sang LAN 2 để tránh lãng phí đường truyền trên LAN 2. Tuy nhiên, do Repeater hoạt động ở tầng 1, nó

không hiểu Frame là gì, nó sẽ chuyển đi mọi thứ mà nó nhận được sang các cổng còn lại. Liên mạng bằng Repeater hay Hub sẽ làm tăng vùng đụng độ của mạng, khả năng đụng độ khi truyền tin của các máy tính sẽ tăng lên, hiệu năng mạng sẽ giảm xuống.

3.2 Giới thiệu về cầu nối

Bây giờ ta thay thế Repeater bằng một Bridge. Khi Frame N2 gởi cho N1 đến công 1 của Bridge nó phân tích và thấy rằng không cần thiết phải chuyển Frame sang LAN 2.



Hình 3.2 – Bridge khắc phục nhược điểm của Repeater/HUB

Bridge là một thiết bị hoạt động ở tầng 2 trong mô hình OSI. Bridge làm nhiệm vụ chuyển tiếp các khung từ nhánh mạng này sang nhánh mạng khác. Điều quan trọng là Bridge « thông minh », nó chuyển frame một cách có chọn lọc dựa vào địa chỉ MAC của các máy tính. Bridge còn cho phép các mạng có tầng vật lý khác nhau có thể giao tiếp được với nhau. Bridge chia liên mạng ra thành những vùng đụng độ nhỏ, nhờ đó cải thiện được hiệu năng của liên mạng tốt hơn so với liên mạng bằng Repeater hay Hub.

Có thể phân Bridge thành 3 loại:

- Cầu nối trong suốt (Transparent Bridge): Cho phép nối các mạng Ethernet/ Fast Ethernet lại với nhau.
- Cầu nối xác định đường đi từ nguồn (Source Routing Bridge): Cho phép nối các mạng Token Ring lại với nhau.
- Cầu nối trộn lẫn (Mixed Media Bridge): Cho phép nối mạng Ethernet và Token Ring lại với nhau.

3.2.1 Cầu nối trong suốt

3.2.1.1 Giới thiệu

Cầu nối trong suốt được phát triển lần đầu tiên bởi Digital Equipment Corporation vào những năm đầu thập niên 80. Digital đệ trình phát minh của mình cho IEEE và được đưa vào chuẩn IEEE 802.1.

Cầu nối trong suốt được sử dụng để nối các mạng Ethernet lại với nhau. Người ta gọi là cầu nối trong suốt bởi vì sự hiện diện và hoạt động của nó thì trong suốt với các máy trạm. Khi liên mạng bằng cầu nối trong suốt, các máy trạm không cần phải cấu hình gì thêm để có thể truyền tải thông tin qua liên mạng.

3.2.1.2 Nguyên lý hoạt động

Khi cầu nối trong suốt được mở điện, nó bắt đầu học vị trí của các máy tính trên mạng bằng cách phân tích địa chỉ máy gởi của các khung mà nó nhận được từ các cổng của mình. Ví dụ, nếu cầu nối nhận được một khung từ cổng số 1 do máy A gởi, nó sẽ kết luận rằng máy A có thể đến được nếu đi ra hướng cổng 1 của nó. Dựa trên tiến trình này,

cầu nối xây dựng được một Bảng địa chỉ cục bộ (Local address table) mô tả địa chỉ của các máy tính so với các cổng của nó.

Địa chỉ máy tính (Địa chỉ MAC)	Cổng hướng đến máy tính
00-2C-A3-4F-EE-07	1
00-2C-A3-5D-5C-2F	2
...	

Hình 3.3 – Bảng địa chỉ cục bộ của cầu nối

Cầu nối sử dụng bảng địa chỉ cục bộ này làm cơ sở cho việc chuyển tiếp khung. Khi khung đến một cổng của cầu nối, cầu nối sẽ đọc 6 bytes đầu tiên của khung để xác định địa chỉ máy nhận khung. Nó sẽ tìm địa chỉ này trong bảng địa chỉ cục bộ và sẽ ứng xử theo một trong các trường hợp sau:

- Nếu máy nhận nằm cùng một cổng với cổng đã nhận khung, cầu nối sẽ bỏ qua khung vì biết rằng máy nhận đã nhận được khung.
- Nếu máy nhận nằm trên một cổng khác với cổng đã nhận khung, cầu nối sẽ chuyển khung sang cổng có máy nhận.
- Nếu không tìm thấy địa chỉ máy nhận trong bảng địa chỉ, cầu nối sẽ gởi khung đến tất cả các cổng còn lại của nó, trừ cổng đã nhận khung.

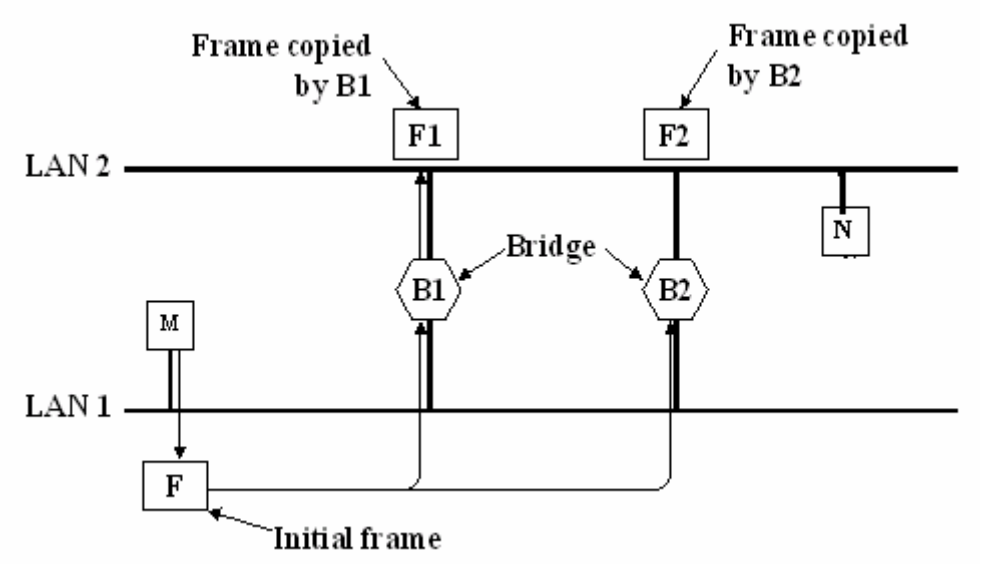
Trong mọi trường hợp, cầu nối đều cập nhật vị trí của máy gởi khung vào trong bảng địa chỉ cục bộ.

Cầu nối trong suốt thành công trong việc phân chia mạng thành những vùng đụng độ riêng rời. Đặc biệt khi quá trình gởi dữ liệu diễn ra giữa hai máy tính nằm về cùng một hướng cổng của cầu nối, cầu nối sẽ lọc không cho luồng giao thông này ảnh hưởng đến các nhánh mạng trên các cổng còn lại. Nhờ điều này cầu nối trong suốt cho phép cải thiện được băng thông trong liên mạng.

3.2.1.3 Vấn đề vòng quẩn - Giải thuật Spanning Tree

Cầu nối trong suốt sẽ hoạt động sai nếu như trong hình trạng mạng xuất hiện các vòng. Xét ví dụ như hình dưới đây:

Giả sử M gởi khung F cho N, cả hai cầu nối B1 và B2 chưa có thông tin gì về địa chỉ của N. Khi nhận được khung F, cả B1 và B2 đều chuyển F sang LAN 2, như vậy trên LAN 2 xuất hiện 2 khung F1 và F2 là phiên bản của F được sao lại bởi B1 và B2. Sau đó F1 đến B2 và F2 đến B1. Tiếp tục B1 và B2 lại lần lượt chuyển F2 và F1 sang LAN1, quá trình này sẽ không dừng, dẫn đến hiện tượng rác trên mạng. Người ta gọi hiện tượng này là vòng quẩn trên mạng.



Hình 3.4 – Vấn đề vòng quẩn trong mạng

Để khắc phục hiện tượng vòng quẩn, Digital đã đưa ra giải thuật nối cây, sau này được chuẩn hóa dưới chuẩn IEEE 802.1d.

Mục tiêu của giải thuật này là nhằm xác định ra các cổng tạo nên vòng quẩn trên mạng và chuyển nó về trạng thái dự phòng (stand by) hay khóa (Blocked), đưa sơ đồ mạng về dạng hình cây (không còn các vòng). Các cổng này được chuyển sang trạng thái hoạt động khi các cổng chính bị sự cố.

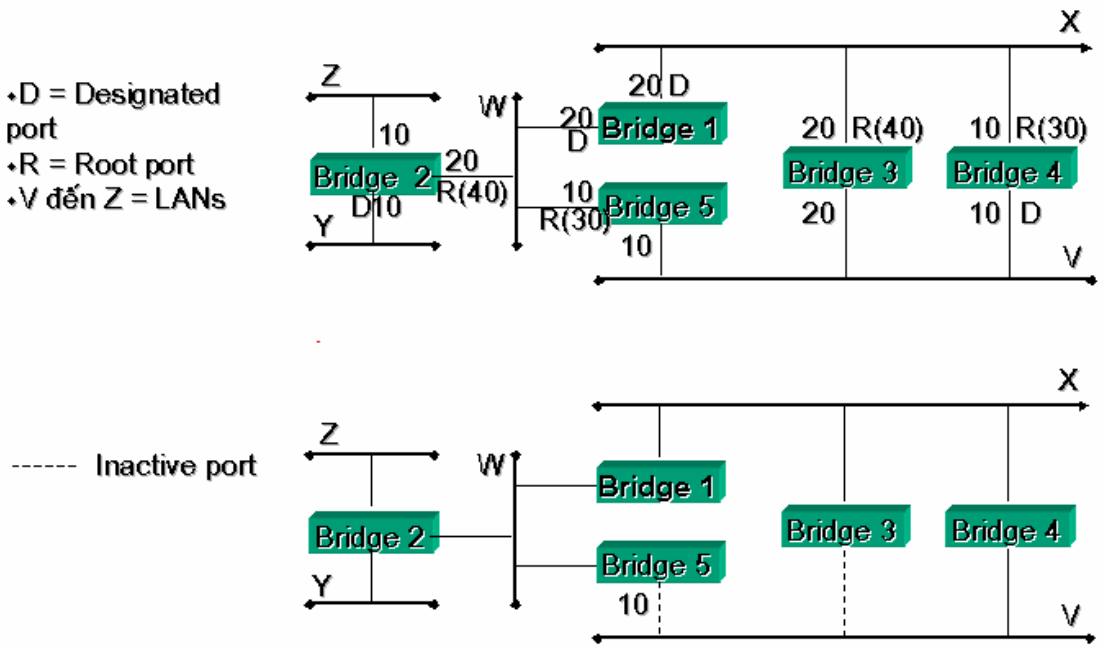
Giải thuật này dựa trên lý thuyết về đồ thị. Giải thuật yêu cầu các vấn đề sau:

- Mỗi cầu nối phải được gán một số hiệu nhận dạng duy nhất.
- Mỗi cổng cũng có một số nhận dạng duy nhất và được gán một giá.

Giải thuật trải qua 4 bước sau:

- Chọn cầu nối gốc (Root Bridge): Để đơn giản cầu nối gốc là cầu nối có số nhận dạng nhỏ nhất.
- Trên các cầu nối còn lại, chọn cổng gốc (Root Port): Là cổng mà giá đường đi từ cầu nối hiện tại về cầu nối gốc thông qua nó là thấp nhất so với các cổng còn lại.
- Trên mỗi LAN, chọn cầu nối được chỉ định (Designated BrIDge): Cầu nối được chỉ định của một LAN là cầu nối mà thông qua nó, giá đường đi từ LAN hiện tại về gốc là thấp nhất. Cổng nối LAN và cầu nối được chỉ định được gọi là cổng được chỉ định (Designated Port).
- Đặt tất cả các cổng gốc, cổng chỉ định ở trạng thái hoạt động, các cổng còn lại ở trạng thái khóa

Ví dụ: Cho một liên mạng gồm các LAN V,W,X,Y,Z được nối lại với nhau bằng 5 cầu nối có số nhận dạng từ 1 đến 5. Trên liên mạng này tồn tại nhiều vòng quẩn. Áp dụng giải thuật nối cây xác định được các cổng gốc (ký hiệu bằng R) và các cổng được chỉ định (Ký hiệu bằng D). Bên cạnh các cổng gốc có cả giá về gốc thông qua cổng này (nằm trong dấu ngoặc R(30)). Từ đó vẽ lại hình trạng mạng sau khi đã loại bỏ các vòng quẩn.



Hình 3.5 – Mạng xây dựng lại bằng giải thuật Spanning tree

3.2.2 Cầu nối xác định đường đi từ nguồn

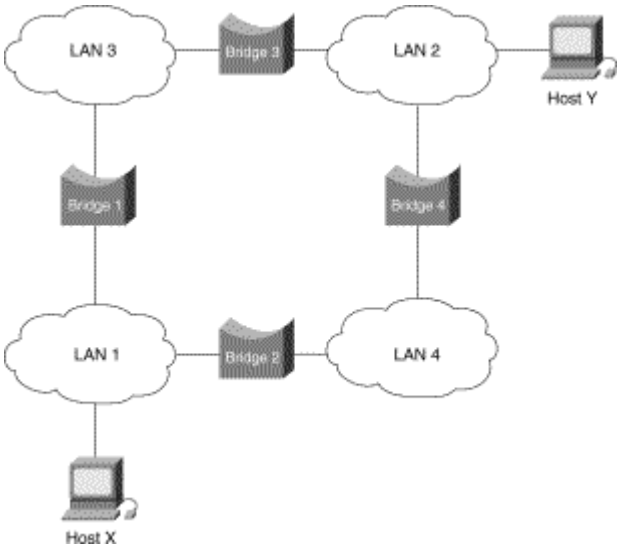
3.2.2.1 Giới thiệu

Cầu nối xác định đường đi từ nguồn (SRB-Source Route Bridge) được phát triển bởi IBM và được đệ trình lên ủy ban IEEE 802.5 như là một giải pháp để nối các mạng Token lại với nhau.

Cầu nối SRB được gọi tên như thế bởi vì chúng qui định rằng : đường đi đầy đủ từ máy tính gởi đến máy nhận phải được đưa vào bên trong của khung dữ liệu gởi đi bởi máy gởi (Source). Các cầu nối SRB chỉ có nhiệm vụ lưu và chuyển các khung như đã được chỉ dẫn bởi đường đi được lưu trong trong khung.

3.2.2.2 Nguyên lý hoạt động

Xét một liên mạng gồm 4 mạng Token Ring được nối lại với nhau bằng 4 cầu nối SRB như hình dưới đây:



Hình 3.6 – Cầu nối trong mạng Token Ring

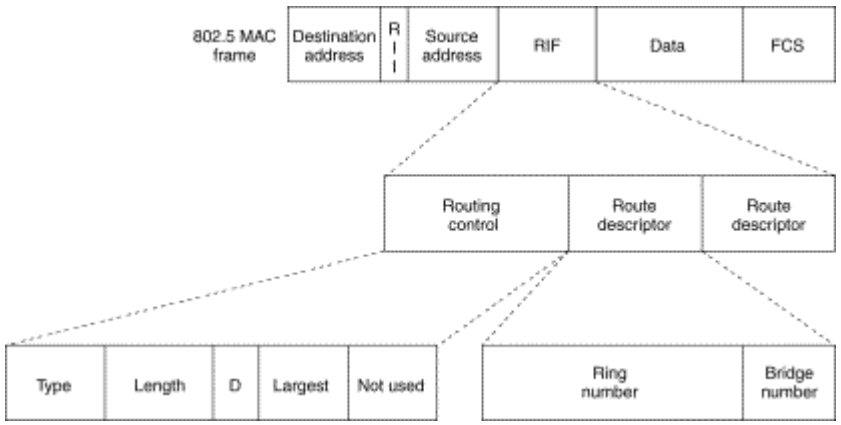
Giả sử rằng máy X muốn gởi một khung dữ liệu cho máy Y. Đầu tiên X chưa biết được Y có nằm cùng LAN với nó hay không. Để xác định điều này, X gởi một **Khung kiểm tra** (Test Frame). Nếu khung kiểm tra trở về X mà không có dấu hiệu đã nhận của Y, X sẽ kết luận rằng Y nằm trên một nhánh mạng khác.

Để xác định chính xác vị trí của máy Y trên mạng ở xa, X gởi một **Khung thăm dò** (Explorer Frame). Mỗi cầu nối khi nhận được khung thăm dò (Bridge 1 và Bridge 2 trong trường hợp này) sẽ copy khung và chuyển nó sang tất cả các cổng còn lại. Thông tin về đường đi được thêm vào khung thăm dò khi chúng đi qua liên mạng. Khi các khung thăm dò của X đến được Y, Y gởi lại các khung trả lời cho từng khung mà nó nhận được theo đường đi đã thu thập được trong khung thăm dò. X nhận được nhiều khung trả lời từ Y với nhiều đường đi khác nhau. X sẽ chọn một trong số đường đi này, theo một tiêu chuẩn nào đó. Thông thường đường đi của khung trả lời đầu tiên sẽ được chọn vì đây chính là đường đi ngắn nhất trong số các đường đi (trở về nhanh nhất).

Sau khi đường đi đã được xác định, nó được đưa vào các khung dữ liệu gởi cho Y trong trường thông tin về đường đi (RIF- Routing Information Field). RIF chỉ được sử dụng đến đối với các khung gởi ra bên ngoài LAN.

3.2.2.3 Cấu trúc khung

Cấu trúc của RIF trong khung được mô tả như hình dưới đây:



Hình 3.7 Cấu trúc của trường thông tin về đường đi

Trong đó:

- **Routing Control Field**: là trường điều khiển đường đi, nó bao gồm các trường con sau:
  - **Type**: Có thể có các giá trị mang ý nghĩa như sau:
    - **Specifically routed:** Khung hiện tại có chứa đường đi đầy đủ đến máy nhận
    - **All paths explorer**: Là khung thăm dò.
    - **Spanning-tree explorer:** Là khung thăm dò có sử dụng giải thuật nối cây để giảm bớt số khung được gởi trong suốt quá trình khám phá.
  - **Length:** Mô tả chiều dài tổng cộng (tính bằng bytes) của trường RIF.
  - **D Bit:** Chỉ định và điều khiển hướng di chuyển (tới hay lui) của khung.

- **Largest Frame:** Chỉ định kích thước lớn nhất của khung mà nó có thể được xử lý trên tiến trình đi đến một đích.

- **Routing Designator Fields:**

Là các trường chứa các Bộ chỉ định đường đi. Mỗi bộ chỉ định đường đi bao gồm 2 trường con là:

- **Ring Number (12 bits):** Là số hiệu nhận dạng của một LAN.
- **Bridge Number (4 bits)**—Là số hiệu nhận dạng của cầu nối. Sẽ là 0 nếu đó là máy tính đích.

Ví dụ: Đường đi từ X đến Y sẽ được mô tả bởi các bộ chỉ định đường đi như sau:

LAN1:Bridge1:LAN 3: Bridge 3: LAN 2: 0

Hay: LAN1:Bridge2:LAN 4: Bridge 4: LAN 2: 0

3.2.3 Cầu nối trộn lẫn (Mixed Media Bridge)

Cầu nối trong suốt được dùng để nối các mạng Ethernet lại với nhau. Cầu nối xác định đường đi từ nguồn dùng để nối các mạng Token Ring. Để nối hai mạng Ethernet và Token Ring lại với nhau, người ta dùng loại cầu nối thứ ba, đó là cầu nối trộn lẫn đường truyền. Cầu nối trộn lẫn đường truyền có hai loại:

- Cầu nối dịch (Translational Bridge)
- Cầu nối xác định đường đi từ nguồn trong suốt (Source-Route-Transparence Bridge)

Chương 4

Cơ sở về bộ chuyển mạch

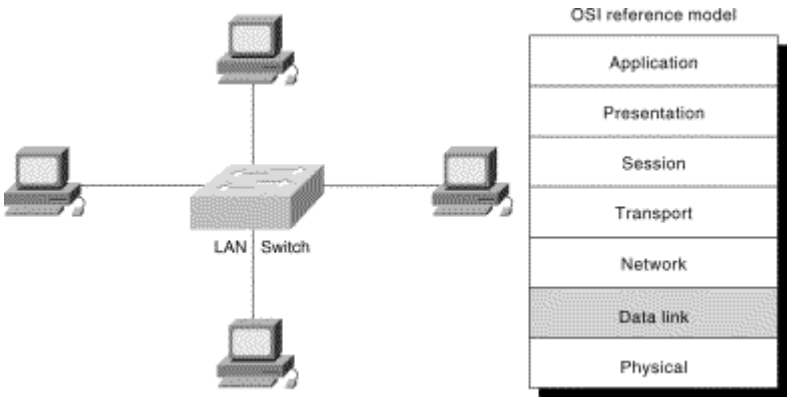
Mục đích

Chương này nhằm giới thiệu cho người đọc những vấn đề sau :

- Chức năng của bộ hoán chuyển (Switch) trong việc mở rộng băng thông mạng cục bộ
- Kiến trúc bộ hoán chuyển
- Các giải thuật hoán chuyển:
    - Store and forward
    - Cut-through
    - Adaptive
- Phân loại bộ hoán chuyển:
    - Workgroup, Segment, Backbone
    - Symetric / Asymetric

4.1 Chức năng và đặc tính mới của switch

LAN Switch là một thiết bị hoạt động ở tầng 2, có đầy đủ tất cả các tính năng của một cầu nối trong suốt như:

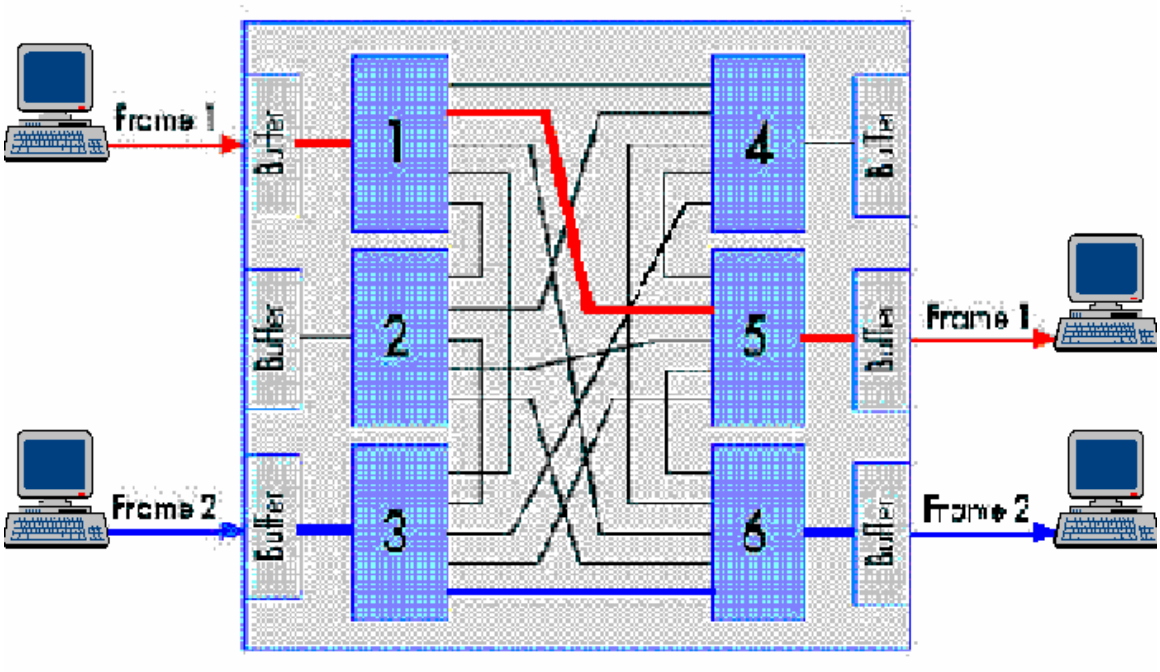


Hình 4.1 – Nối mạng bằng switch

- Học vị trí các máy tính trên mạng
- Chuyển tiếp khung từ nhánh mạng này sang nhánh mạng khác một cách có chọn lọc

Ngoài ra Switch còn hỗ trợ thêm nhiều tính năng mới như:

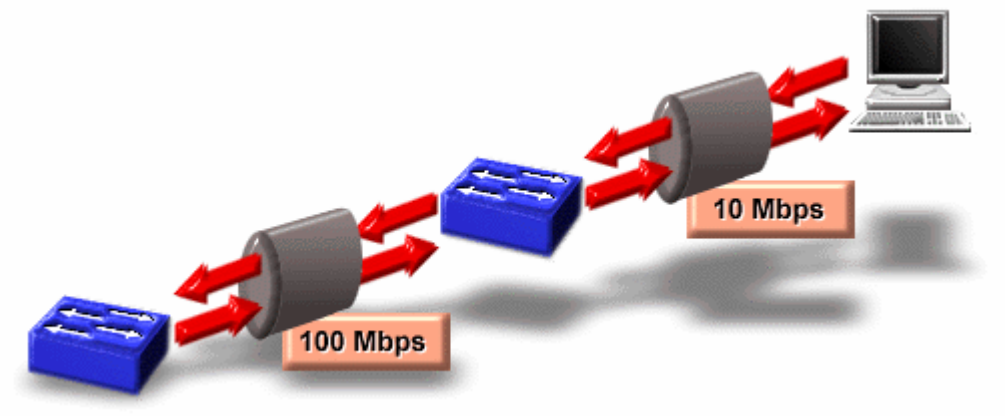
- Hỗ trợ đa giao tiếp đồng thời: Cho phép nhiều cặp giao tiếp diễn ra một cách đồng thời nhờ đó tăng được băng thông trên toàn mạng.



Hình 4.2 - Switch hỗ trợ đa giao tiếp đồng thời

- Hỗ trợ giao tiếp song công (Full-duplex communication): Tiến trình gởi khung và nhận khung có thể xảy ra đồng thời trên một cổng. Điều này làm tăng gấp đôi thông lượng tổng của cổng.

- Điều hòa tốc độ kênh truyền: Cho phép các kênh truyền có tốc độ khác nhau giao tiếp được với nhau. Ví dụ, có thể hoán chuyển dữ liệu giữa một kênh truyền 10 Mbps và một kênh truyền 100 Mbps.

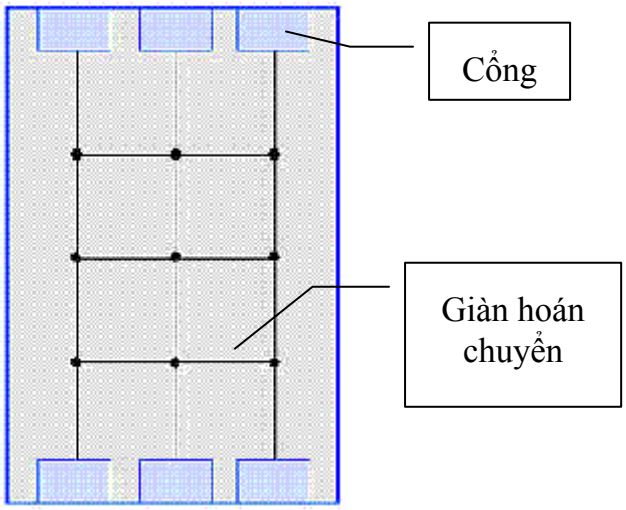


Hình 4.3 – Switch hỗ trợ chế độ giao tiếp song công

4.2 Kiến trúc của switch

Switch được cấu tạo gồm hai thành phần cơ bản là:

- Bộ nhớ làm Vùng đệm tính toán và Bảng địa chỉ (BAT-Buffer anh Address Table).
- Giàn hoán chuyển (Switching Fabric) để tạo nối kết chéo đồng thời giữa các cổng



Hình 4.4 – Cấu trúc bên trong của switch

4.3 Các giải thuật hoán chuyển

Việc chuyển tiếp khung từ nhánh mạng này sang nhánh mạng kia của switch có thể được thực hiện theo một trong 3 giải thuật hoán chuyển sau:

4.3.1 Giải thuật hoán chuyển lưu và chuyển tiếp (Store and Forward Switching)

Khi khung đến một cổng của switch, toàn bộ khung sẽ được đọc vào trong bộ nhớ đệm và được kiểm tra lỗi. Khung sẽ bị bỏ đi nếu như có lỗi. Nếu khung không lỗi, switch sẽ xác định địa chỉ máy nhận khung và dò tìm trong bảng địa chỉ để xác định cổng hướng đến máy nhận. Kế tiếp sẽ chuyển tiếp khung ra cổng tương ứng. Giải thuật này có thời gian trì hoãn lớn do phải thực hiện thao tác kiểm tra khung. Tuy nhiên nó cho phép giao tiếp giữa hai kênh truyền khác tốc độ.

4.3.2 Giải thuật xuyên cắt (Cut-through)

Khi khung đến một cổng của switch, nó chỉ đọc 6 bytes đầu tiên của khung (là địa chỉ MAC của máy nhận khung) vào bộ nhớ đệm. Kế tiếp nó sẽ tìm trong bảng địa chỉ để xác định cổng ra tương ứng với địa chỉ máy nhận và chuyển khung về hướng cổng này.

Giải thuật cut-through có thời gian trì hoãn ngắn bởi vì nó thực hiện việc hoán chuyển khung ngay sau khi xác định được cổng hướng đến máy nhận. Tuy nhiên nó chuyển tiếp luôn cả các khung bị lỗi đến máy nhận.

4.3.3 Hoán chuyển tương thích (Adaptive – Switching)

Giải thuật hoán chuyển tương thích nhằm tận dụng tối đa ưu điểm của hai giải thuật hoán chuyển Lưu và chuyển tiếp và giải thuật Xuyên cắt. Trong giải thuật này, người ta định nghĩa một ngưỡng lỗi cho phép. Đầu tiên, switch sẽ hoạt động theo giải thuật Xuyên cắt. Nếu tỉ lệ khung lỗi lớn hơn ngưỡng cho phép, switch sẽ chuyển sang chế độ hoạt động theo giải thuật Lưu và chuyển tiếp. Ngược lại khi tỷ lệ khung lỗi hạ xuống nhỏ hơn ngưỡng, switch lại chuyển về hoạt động theo giải thuật Xuyên cắt.

4.4 Thông lượng tổng (Aggregate throughput)

Thông lượng tổng (Aggregate throughput) là một đại lượng dùng để đo hiệu suất của switch. Nó được định nghĩa là lượng dữ liệu chuyển qua switch trong một giây. Nó có thể được tính bằng tích giữa số nối kết tối đa đồng thời trong một giây nhân với băng thông của từng nối kết. Như vậy, thông lượng tổng của một switch có N cổng sử dụng, mỗi cổng có băng thông là B được tính theo công thức sau:

Aggregate throughput = (N div 2) * (B*2) = N*B

Ví dụ: Cho một mạng gồm 10 máy tính được nối lại với nhau bằng một switch có các cổng 10 Base-T. Khi đó, số nối kết tối đa đồng thời là 10/2. Mỗi cặp nối kết trong một giây có thể gởi và nhận dữ liệu với lưu lượng là 10Mbps*2 (do Full duplex). Như vậy thông lượng tổng sẽ là: 10/2*10*2 = 100 Mbps

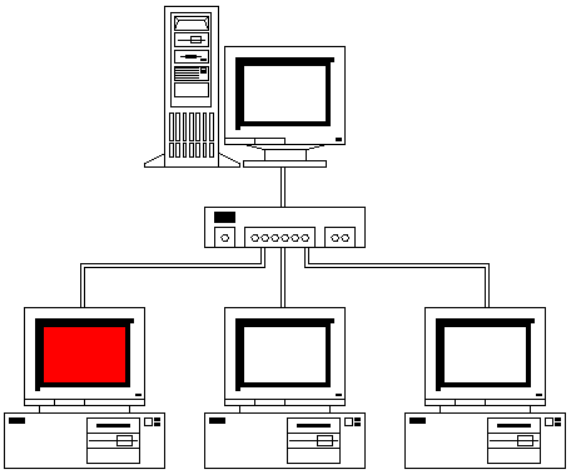
4.5 Phân biệt các loại Switch

Dựa vào mục đích sử dụng, người ta có thể chia switch thành những loại sau:

4.5.1 Bộ hoán chuyển nhóm làm việc (Workgroup Switch)

Là loại switch được thiết kế nhằm để nối trực tiếp các máy tính lại với nhau hình thành một mạng ngang hàng (workgroup) . Như vậy, tương ứng với một cổng của switch chỉ có một địa chỉ máy tính trong bảng địa chỉ. Chính vì thế, loại này không cần thiết phải

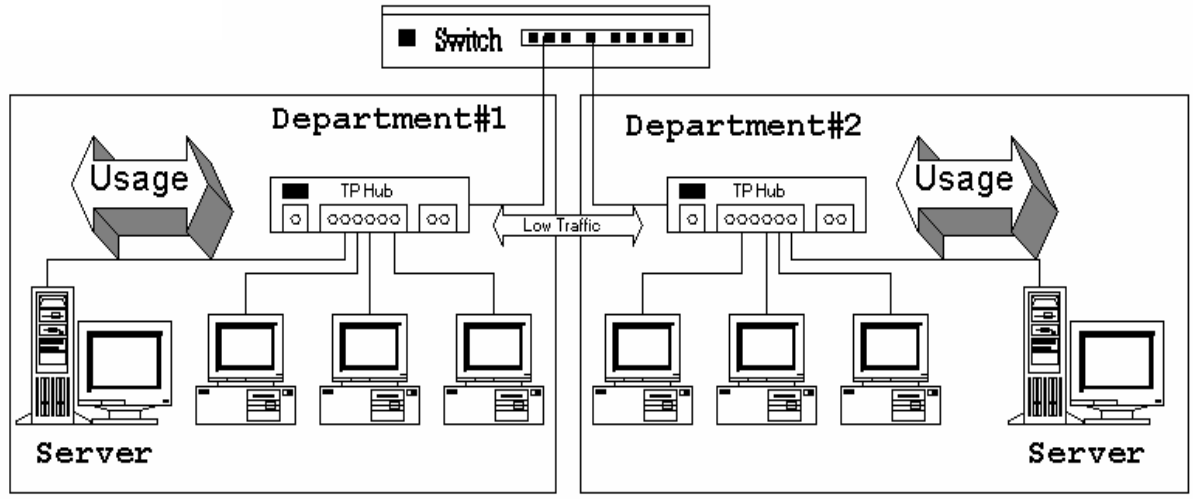
có bộ nhớ lớn cũng như tốc độ xử lý cao. Giá thành workgroup switch thấp hơn các loại còn lại.



Hình 4.5 – Workgroup switch

4.5.2 Bộ hoán chuyển nhánh mạng (Segment Switch)

Mục đích thiết kế của Segment switch là nối các Hub hay workgroup switch lại với nhau, hình thành một liên mạng ở tầng hai. Tương ứng với mỗi cổng trong trường hợp này sẽ có nhiều địa chỉ máy tính, vì thế bộ nhớ cần thiết phải đủ lớn. Tốc độ xử lý đòi hỏi phải cao vì lượng thông tin cần xử lý tại switch là lớn.

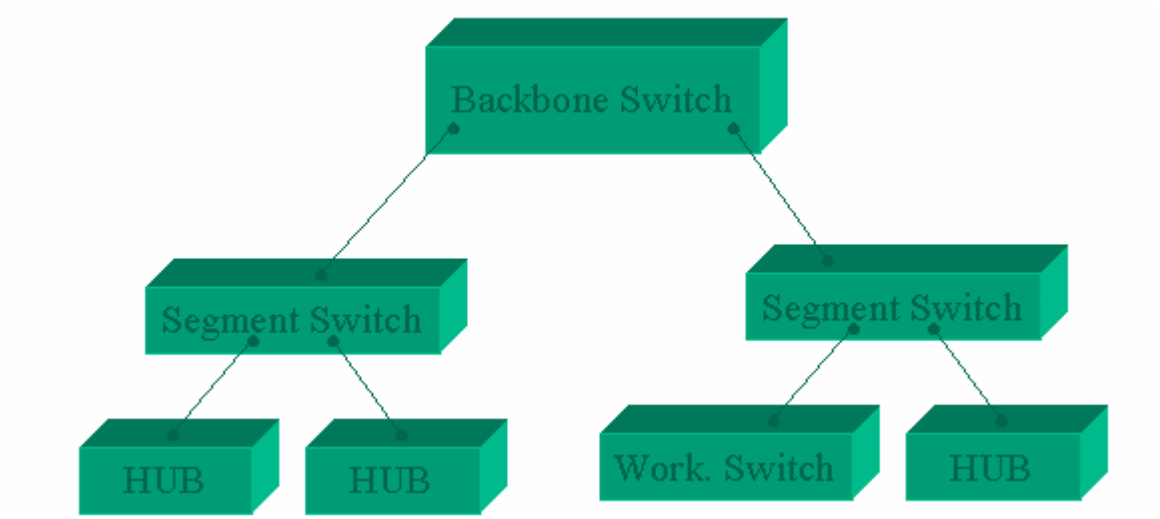


Hình 4.6 – Segment switch

4.5.3 Bộ hoán chuyển xương sống (Backbone Switch)

Mục đích thiết kế của Backbone switch là để nối kết các Segment switch lại với nhau. Trong trường hợp này, bộ nhớ và tốc độ xử lý của switch phải rất lớn để đủ chứa địa

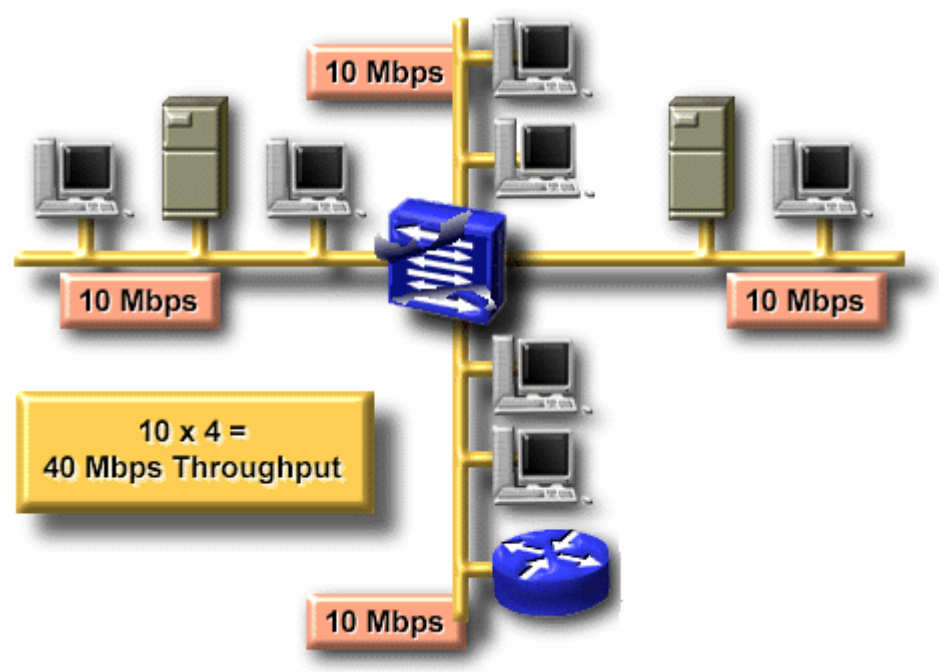
chỉ cho tất cả các máy tính trong toàn liên mạng cũng như hoán chuyển kịp thời dữ liệu giữa các nhánh.



Hình 4.7 – Backbone switch

4.5.4 Bộ hoán chuyển đối xứng (Symetric Switch)

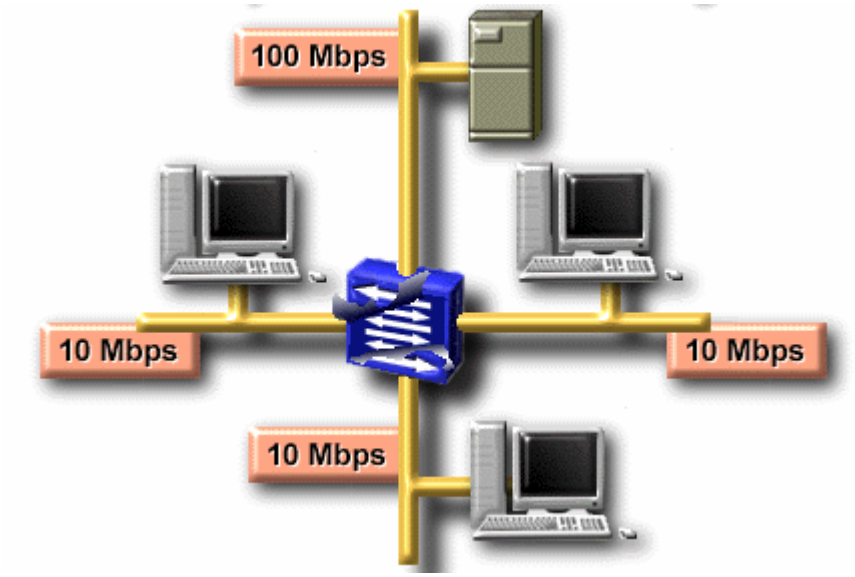
Symetric switch là loại switch mà tất cả các cổng của nó đều có cùng tốc độ. Thông thường workgroup switch thuộc loại này. Nhu cầu băng thông giữa các máy tính là gần bằng nhau.



Hình 4.8 – Symetric switch

4.5.5 Bộ hoán chuyển bất đối xứng (Asymetric Switch)

Asymetric switch là loại switch có một hoặc hai cổng có tốc độ cao hơn so với các cổng còn lại của nó. Thông thường các cổng này được thiết kế để dành cho các máy chủ hay là cổng để nối lên một switch ở mức cao hơn.



Hình 4.8 – Asymetric switch

Chương 5

Cơ sở về bộ chọn đường

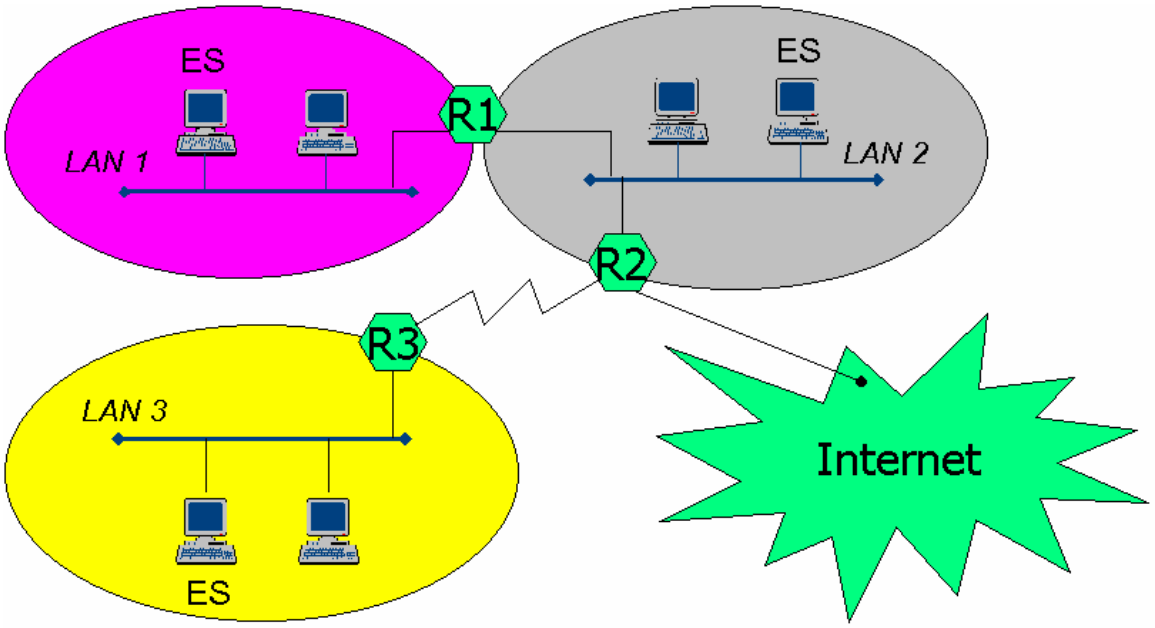
Mục đích

Chương này nhằm giới thiệu cho người đọc những vấn đề sau :

- Các vấn đề liên quan đến việc xây dựng mạng diện rộng
- Vai trò của bộ chọn đường (Router) trong mạng diện rộng
- Nguyên tắc hoạt động của bộ chọn đường
- Các vấn đề liên quan đến việc thiết kế giải thuật chọn đường
- Cách thức thiết lập mạng IP
- Các giao thức chọn đường phổ biến: RIP, OSPF, BGP

5.1 Mô tả

Bridge và switch là các thiết bị nối mạng ở tầng hai. Switch cho phép liên kết nhiều mạng cục bộ lại với nhau thành một liên mạng với băng thông và hiệu suất mạng được cải thiện rất tốt. Nhiệm vụ của switch là chuyển tiếp các khung từ nhánh mạng này sang nhánh mạng khác một cách có chọn lọc dựa vào địa chỉ MAC của các máy tính. Để làm được điều này, switch cần phải duy trì trong bộ nhớ của mình một bảng địa chỉ cục bộ chứa vị trí của tất cả các máy tính trong mạng. Mỗi máy tính sẽ chiếm một mục từ trong bảng địa chỉ. Mỗi switch được thiết kế với một dung lượng bộ nhớ giới hạn. Và như thế, nó xác định khả năng phục vụ tối đa của một switch. Chúng ta không thể dùng switch để nối quá nhiều mạng lại với nhau. Hơn nữa, các liên mạng hình thành bằng cách sử dụng switch cũng chỉ là các mạng cục bộ, có phạm vi nhỏ. Muốn hình thành các mạng diện rộng ta cần sử dụng thiết bị liên mạng ở tầng 3. Đó chính là bộ chọn đường (Router).



Hình 5.1 – Xây dựng liên mạng bằng router

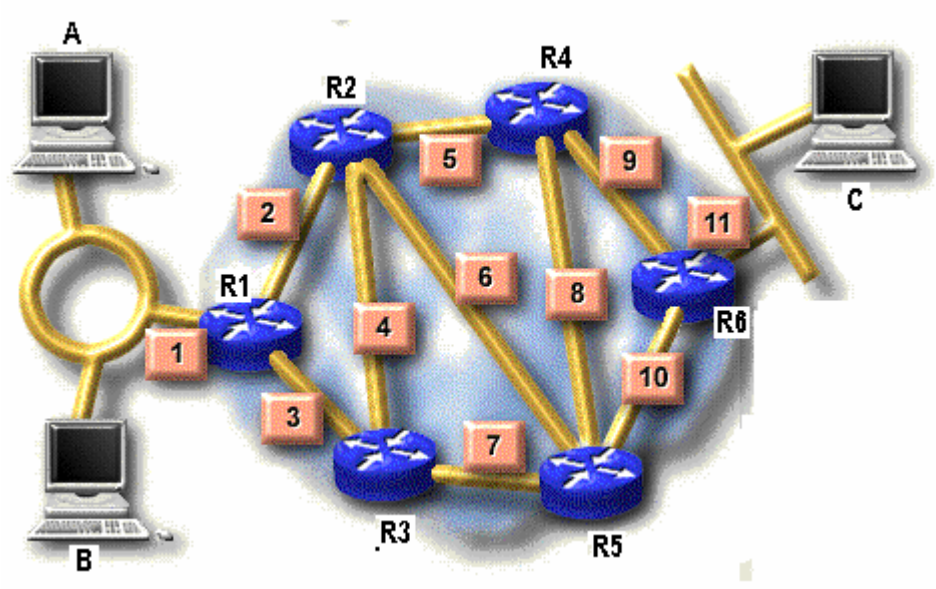
Trong mô hình trên, các mạng LAN 1, LAN 2, LAN 3 và mạng Internet được nối lại với nhau bằng 3 router R1, R2 và R3.

Router là một thiết bị liên mạng ở tầng 3, cho phép nối hai hay nhiều nhánh mạng lại với nhau để tạo thành một liên mạng. Nhiệm vụ của router là chuyển tiếp các gói tin từ mạng này đến mạng kia để có thể đến được máy nhận. Mỗi một router thường tham gia vào ít nhất là 2 mạng. Nó có thể là một thiết bị chuyên dùng với hình dáng giống như Hub hay switch hoặc có thể là một máy tính với nhiều card mạng và một phần mềm cài đặt giải thuật chọn đường. Các đầu nối kết (cổng) của các router được gọi là các Giao diện (Interface).

Các máy tính trong mạng diện rộng được gọi là các Hệ thống cuối (End System), với ý nghĩa đây chính là nơi xuất phát của thông tin lưu thông trên mạng, cũng như là điểm dừng của thông tin.

Về mặt kiến trúc, các router chỉ cài đặt các thành phần thực hiện các chức năng từ tầng 1 đến tầng 3 trong mô hình OSI. Trong khi các End System thì cài đặt chức năng của cả bảy tầng. .

5.2 Chức năng của bộ chọn đường



Hình 5.2 – Nhiều đường đi cho một đích đến

Trong một mạng diện rộng, thường có nhiều đường đi khác nhau cho cùng một đích đến. Ta xét trường hợp A gởi cho C một gói tin. Gói tin được chuyển đến router R1, và được lưu vào trong hàng đợi các gói tin chờ được chuyển đi của R1. Khi một gói tin trong hàng đợi đến lượt được xử lý, router sẽ xác định đích đến của gói tin, từ đó tìm ra router kế tiếp cần chuyển gói tin đến để có thể đi đến đích. Đối với Router 1, có hai đường đi, một nối đến router R2 và một nối đến R3. Khi đã chọn được đường đi cho gói tin, router R1 sẽ chuyển gói tin từ hàng đợi ra đường đã chọn. Một quá trình tương tự cũng xảy ra trên Router kế tiếp. Cứ như thế, gói tin sẽ được chuyển từ router này đến router khác cho đến khi nó đến được mạng có chứa máy tính nhận và sẽ được nhận bởi máy tính nhận.

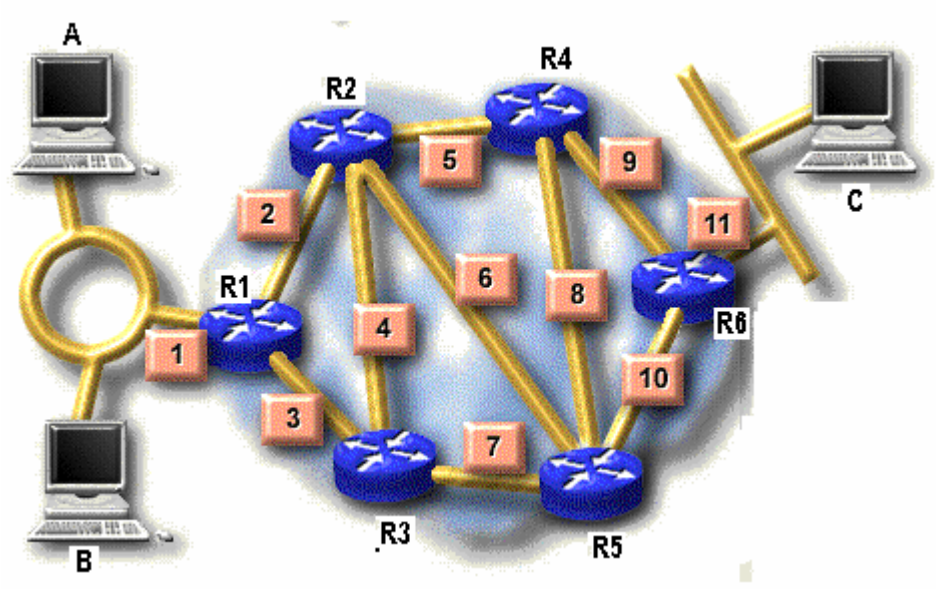
Như vậy, hai chức năng chính mà một bộ chọn đường phải thực hiện là:

- Chọn đường đi đến đích với 'chi phí' (metric) thấp nhất cho một gói tin.
- Lưu và chuyển tiếp các gói tin từ nhánh mạng này sang nhánh mạng khác.

5.3 Nguyên tắc hoạt động của bộ chọn đường

5.3.1 Bảng chọn đường (Routing table)

Để xác định được đường đi đến đích cho các gói tin, các router duy trì một Bảng chọn đường (Routing table) chứa đường đi đến những điểm khác nhau trên toàn mạng. Hai trường quan trọng nhất trong bảng chọn đường của router là Đích đến (Destination) và Bước kế tiếp (Next Hop) cần phải chuyển gói tin để có thể đến được Đích đến.



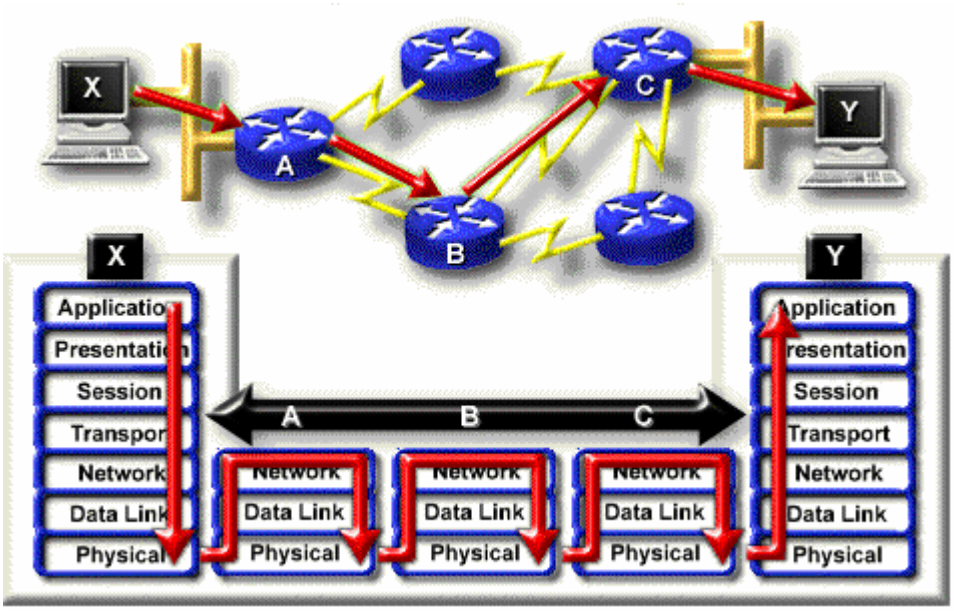
R1 - Routing Table	
Destination	Next Hop
1	Local
2	Local
3	Local
4	R2
5	R2
7	R3
11	R2

Hình 5.3 – Bảng chọn đường của router R1

Thông thường, đích đến trong bảng chọn đường là địa chỉ của các mạng. Trong khi Next Hop là một router láng giềng của router đang xét. Hai router được gọi là láng giềng của nhau nếu tồn tại một đường nối kết vật lý giữa chúng. Thông tin có thể chuyển tải bằng tầng hai giữa hai router láng giềng. Trong mô hình mạng ở trên, router R1 có hai láng giềng là R2 và R3.

5.3.2 Nguyên tắc hoạt động

Cho hệ thống mạng như hình dưới đây :



Hình 5.4- Đường đi của một gói tin qua liên mạng

Giả sử máy tính X gởi cho máy tính Y một gói tin. Con đường đi của gói tin được mô tả như sau:

- Vì Y nằm trên một mạng khác với X cho nên gói tin sẽ được chuyển đến router A.
- Tại router A:
  - Tầng mạng đọc địa chỉ máy nhận để xác định địa chỉ của mạng đích có chứa máy nhận và kế tiếp sẽ tìm trong bảng chọn đường để biết được next hop cần phải gởi đi là đâu. Trong trường hợp này là Router B.
  - Gói tin sau đó được đưa xuống tầng 2 để đóng vào trong một khung và đưa ra hàng đợi của giao diện/cổng hướng đến next hop và chờ được chuyển đi trên đường truyền vật lý.
- Tiến trình tương tự diễn ra tại router B và C.
- Tại Router C, khung của tầng 2 sẽ chuyển gói tin đến máy tính Y.

5.3.3 Vấn đề cập nhật bảng chọn đường

Quyết định chọn đường của router được thực hiện dựa trên thông tin về đường đi đi trong bảng chọn đường. Vấn đề đặt ra là bằng cách nào router có được thông tin trong bảng chọn đường. Hoặc khi mạng bị thay đổi thì ai sẽ là người cập nhật lại bảng chọn đường cho router. Hai vấn đề này gọi chung là vấn đề cập nhật bảng chọn đường.

Có ba hình thức cập nhật bảng chọn đường:

- Cập nhật thủ công: Thông tin trong bảng chọn đường được cập nhật bởi nhà quản trị mạng. Hình thức này chỉ phù hợp với các mạng nhỏ, có hình trạng đơn giản, ít bị thay đổi. Nhược điểm của loại này là không cập nhật kịp thời bảng chọn đường khi hình trạng mạng bị thay đổi do gặp sự cố về đường truyền.
- Cập nhật tự động: Tồn tại một chương trình chạy bên trong router tự động tìm kiếm đường đi đến những điểm khác nhau trên mạng. Loại này thích hợp

cho các mạng lớn, hình trạng phức tạp, có thể ứng phó kịp thời với những thay đổi về hình trạng mạng. Vấn đề đặt ra đối với cập nhật bảng chọn đường động chính là giải thuật được dùng để tìm ra đường đi đến những điểm khác nhau trên mạng. Người ta gọi giải thuật này là giải thuật chọn đường (Routing Algorithme).

- Cập nhật hỗn hợp: Vừa kết hợp cả hai phương pháp cập nhật bảng chọn đường thủ công và cập nhật bảng chọn đường tự động. Đầu tiên, nhà quản trị cung cấp cho router một số đường đi cơ bản, sau đó giải thuật chọn đường sẽ giúp router tìm ra các đường đi mới đến các điểm còn lại trên mạng.

5.4 Giải thuật chọn đường

5.4.1 Chức năng của giải thuật vạch đường

Chức năng của giải thuật chọn đường là tìm ra đường đi đến những điểm khác nhau trên mạng. Giải thuật chọn đường chỉ cập nhật vào bảng chọn đường một đường đi đến một đích đến mới hoặc đường đi mới tốt hơn đường đi đã có trong bảng chọn đường.

5.4.2 Đại lượng đo lường (Metric)

Một đường đi tốt là một đường đi «ngắn ». Khái niệm « dài », « ngắn » ở đây không thuần túy là khoảng cách địa lý mà chúng được đo dựa vào một thước đo (metric) nào đó. Có thể dùng các thước đo sau để đo độ dài đường đi cho các giải thuật chọn đường:

- Chiều dài đường đi (length path): Là số lượng router phải đi qua trên đường đi.
- Độ tin cậy (reliable) của đường truyền
- Độ trì hoãn (delay) của đường truyền
- Băng thông (bandwidth) kênh truyền
- Tải (load) của các router
- Cước phí (cost) kênh truyền

Cùng một đích đến nhưng đo với hai tiêu chuẩn khác nhau có thể sẽ chọn được hai đường đi khác nhau.

Mỗi giải thuật chọn đường phải xác định rõ tiêu chuẩn chọn lựa đường đi mà mình sử dụng là gì. Có thể chỉ là một thước đo hoặc là sự phối hợp của nhiều tiêu chuẩn lại với nhau.

5.4.3 Mục đích thiết kế

Chức năng chính của giải thuật chọn đường là tìm ra được đường đi đến những điểm khác nhau trên mạng. Tuy nhiên, tùy vào mục tiêu khi thiết kế giải thuật chọn đường sẽ dẫn đến chất lượng về đường đi sẽ khác nhau. Các giải thuật chọn đường có thể được thiết kế cho các mục tiêu sau:

- Tối ưu (optimality): Đường đi do giải thuật tìm được phải là đường đi tối ưu trong số các đường đi đến một đích đến nào đó
- Đơn giản, ít tốn kém (Simplicity and overhead): Giải thuật được thiết kế hiệu quả về mặt xử lý, ít đòi hỏi về mặt tài nguyên như bộ nhớ, tốc độ xử lý của router.

- Tính ổn định (stability): Giải thuật có khả năng ứng phó được với các sự cố về đường truyền.
- Hội tụ nhanh (rapid convergence): Quá trình thống nhất giữa các router về một đường đi tốt phải nhanh chóng.
- Tính linh hoạt (Flexibility): Đáp ứng được mọi thay đổi về môi trường vận hành của giải thuật như băng thông, kích bộ nhớ, độ trì hoãn của đường truyền

5.4.4. Phân loại giải thuật chọn đường

Thông thường các giải thuật chọn đường được phân loại bằng các tiêu chuẩn có tính chất đối ngẫu nhau, ví dụ như:

- Giải thuật chọn đường tĩnh - Giải thuật chọn đường động
- Giải thuật chọn đường bên trong - Giải thuật chọn đường bên ngoài khu vực
- Giải thuật chọn đường trạng thái nối kết - Giải thuật véctơ khoảng cách.

5.4.4.1 Giải thuật chọn đường tĩnh - Giải thuật chọn đường động

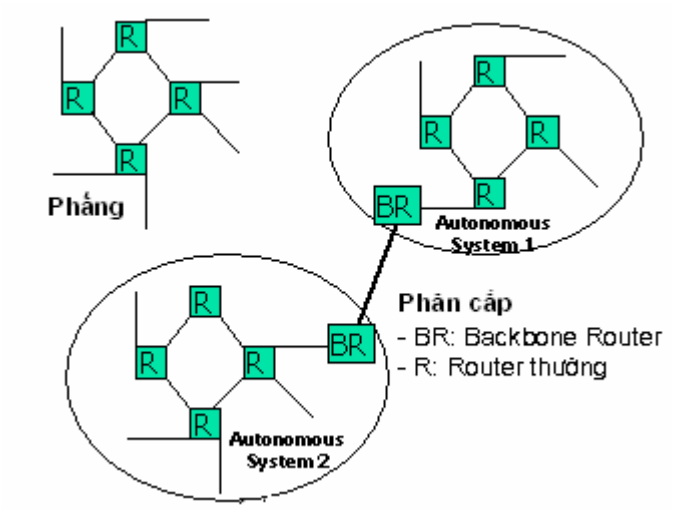
- Giải thuật chọn đường tĩnh (static routing): Bảng chọn đường được cập nhật bởi nhà quản trị mạng. Hình thức này chỉ phù hợp cho các mạng nhỏ, có hình trạng đơn giản, ít bị thay đổi. Nhược điểm của loại này là không cập nhật kịp thời bảng chọn đường khi hình trạng mạng bị thay đổi do gặp sự cố về đường truyền.
- Giải thuật chọn đường động (dynamic routing): Router tự động tìm kiếm đường đi đến những điểm khác nhau trên mạng. Loại này thích hợp cho các mạng lớn, hình trạng phức tạp. Nó có thể ứng phó kịp thời với những thay đổi về hình trạng mạng

5.4.4.2 Giải thuật chọn đường một đường - Giải thuật chọn đường nhiều đường

- Giải thuật chọn đường một đường (single path): Tồn tại một đường đi đến một đích đến trong bảng chọn đường.
- Giải thuật chọn đường nhiều đường (multi path): Hỗ trợ nhiều đường đi đến cùng một đích đến, nhờ đó tăng được thông lượng và độ tin cậy trên mạng.

5.4.4.3 Giải thuật chọn đường bên trong khu vực - Giải thuật chọn đường liên khu vực

Một số giải thuật chọn đường xem các router đều cùng một cấp. Các router có vai trò ngang bằng nhau. Người ta gọi là giải thuật chọn đường phẳng (Flat routing).



Hình 5.5 – Mạng cấu trúc phẳng và mạng phân cấp

Tuy nhiên, trong các mạng lớn người ta thường xây dựng mạng theo kiểu phân cấp. Ở đó các máy tính lại nhóm lại với nhau thành những vùng tự trị (Autonomous System) và có sự phân cấp các router. Các router bình thường (Normal Router) đảm nhiệm việc vạch đường bên trong một Autonomous System. Công việc vạch đường giữa các autonomous system thì được giao về cho các router nằm ở đường trục (Backbone router).

Một autonomous system là một tập hợp các mạng và các router chịu sự quản lý duy nhất của một nhà quản trị mạng. Ví dụ là mạng của một công ty, một trường đại học hay mạng đường trục của một quốc gia.

Việc phân cấp các router thành hai loại dẫn đến có hai loại giải thuật chọn đường: Giải thuật chọn đường bên trong vùng (Intradomain hay Interior Protocol) và liên vùng (Interdomain hay Exterior protocol).

Ví dụ:

- Một số giải thuật chọn đường bên trong vùng:
  - RIP: Routing Information Protocol
  - OSPF: Open Shortest Path First
  - IGRP: Interior Gateway Routing Protocol
- Một số giải thuật chọn đường liên vùng:
  - EGP: Exterior Gateway Protocol
  - BGP: Boder Gateway Protocol

5.4.4.4 Giải thuật chọn đường theo kiểu trạng thái nối kết (Link State Routing) và Giải thuật chọn đường theo kiểu vector khoảng cách (Distance vector)

- Trong giải thuật vạch đường theo kiểu trạng thái nối kết
  - Mỗi router sẽ gởi thông tin về trạng thái nối kết của mình (các mạng nối kết trực tiếp và các router láng giềng) cho tất cả các router trên toàn mạng. Các router sẽ thu thập thông tin về trạng thái nối kết của các router khác, từ đó xây dựng lại hình trạng mạng, chạy các giải thuật tìm đường đi ngắn nhất trên hình trạng mạng có được. Từ đó xây dựng bảng chọn đường cho mình.

- Khi một router phát hiện trạng thái nối kết của mình bị thay đổi, nó sẽ gởi một thông điệp yêu cầu cập nhật trạng thái nối kết cho tất các các router trên toàn mạng. Nhận được thông điệp này, các router sẽ xây dựng lại hình trạng mạng, tính toán lại đường đi tối ưu và cập nhật lại bảng chọn đường của mình.
- Giải thuật chọn đường trạng thái nối kết tạo ra ít thông tin trên mạng. Tuy nhiên nó đòi hỏi router phải có bộ nhớ lớn, tốc độ tính toán của CPU phải cao.

- Trong giải thuật chọn đường theo kiểu vectơ khoảng cách:
  - Đầu tiên mỗi router sẽ cập nhật đường đi đến các mạng nối kết trực tiếp với mình vào bảng chọn đường.
  - Theo định kỳ, một router phải gởi bảng chọn đường của mình cho các router láng giềng.
  - Khi nhận được bảng chọn đường của một láng giềng gởi sang, router sẽ tìm xem láng giềng của mình có đường đi đến một mạng nào mà mình chưa có hay một đường đi nào tốt hơn đường đi mình đã có hay không. Nếu có sẽ đưa đường đi mới này vào bảng chọn đường của mình với Next hop để đến đích chính là láng giềng này.

5.5 Thiết kế liên mạng với giao thức IP

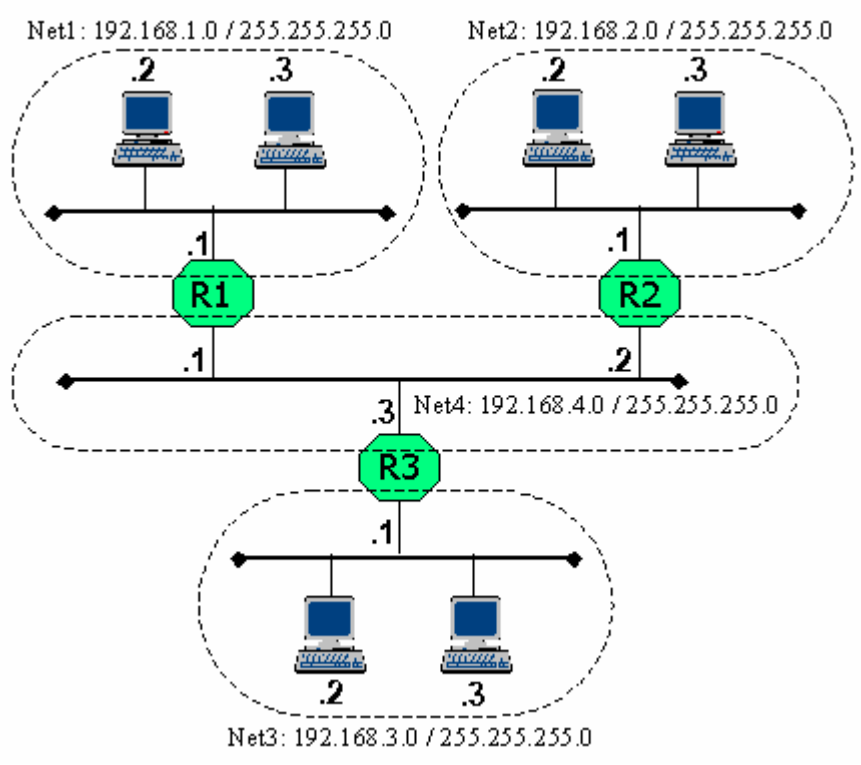
5.5.1 Xây dựng bảng chọn đường

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 một liên mạng IP là chọn địa chỉ mạng cho các nhánh mạng. Trong trường hợp này ta chọn mạng lớp C cho 4 mạng như bảng sau:

Mạng	**Địa chỉ mạng**	**Mặt nạ mạng**
Net1	192.168.1.0	255.255.255.0
Net2	192.168.2.0	255.255.255.0
Net3	192.168.3.0	255.255.255.0
Net4	192.168.4.0	255.255.255.0

Hình 5.6 – Cấu trúc bảng chọn đường trong giao thức IP

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 IP là 192.168.1.1 và giao diện tham gia vào mạng NET4 có địa chỉ là 192.168.4.1.



Hình 5.7 – 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	192.168.4.3
192.168.3.0/255.255.255.0	local	local
192.168.4.0/255.255.255.0	local	local

Hình 5.8 – Bảng chọn đường của các router

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

Hình 5.9 – Bảng chọn đường của máy tính

Mạng đích mặc định (default) ý nói rằng ngoài những đường đi đến các mạng đã liệt kê phía trên, các đường đi còn lại thì gởi cho NextHop của mạng default này. Như vậy, để gởi 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.

5.5.2 Đường đi của gói tin

Để hiểu rõ có chế hoạt động của giao thức IP, ta hãy xét hai trường hợp gởi gói tin: Trường hợp máy tính gởi và nhận nằm trong cùng một mạng và trường hợp máy tính gởi 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 gởi sẽ đặt gói tin vào một khung với địa chỉ nhận là địa chỉ vật lý của máy 192.168.3.2 và gởi khung lên đường truyền NET3, trên đó máy tính 192.168.3.2 sẽ nhận được gói tin.

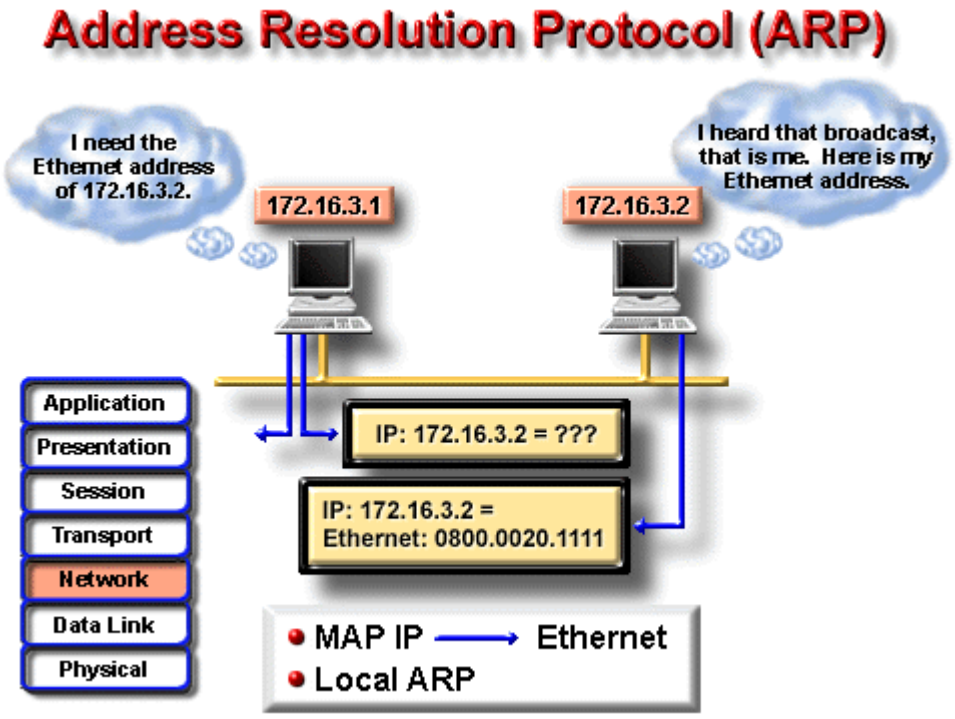
Bây giờ ta xét trường hợp máy tính có địa chỉ 192.168.3.3 trên mạng NET3 gởi gói tin cho máy tính có địa chỉ 192.168.1.2 trên mạng Net1. Theo như bảng chọn đường của máy gởi, các gói tin có địa chỉ nằm ngoài mạng 192.168.3.0 sẽ được chuyển đến router R3 (địa chỉ 192.168.3.1). Chính vì thế, máy tính gởi 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.

5.5.3 Giao thức phân giải địa chỉ (Address Resolution Protocol)

Nếu một máy tính muốn truyền một gói tin IP nó cần đặt gói tin này vào trong một khung trên đường truyền vật lý mà nó đang nối kết. Để có thể truyền thành công khung, máy tính gởi 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 5.10 – 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 địa chỉ của 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	Địa chỉ IP máy cần tìm địa chỉ MAC

Nếu một máy tính trên mạng nhận ra địa chỉ IP của mình trong gói tin yêu cầu ARP nó sẽ gởi một gói tin trả lời ARP cho máy yêu cầu trong đó có thông tin về địa chỉ MAC của nó.

Nhờ vào việc gởi 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 các 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 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 gởi sẽ được chuyển hướng cho một router nằm cùng mạng với máy gởi 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 yêu cầu được quảng bá này để lấy thông tin về địa chỉ vật lý và địa chỉ IP của máy gởi yêu cầu và bổ sung vào vùng cache của nó khi cần thiết. Khi một máy tính khởi động, nó gởi 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.

5.5.4 Giao 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 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 máy chủ 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, máy chủ tìm trong bảng địa chỉ và trả về địa chỉ IP tương ứng cho máy trạm đã gởi yêu cầu.

5.5.5 Giao thức thông điệp điều khiển mạng 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 gởi 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, được tạo ra 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 gởi và máy nhận có thể giao tiếp được với nhau.

Một thông điệp « Chuyển hướng » được gởi bởi một router đến máy đã gởi 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 gởi 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.

5.5.6 Giao thức chọn đường RIP (Routing Information Protocol)

5.5.6.1 Giới thiệu

RIP là giải thuật chọn đường động theo kiểu véctơ khoảng cách. RIP được định nghĩa trong hai tài liệu là RFC 1058 và Internet Standard 56 và được cập nhật bởi IETF – (Internet Engineering Task Force). Phiên bản thứ 2 của RIP được định nghĩa trong RFC 1723 vào tháng 10 năm 1994. RIP 2 cho phép các thông điệp của RIP mang nhiều thông tin hơn để sử dụng cơ chế chứng thực đơn giản đảm bảo tính bảo mật khi cập nhật bảng chọn đường. Quan trọng nhất là RIP 2 hỗ trợ mặt nạ mạng con, tính năng thiếu trong RIP ban đầu.

5.5.6.2 Vấn đề cập nhật đường đi (Routing Update)

RIP gởi các Thông điệp cập nhật chọn đường (routing-update messages) định kỳ và khi hình trạng mạng bị thay đổi. Khi một router nhận được một Thông điệp cập nhật chọn đường có chứa những thay đổi trong một mục từ, nó sẽ cập nhật bảng chọn đường của nó

để thể hiện đường đi mới. Độ dài đường đi mới sẽ được tăng lên 1 và router gởi trở thành next hop của đường đi vừa cập nhật. Khi cập nhật xong bảng chọn đường của mình, router sẽ gởi ngay thông điệp cập nhật chọn đường cho các router láng giềng khác trên mạng.

5.5.6.3 Thước đo đường đi của RIP

RIP sử dụng một thước đo đường đi là số lượng mạng trung gian (hop count) giữa mạng gởi và mạng nhận gói tin. Mỗi hop trên đường đi từ nơi gởi đến nơi nhận được gán một giá trị, thông thường là 1. Khi một router nhận một thông điệp cập nhật chọn đường có chứa một mạng đích mới, hay đường đi mới, router cộng thêm 1 vào giá của đường đi này và đưa vào bảng chọn đường của nó với next hop là địa chỉ IP của router vừa gởi.

5.5.6.4 Tính ổn định của RIP

RIP đề phòng trường hợp vạch đường lòng vòng bằng cách giới hạn số hop tối đa từ máy gởi đến máy nhận là 15. Nếu một router nhận được một đường đi mới từ láng giềng gởi sang, sau khi cộng 1 vào giá của đường đi thì nó lên đến 16 thì xem như đích đến này không đến được. Điều này có nghĩa là giới hạn đường kính mạng sử dụng RIP phải nhỏ hơn 16 router.

5.5.6.5 Bộ đếm thời gian của RIP (RIP Timer)

RIP sử dụng một bộ đếm thời gian số để điều hòa hiệu năng của nó. Nó bao gồm một Bộ đếm thời gian cập nhật chọn đường (routing-update timer), một Bộ đếm thời gian quá hạn (route-timeout timer) và một Bộ đếm thời gian xóa đường đi (route-flush timer). Bộ đếm thời gian cập nhật chọn đường theo dõi khoảng thời gian định kỳ cập nhật chọn đường, thông thường là 30 giây. Mỗi mục từ trong bảng chọn đường có một bộ đếm thời gian quá hạn gán với nó. Nếu thời gian này trôi qua, đường đi tương ứng được đánh dấu là không còn đúng nữa, tuy nhiên nó vẫn được giữa lại trong bảng chọn đường cho đến khi bộ đếm thời gian xóa đường đi quá hạn.

5.5.6.6 Định dạng gói tin RIP

Gói tin của RIP gồm có chín trường như hình sau:

1-octet command field	1-octet version number field	2-octet zero field	2-octet AFI field	2-octet zero field	4-octet IP address field	4-octet zero field	4-octet zero field	4-octet metric field

Trong đó:

- **Command**—Xác định là gói tin yêu cầu hay trả lời. Một gói tin yêu cầu sẽ yêu cầu một router gởi tất cả hay một phần của bảng chọn đường. Một trả lời có thể là một thông điệp cập nhật chọn đường được gởi theo định kỳ hoặc là một trả lời cho một yêu cầu. Thông điệp trả lời chứa các mục từ của bảng chọn đường. Các bảng chọn đường lớn có thể được gởi đi trong nhiều thông điệp.
- **Version number**—Mô tả phiên bản RIP được sử dụng.
- **Zero**—Trường này không được sử dụng bởi RIP theo đặc tả RFC 1058
- **Address-family Identifier (AFI)**—Mô tả họ địa chỉ được sử dụng. Trường này được thiết kế để cho phép RIP dùng với nhiều giao thức khác nhau. Nếu sử dụng giao thức IP, thì có giá trị là 2.

- **Address**—Mô tả địa chỉ IP cho mục từ (đích đến).
- **Metric**—Giá của đường đi
- **Lưu ý:** Có thể cho phép đến 25 thể hiện của các trường AFI, Address và Metric xuất hiện trong cùng một gói tin RIP. Tức có thể mô tả 25 đích đến trong chỉ một gói tin RIP**.**

5.5.6.7 Định dạng của gói tin RIP 2

RIP 2 được mô tả trong RFC 1723 có định dạng gói tin như hình dưới đây:

1-octet command field	1-octet version number field	2-octet unused field	2-octet AFI field	2-octet route tag field	4-octet network address field	4-octet subnet mask field	4-octet next hop field	4-octet metric field

RIP 2 có một số trường mới so với RIP là:

- **Unused**—Có giá trị là 0.
- **Address-family IDentifier (AFI)**—Mô tả họ địa chỉ được sử dụng. Điểm khác so với RIP là, nếu AFI của mục từ đầu tiên trong gói tin có giá trị là 0xFFFF, thì các mục từ còn lại chứa thông tin về chứng thực. Hiện tại chỉ sử dụng phương pháp chứng thực dựa trên mật khẩu đơn giản.
- **Route tag**—Cung cấp một phương thức để phân biệt giữa các đường đi bên trong (RIP học được) và các đường đi bên ngoài (do các giao thức khác học được).
- **IP address**—Địa chỉ IP của đích đến.
- **Subnet mask**—Mặt nạ cho địa chỉ đến. Nếu bằng 0 thì không mô tả mặt nạ.
- **Next hop**—Địa chỉ IP kế tiếp cần chuyển gói tin đi.

Lưu ý, tối đa một gói tin RIP có thể mô tả 24 đường đi, do có 1 mục từ trong gói tin được dùng để mô tả mật khẩu.

5.5.7 Giải thuật vạch đường OSPF

5.5.7.1 Giới thiệu

Giải thuật đường đi ngắn nhất đầu tiên OSPF (*Open Shortest Path First)* được phát triển cho các mạng sử dụng giao thức IP bởi nhóm làm việc cho giao thức IGP (Interior Gateway Protocol) của IETF (Internet Engineering Task Force). Nhóm này được hình thành vào năm 1988 để thiết kế Giao thức bên trong cửa khẩu IGP dựa trên giải thuật tìm đường đi ngắn nhất đầu tiên SPF (Shortest Path First) để sử dụng trong mạng Internet.

OSPF có hai đặc trưng chính. Đặc trưng thứ nhất đó là một giao thức mở, có nghĩa là đặc tả của nó thuộc về phạm vi công cộng. OSPF được đặc tả trong RFC 1247. Đặc trưng thứ hai của OSPF là nó dựa vào giao thức SPF, đôi khi còn gọi là giải thuật Dijkstra.

OSPF là một giao thức vạch đường thuộc loại Trạng thái nối kết, trong đó mỗi router sẽ phải gởi các thông tin quảng cáo về trạng thái LSA (Link-State Advertisements) nối kết của mình cho các router còn lại trong cùng một khu vực (area) của một mạng có cấu trúc thứ bậc. Thông tin về các giao diện được gắn vào, các thước đo được sử dụng và các thông số khác được đưa vào trong các LSA . Mỗi router sẽ thu thập thông tin về trạng thái nối kết của các router khác, từ đó xây dựng lại hình trạng của mạng, và sử dụng giải thuật Dijkstra để tìm đường đi ngắn đến các nút còn lại.

5.5.7.2 Vạch đường phân cấp (Routing Hierarchy).

Không giống như RIP, OSPF có thể vận hành với một cấu trúc phân cấp. Thực thể lớn nhất của cấu trúc này là hệ thống tự trị (AS - Autonomous System), đó là một tập hợp các mạng dưới một sự quản lý chung và cùng chia sẻ một chiến lược vạch đường chung. OSPF là một giao thức vạch đường bên trong miền (Intra Autonomous System hay Interior gateway protocol) mặc dù nó có khả năng khả năng nhận/gởi các đường đi từ/đến các AS khác.

Một AS có thể được phân chia thành một số các khu vực (Area), đó là một nhóm các mạng kề cận nhau (láng giềng) cùng các máy tính trên các mạng đó. Các router với nhiều giao diện có thể tham gia vào nhiều khu vực. Những router này được gọi là Bộ chọn đường đường biên khu vực (Area Border Router), có nhiệm vụ duy trì cơ sở dữ liệu về hình trạng mạng riêng rời cho từng khu vực.

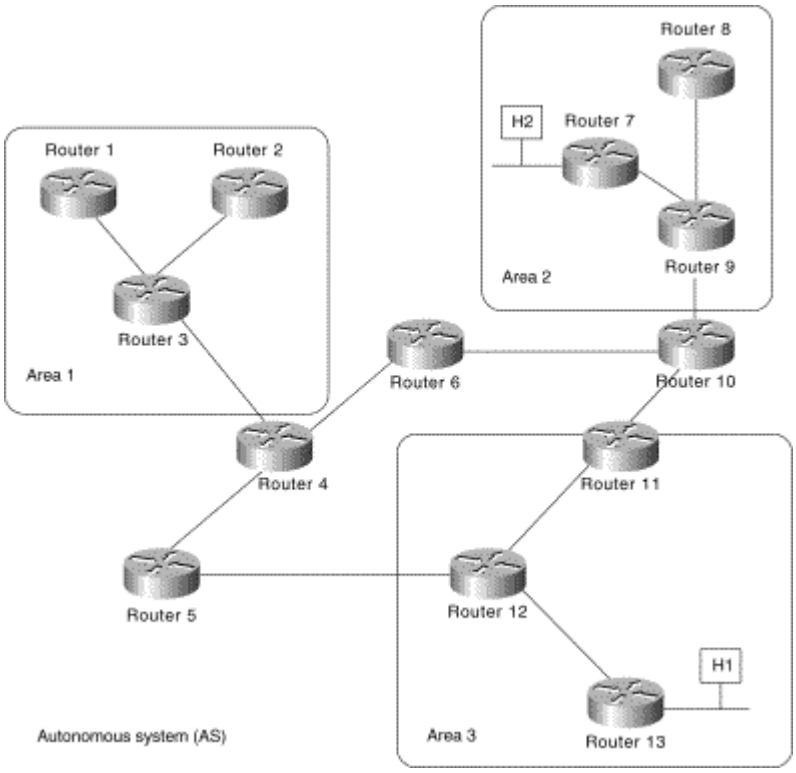
Một cơ sở dữ liệu hình trạng mạng là một bức tranh tổng thể về mạng trong mối quan hệ với các router. Một cơ sở dữ liệu hình trạng mạng lưu giữ một tập hợp các LSA nhận được từ các router trong cùng khu vực. Bởi vì các router trong cùng một khu vực chia sẻ thông tin cho nhau nên chúng có cơ sở dữ liệu hình trạng mạng về khu vực mà chúng đang thuộc về hoàn toàn giống nhau .

Lưu ý: Khái niệm miền (domain) đôi khi được sử dụng để mô tả một phần của mạng mà trong đó tất cả các router có cùng cơ sở dữ liệu hình trạng mạng hoàn toàn giống nhau. Tuy nhiên thông thường Domain được dùng như là một AS.

Hình trạng của một khu vực thì không thấy được đối với các thực thể bên ngoài khu vực. Bằng cách giữ hình trạng mạng phân tách giữa các khu vực, OSPF tạo ra ít giao thông trên mạng hơn so với trường hợp AS không được phân chia khu vực.

Việc phân chia khu vực tạo ra hai kiểu vạch đường khác nhau tùy thuộc vào địa chỉ máy gởi và máy nhận nằm cùng khu vực hay khác khu vực. Vạch đường bên trong khu vực (Intra-Area) sẽ được dùng đến khi địa chỉ nhận và địa chỉ gởi nằm trong cùng một khu vực và Vạch đường liên khu vực sẽ được sử dụng đến khi chúng nằm ở những khu vực khác nhau.

Đường trục của OSPF thì đảm trách việc phân phát thông tin vạch đường giữa các khu vực. Đường trục này bao gồm tất cả các Bộ chọn đường đường biên khu vực, các mạng không thuộc vào các khu vực khác và các router gắn vào chúng.



Hình 5.11 – Kiến trúc mạng phân cấp trong OSPF

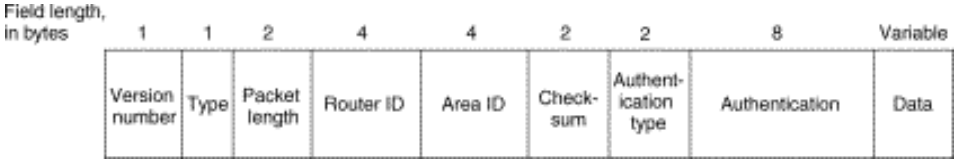
Ví dụ: Trong hình trên, các router 4, 5, 6,10,11 và 12 hình thành nên đường trục. Nếu máy H1 trong khu vực 3 muốn gởi một gói tin cho máy H2 ở khu vực 2, thì gói tin sẽ được gởi đến router R13, đến lược R13 chuyển gói tin sang cho router R12, rồi chuyển tiếp cho R11. Sau đó R11 sẽ chuyển gói tin theo đường trục đến bộ chọn đường đường biên R10 nơi chịu trách nhiệm chuyển gói tin trong khu vực (qua các router R9, R7) và cuối cùng đến được máy nhận H2.

Đường trục cũng là một khu vực OSPF, vì thế tất cả các router nằm trên mạng đường trục cũng sử dụng cùng một thủ tục và giải thuật để lưu trữ thông tin vạch đường trên mạng đường trục. Hình trạng của đường trục thì không thấy được đối với các router nằm bên trong một khu vực.

Các khu vực được định nghĩa theo cách của đường trục có thể không phải là các mạng láng giềng của nhau. Trong trường hợp này, việc kết nối của đường trục phải thực hiện thông qua các đường nối kết ảo (Virtual Link). Đường nối kết ảo được hình thành giữa những router trên đường trục và các khu vực không phải đường trục và vận hành như thể giữa cũng có một đường nối kết trực tiếp.

5.5.7.3 Định dạng gói tin (Packet Format)

Tất cả các gói tin OSPF được bắt đầu với một tiêu đề 24 bytes được mô tả như hình dưới đây



Hình 5.12 – Cấu trúc gói tin OSPF

Ý nghĩa các trường được mô tả như sau:

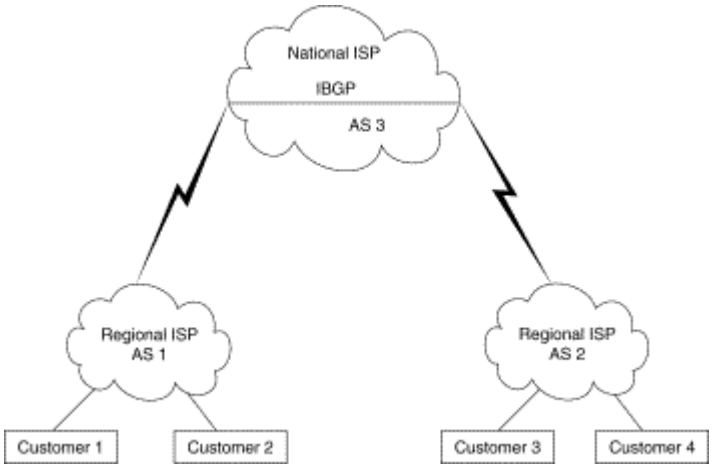
- **Version number—**Nhận dạng phiên bản OSPF được sử dụng.
- **Type**—Nhận dạng kiểu gói tin OSPF, là một trong số các kiểu sau:
  - **Hello**—Thiết lập và duy trì mối quan hệ với các láng giềng.
  - **Database description**—Mô tả nội dung của cơ sở dữ liệu hình trạng mạng. Các thông điệp loại này được trao đổi khi một láng giềng mới xuất hiện.
  - **Link-state request**—Những mẫu yêu cầu về cơ sở dữ liệu hình trạng mạng từ láng giềng. Các thông điệp này được gởi đi sau khi một router phát hiện rằng một phần trong cơ sở dữ liệu hình trạng mạng của nó đã bị lỗi thời không còn đúng thực tế nữa.
  - **Link-state update**—Trả lời cho các link-state request packet. Các thông điệp này cũng được sử dụng cho quá trình phân phát các LSA bình thường..
  - **Link-state acknowledgment**—Báo nhận cho một link-state update packets.
- **Packet length**—Mô tả chiều dài của gói tin, tính luôn cả phần tiêu đề, bằng đơn vị bytes.
- **Router ID**—Nhận dạng của router gởi gói tin.
- **Area ID**—Nhận dạng của khu vực mà gói tin thuộc về.
- **Checksum**—Tổng kiểm tra lỗi của gói tin.
- **Authentication type**—Chứa kiểu chứng thực. Tất cả các thông tin trao đổi trong OSPF phải được chứng thực.
- **Authentication**—Chứa các thông tin chứng thực.
- **Data**—Chứa thông tin của lớp phía trên.

5.5.8 Giải thuật vạch đường BGP (Border Gateway Protocol)

5.5.8.1 Giới thiệu

BGP là giao thức vạch đường liên vùng (inter-autonomous system). BGP được sử dụng để chia sẻ thông tin chọn đường trên mạng Internet và là giao thức được sử dụng để vạch đường giữa những nhà cung cấp dịch vụ Internet. Mạng của các công ty, các trường đại học thường sử dụng các giao thức vạch đường bên trong cửa khẩu (IGP-Interior Gateway Protocol) như RIP hoặc OSPF để trao đổi thông tin chọn đường giữa các mạng của họ. Những khách hàng nối kết đến các ISP và các ISP sử dụng BGP để trao đổi đường đi với họ.

Khi BGP được sử dụng giữa các vùng tự trị, thì giao thức được biết đến như là giao thức BGP bên ngoài BGP (EBGP - External Border Gateway Protocol). Nếu một nhà cung cấp dịch vụ sử dụng BGP để trao đổi giữa các bộ chọn đường bên trong một vùng tự trị thì nó được biết đến như là giao thức BGP bên trong (IBGP - Internal External Border Gateway Protocol).



Hình 5.13 – Phân biệt giữa IBGP và EBGP

BGP là một giao thức chọn đường mạnh và có khả năng mở rộng tốt, vì thế nó được dùng cho mạng Internet. Bảng chọn đường của BGP có thể chứa đến hơn 90.000 đường đi.

Bên cạnh đó, BGP hỗ trợ cơ chế vạch đường liên miền không phân lớp CIDR để giảm kích thước của bảng chọn đường cho mạng Internet. Ví dụ, giả sử rằng một ISP sở hữu khối địa chỉ IP 195.10.x.x từ không gian địa chỉ lớp C của chuẩn phân lớp hoàn toàn. Khối địa chỉ này bao gồm 256 địa chỉ lớp C từ 195.10.0.0 đến 195.10.255.0. Giả sử rằng ISP gán mỗi khách hàng một địa chỉ mạng. Nếu không có CIDR, ISP phải quảng bá 256 địa chỉ này sang các BGP láng giềng. Nếu có CIDR, BGP chỉ cần gởi phần chung của 256 địa chỉ mạng này, 195.10.x.x, sang các BGP láng giềng. Phần chung này chỉ tương ứng chỉ với một địa chỉ IP ở lớp B truyền thống điều này cho phép giảm được kích thước của bảng chọn đường của BGP.

Các láng giềng BGP trao đổi toàn bộ thông tin chọn đường khi nối kết TCP giữa chúng được thiết lập lần đầu tiên. Khi phát hiện hình trạng mạng bị thay đổi, bộ chọn đường BGP sẽ gởi cho các láng giềng của nó những thông tin liên quan đến chỉ những đường đi vừa bị thay đổi. Các bộ chọn đường BGP không gởi định kỳ thông tin cập nhật đường đi và những thông tin cập nhật đường đi chỉ chứa các đường đi tối ưu đến một đích đến.

5.5.8.2 Các thuộc tính của BGP

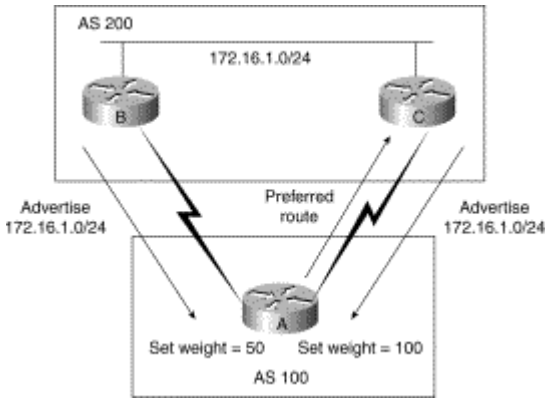
Các đường đi được học bởi BGP có gán các thuộc tính được sử dụng để xác định đường đi tốt nhất đến một đích đến khi tồn tại nhiều đường đi đến đích đến đó. Gồm có các thuộc tính như:

- Trọng lượng (Weight)
- Tham khảo cục bộ (Local preference)
- Multi-exit discriminator
- Origin
- AS_path
- Next hop
- Community

- **Thuộc tính trọng lượng (Weight Attribute)**

Trọng lượng là một thuộc tính được định nghĩa bởi Cisco, nó có tính chất cục bộ đối với một router. Nếu một router biết được nhiều hơn một đường đi đến một đích đến thì đường có trọng lượng lớn nhất sẽ được tham khảo đến.

Trong sơ đồ dưới đây, Router A nhận một thông báo về 172.16.1.0 từ các router B và C. Khi A nhận được thông báo từ B, trọng lượng của đường đi được đặt là 50. Khi A nhận được thông báo từ C, trọng lượng đường đi được đặt là 100. Cả hai đường đi đến mạng 172.16.1.0 đều được lưu trong bảng chọn đường BGP cùng với trọng lượng tương ứng. Đường đi có trọng lượng lớn nhất sẽ được cài đặt vào bảng chọn đường của giao thức IP.

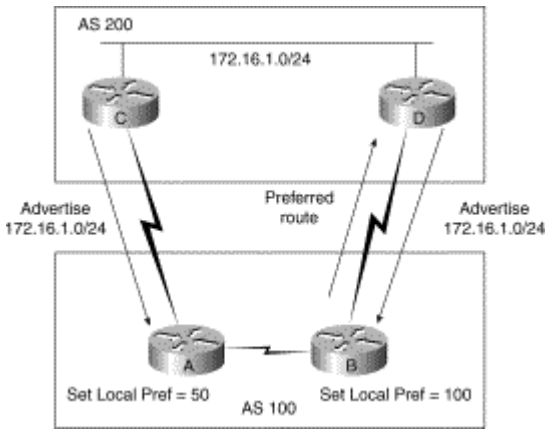


Hình 5.14 – Sử dụng thuộc tính weight trong BGP

- **Thuộc tính tham khảo cục bộ (Local Preference Attribute)**

Thuộc tính tham khảo cục bộ được sử dụng để tham khảo đến một lối thoát (exit) từ hệ thống tự trị cục bộ. Không giống như thuộc tính trọng lượng, các thuộc tính tham khảo cục bộ được lan truyền trên tất cả các router của hệ thống tự trị cục bộ. Nếu có nhiều lối thoát từ hệ thống tự trị, thuộc tính tham khảo cục bộ được dùng để gán lối thoát cho một đường đi xác định.

Như hình phía dưới, AS 100 nhận được 2 thông tin cập nhật đường đi cho mạng 172.16.1.0 từ AS 200. Khi Router A nhận thông tin cập nhật đường đi cho mạng 172.16.1.0, thuộc tính tham khảo cục bộ tương ứng sẽ được đặt là 50. Khi Router B nhận thông tin cập nhật đường đi cho mạng 172.16.1.0, thuộc tính tham khảo cục bộ tương ứng sẽ được đặt là 100. Các giá trị tham khảo cục bộ này sẽ được trao đổi giữa các router A và B. Bởi vì Router B có số tham khảo cao hơn của Router A, nên router B sẽ được sử dụng như là lối thoát ra ngoài AS 100 để đến được mạng 172.16.1.0 trong AS 200.

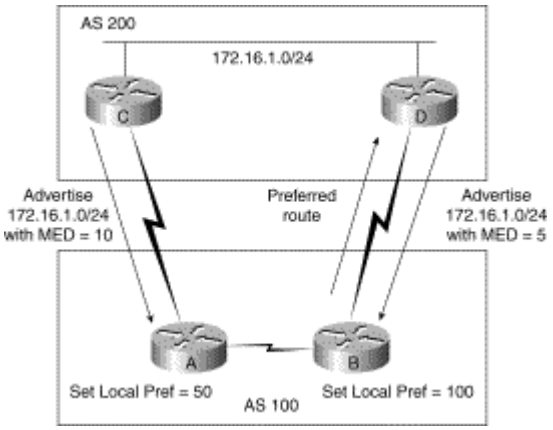


Hình 5.15 – Sử dụng thuộc tính Local Preference trong BGP

- **Bộ chọn lựa đa lối thoát (Multi-Exit Discriminator Attribute)**

Bộ chọn lựa đa lối thoát (MED - Multi-Exit Discriminator) hay còn gọi là thuộc tính thước đo (metric attribute) được sử dụng như là một lời đề nghị đối cho một AS bên ngoài hãy tham khảo đến những thước đo về các đường đi đang được gởi đến. Thuật *ngữ đề nghị* được sử dụng bởi vì AS bên ngoài đang nhận MED có thể sử dụng các thuộc tính khác để chọn đường đi so với AS gởi thông tin cập nhật đường đi.

Ví dụ: Như hình 5.16, Router C đang quảng bá đường đi đến mạng 172.16.1.0 với metric là 10, trong khi Router D thì đang quảng bá đường đi đến mạng 172.16.1.0 với metric là 5. Giá trị thấp hơn của metric sẽ được tham khảo đến vì thế AS 100 sẽ chọn router D để đi đến mạng 172.16.1.0 trong AS 200. Và các MED sẽ được quảng bá trong toàn AS 100.



Hình 5.16 – Sử dụng thuộc tính Multi-Exit Discriminator trong BGP

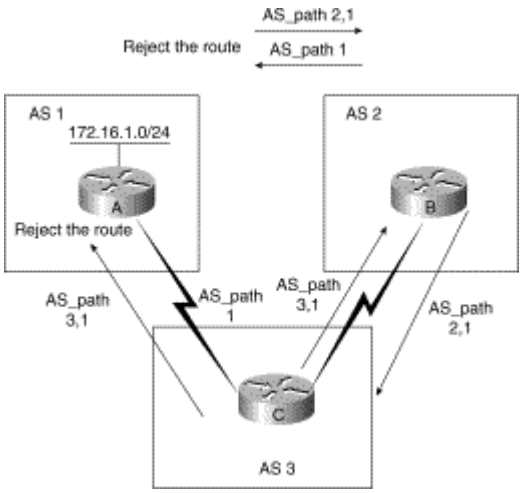
- **Thuộc tính gốc (Origin Attribute)**

Thuộc tính gốc thể hiện cách thức mà BGP đã học một đường đi đặc biệt. Thuộc tính gốc có thể có một trong ba giá trị sau:

- **IGP:** Đường đi nằm bên trong một AS. Giá trị này được thiết lập bằng lệnh cấu hình cho router của mạng để đưa đường đi vào trong BGP.
- **EGP**: Đường đi được học thông qua giao thức BGP bên ngoài.
- **Incomplete:** Gốc của đường đi thì không được biết hoặc được học bằng một cách thức nào khác. Một gốc không hoàn chỉnh xảy ra khi một đường đi được phân phối lại cho các BGP.

- **Giá trị đường qua hệ thống tự trị (AS_path Attribute)**

Khi một thông tin quảng bá đường đi chuyển qua một hệ thống tự trị, số của hệ thống tự trị được đưa vào trong danh sách có thứ tự các AS mà thông tin quảng bá đường đi này đã đi qua. Hình dưới đây mô tả trường hợp trong đó một đường đi thì được gởi xuyên qua ba hệ thống tự trị.



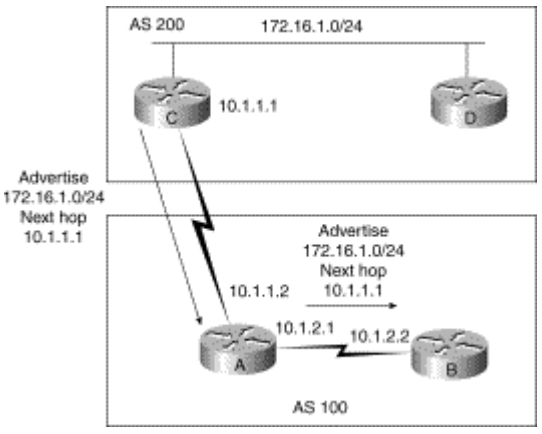
Hình 5.17 – Sử dụng thuộc tính AS_path trong BGP

AS 1 định vị đường đi đến mạng 172.16.1.0 và quảng bá đường đi này đến AS 2 và AS 3 với giá đường đi qua hệ thống tự trị là {1}. AS 3 sẽ quảng bá trở lại AS 1 với giá đường đi qua hệ thống tự trị là {3,1} và AS 2 sẽ quảng bá trở lại AS 1 với giá qua hệ thống tự trị là {2,1}. AS 1 sẽ từ chối các đường đi này khi AS phát hiện ra số hiệu của nó nằm trong thông tin quảng bá đường đi. Đây chính là cơ chế mà BGP sử dụng để phát hiện các vòng quẩn trong đường đi.

AS 2 và AS 3 gởi đường đi đến các AS khác với số hiệu của chúng được đưa vào thuộc tính đường đi qua hệ thống tự trị. Các đường đi này sẽ không được cài vào bảng chọn đường của giao thức IP bởi vì AS 2 và AS 3 đã học một đường đi đến mạng 172.16.1.0 từ AS 1 với một danh sách các hệ thống tự trị là ngắn nhất.

- **Thuộc tính bước kế tiếp (Next-Hop Attribute)**

Giá trị thuộc tính kế tiếp của EBGP là một địa chỉ IP được sử dụng để đến được router đang gởi thông tin quảng bá. Đối với các láng giềng EBGP, địa chỉ bước kế tiếp là địa chỉ IP của nối kết giữa các láng giềng. Đối với IBGP, địa chỉ bước kế của EBGP được đưa vào một AS như minh họa dưới đây:



Hình 5.18 – Sử dụng thuộc tính Next-Hop trong BGP

Router C quảng bá đường đi đến mạng 172.16.1.0 với bước kế tiếp là 10.1.1.1. Khi router A truyền bá đường đi này trong AS của nó, thông tin về bước kế tiếp ra bên ngoài AS hiện tại vẫn được giữ lại. Nếu router B không có thông tin chọn đường liên quan đến

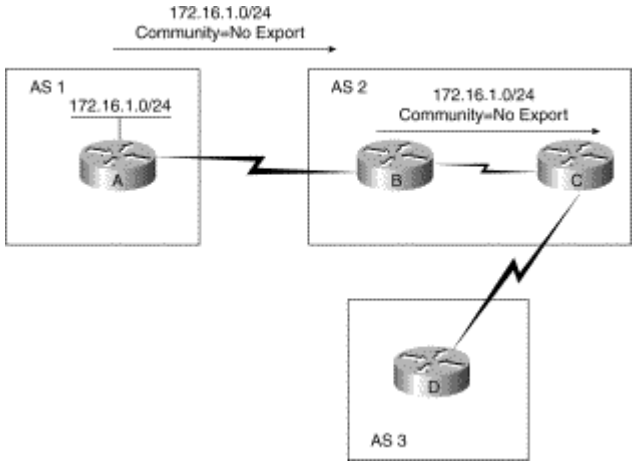
bước kế tiếp này, đường đi sẽ bị hủy bỏ. Chính vì thế, điều quan trọng là cần phải có một IGP vận hành bên trong một AS để truyền tải tiếp thông tin về đường đi đến bước kế tiếp

- Thuộc tính cộng đồng (Community Attribute)

Thuộc tính cộng đồng cung cấp một phương tiện để nhóm các đích đến lại với nhau thành các cộng đồng mà dựa vào đó các quyết định chọn đường được áp dụng. Bản đồ đường đi được sử dụng đối với thuộc tính cộng đồng. Các thuộc tính cộng đồng được định nghĩa trước gồm có:

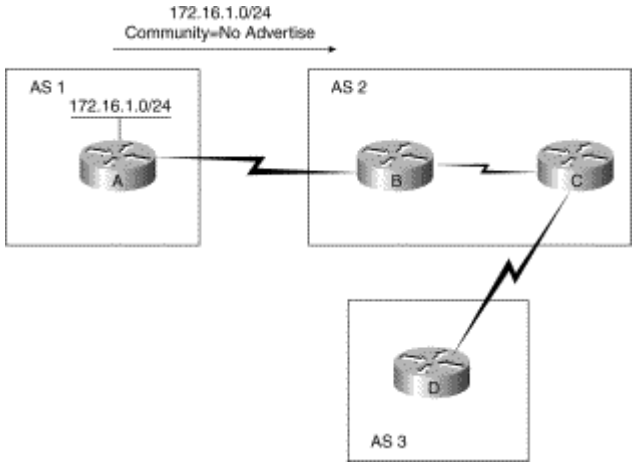
- **no-export:** Không quảng bá đường đi này đến các láng giềng EBGP.
- **no-advertise:** Không quảng bá đường đi này đến bất kỳ láng giềng nào.
- **internet:** Quảng bá đường đi này đến cộng đồng Internet .

Hình dưới đây minh họa cho cộng đồng no-export. AS 1 quảng bá mạng 172.16.1.0 đến AS 2 với thuộc tính cộng đồng no-export. AS 2 sẽ truyền đường đi này trong AS 2 nhưng sẽ không gởi nó đến AS 3 hoặc bất kỳ một AS khác.



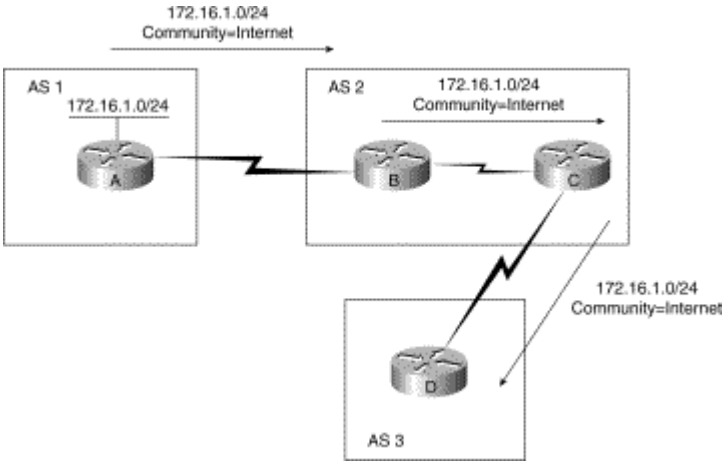
Hình 5.19 – Sử dụng thuộc tính community trong BGP

Hình dưới đây minh họa trường hợp AS1 quảng bá mạng 172.16.1.0 đến AS 2 với thuộc tính cộng đồng là no-advertise. Router B trong AS 2 sẽ không quảng bá thông tin này đến bất kỳ router nào khác.



Hình 5.20 – Sử dụng thuộc tính no-advertise trong BGP

Hình dưới đây minh họa cho thuộc tính cộng đồng Internet. Khi đó sẽ không có giới hạn về các router sẽ nhận được thông tin quảng bá này từ AS 1.



Hình 5.21 – Sử dụng thuộc tính Internet trong BGP

5.5.8.3 Chọn lựa đường đi trong BGP (BGP Path Selection)

Một router BGP có khả năng nhận nhiều thông tin quảng bá đường đi cho cùng một đích đến từ nhiều nguồn khác nhau. BGP chọn lựa một đường đi trong số chúng như là đường đi tốt nhất. Khi một đường đi được chọn, BGP đặt đường đi này vào trong bảng chọn đường của giao thức IP và gởi đường đi này đến các láng giềng của nó. BGP sử dụng các tiêu chuẩn sau, theo thứ tự được liệt kê, để chọn đường đi đến một đích đến nào đó:

- Nếu bước kế tiếp trong đường đi không thể đến được, loại bỏ thông tin cập nhật đường đi này.
- Tham khảo đến các đường đi có trọng lượng lớn nhất.
- Nếu có nhiều đường đi có trọng lượng lớn nhất bằng nhau, đường đi có thuộc tính tham khảo cục bộ lớn nhất sẽ được chọn.
- Nếu các thuộc tính tham khảo cục bộ lại giống nhau, đường đi có gốc là router BGP hiện tại được chọn lựa.
- Nếu không có đường đi với gốc xuất phát là router hiện tại, tham khảo đến đường đi đi qua các AS ngắn nhất.
- Nếu tất cả các đường đi có cùng số AS, tham khảo đến đường đi với kiểu xuất phát nhỏ nhất (Với IGP thì thấp hơn EGP, và EGP thì thấp hơn không hoàn chỉnh).
- Nếu mã của gốc giống nhau, tham khảo đến đường đi có thuộc tính MED thấp nhất..
- Nếu cùng MED, tham khảo đến các đường đi ra bên ngoài hơn là đường đi bên trong.
- Nếu vẫn cùng đường đi thì tham khảo đến các đường đi xuyên qua một IGP láng giềng gần nhất.
- Tham khảo đến đường đi có địa chỉ IP thấp nhất như được đặc tả bởi số hiệu của các router BGP.

Chương 6

Mạng cục bộ ảo (Virtual LAN)

Mục đích

Chương này nhằm giới thiệu cho người đọc những vấn đề sau:

- Vai trò của VLAN
- Vai trò của Swicth trong VLAN
- Lợi ích của VLAN
- Các mô hình cài đặt VLAN: dựa trên cổng, tĩnh, động

6.1 Giới thiệu

Một mạng LAN ảo (VLAN) được định nghĩa như là một vùng quảng bá (broadcast domain) trong một mạng sử dụng switch. Vùng quảng bá là một tập hợp các thiết bị trên mạng mà nó sẽ nhận các khung quảng bá được gởi đi từ một thiết bị trong tập hợp đó. Các vùng quảng bá thường được giới hạn nhờ vào các router, bởi vì các router không chuyển tiếp các khung quảng bá.

Một số switch có hỗ trợ thêm tính năng VLAN nhờ đó có thể định nghĩa một hay nhiều VLAN trong mạng. Khi một switch hỗ trợ nhiều VLAN, khung quảng bá trong một VLAN sẽ không xuất hiện trên các VLAN khác.

Việc định nghĩa các VLAN cho phép nhà quản trị mạng xây dựng các vùng quảng bá với ít người dùng trong một vùng quảng bá hơn. Nhờ đó tăng được băng thông cho người dùng.

Các router cũng duy trì sự tách biệt của các vùng đụng độ bằng cách khóa các khung quảng bá. Vì thế, giao thông giữa các VLAN chỉ được thực hiện thông qua một bộ chọn đường mà thôi.

Thông thường, mỗi mạng con (subnet) thuộc về một VLAN khác nhau. Vì thế, một mạng với nhiều mạng con sẽ có thể có nhiều VLAN. Switch và VLAN cho phép nhà quản trị mạng gán những người dùng vào các vùng quảng bá dựa trên yêu cầu công việc của họ. Điều này cho phép triển khai các mạng với mức độ mềm dẽo cao trong vấn đề quản trị.

Sử dụng VLAN có các lợi ích sau:

- Phân tách các vùng quảng bá để tạo ra nhiều băng thông hơn cho người sử dụng
- Tăng cường tính bảo mật bằng cách cô lập người sử dụng dựa vào kỹ thuật của cầu nối.
- Triển khai mạng một cách mềm dẻo dựa trên chức năng công việc của người dùng hơn là dựa vào vị trí vật lý của họ. VLAN có thể giải quyết những vấn đề liên quan đến việc di chuyển, thêm và thay đổi vị trí các máy tính trên mạng.

6.2 Vai trò của Switch trong VLAN

Switch là một trong những thành phần cốt lõi thực hiện việc truyền thông trong VLAN. Chúng là điểm nối kết các trạm đầu cuối vào giàn hoán chuyển của switch và cho các cuộc giao tiếp diễn ra trên toàn mạng. Switch cung cấp một cơ chế thông minh để nhóm những người dùng, các cổng hoặc các địa chỉ luận lý vào các cộng đồng thích hợp. Switch cung cấp một cơ chế thông minh để thực hiện các quyết định lọc và chuyển tiếp các khung dựa trên các thước đo của VLAN được định nghĩa bởi nhà quản trị.

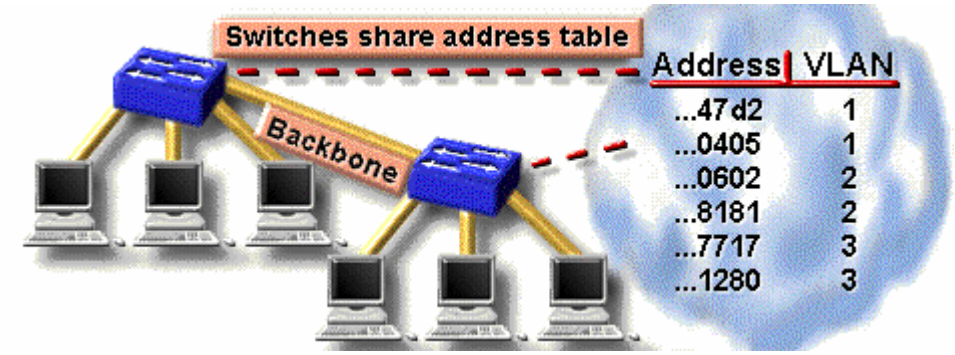
Tiếp cận thông thường nhất để phân nhóm người sử dụng mạng một cách luận lý vào các VLAN riêng biệt là lọc khung (filtering frame) và nhận dạng khung (frame Identification).

Cả hai kỹ thuật trên đều xem xét khung khi nó được nhận hay được chuyển tiếp bởi switch. Dựa vào một tập hợp các luật được định nghĩa bởi nhà quản trị mạng, các kỹ thuật này xác định nơi khung phải được gởi đi (lọc hay là quảng bá). Các cơ chế điều khiển này

được quản trị tập trung (bằng một phần mềm quản trị mạng) và dễ dàng triển khai trên mạng.

6.2.1 Cơ chế lọc khung (Frame Filtering)

Lọc khung là một kỹ thuật mà nó khảo sát các thông tin đặc biệt trên mỗi khung. Ý tưởng của việc lọc khung cũng tương tự như cách thông thường mà các router sử dụng. Một bảng lọc được thiết lập cho mỗi switch để cung cấp một cơ chế điều khiển quản trị ở mức cao. Nó có thể khảo sát nhiều thuộc tính trong mỗi khung. Tùy thuộc vào mức độ phức tạp của switch, bạn có thể nhóm người sử dụng dựa vào địa chỉ MAC của các trạm, kiểu của giao thức ở tầng mạng hay kiểu ứng dụng. Các mục từ trong bảng lọc sẽ được so sánh với các khung cần lọc bởi switch và nhờ đó switch sẽ có các hành động thích hợp.



Hình 6.1 – VLAN sử dụng cơ chế lọc khung

6.2.2 Cơ chế nhận dạng khung (Frame Identification)

Cơ chế nhận dạng khung gán một số nhận dạng duy nhất được định nghĩa bởi người dùng cho từng khung. Kỹ thuật này được chọn bởi IEEE vì nó cho khả năng mở rộng tốt hơn so với kỹ thuật lọc khung.

Cơ chế nhận dạng khung trong VLAN là một tiếp cận mà ở đó được phát triển đặc biệt cho các cuộc giao tiếp dựa vào switch. Tiếp cận này đặt một bộ nhận dạng (Identifier) duy nhất trong tiêu đề của khung khi nó được chuyển tiếp qua trục xương sống của mạng. Bộ nhận dạng này được hiểu và được phân tích bởi switch trước bất kỳ một thao thác quảng bá hay truyền đến các switch, router hay các thiết bị đầu cuối khác. Khi khung ra khỏi đường trục của mạng, switch gở bộ nhận dạng trước khi khung được truyền đến máy tính nhận.

Kỹ thuật nhận dạng khung được thực hiện ở tầng 2 trong mô hình OSI. Nó đòi hỏi một ít xử lý và các nỗ lực quản trị.

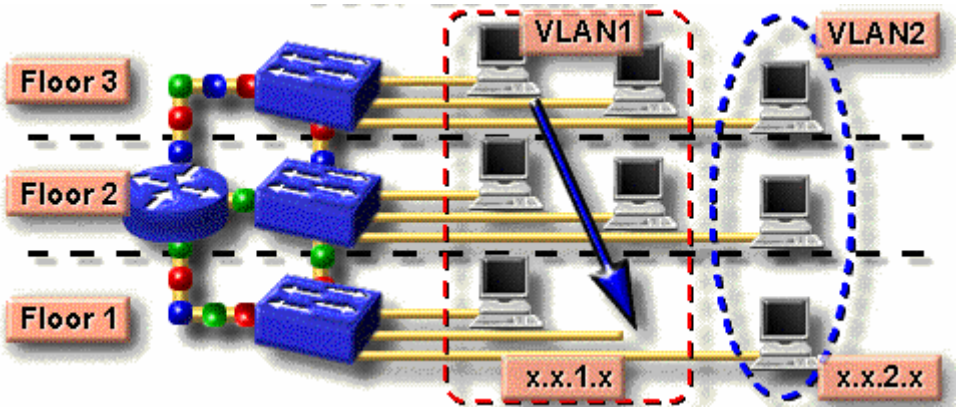
6.3 Thêm mới, xóa, thay đổi vị trí người sử dụng mạng

Các cơ quan xí nghiệp thường hay sắp xếp lại tổ chức của mình. Tính trung bình, có từ 20% đến 40% các tác vụ phải di dời hàng năm. Việc di dời, thêm và thay đổi là một trong những vấn đề đau đầu nhất của các nhà quản trị mạng và tốn nhiều chi phí cho công tác quản trị nhất. Nhiều sự di dời đòi hỏi phải đi lại hệ thống dây cáp và hầu hết các di dời đều cần phải đánh địa chỉ mới cho các máy trạm và cấu hình lại các Hub và các router.

VLAN cung cấp một cơ chế hiệu quả để điều khiển những thay đổi này, giảm thiểu các chi phí liên quan đến việc cấu hình lại Hub và các router. Các người dùng trong các

VLAN có thể chia sẻ cùng một mạng với cùng một địa chỉ mạng / mạng con mà không quan tâm đến vị trí vật lý của họ.

Khi người sử dụng trong một VLAN di dời từ vị trí này đến vị trí khác, do họ vẫn ở trong VLAN trước đó nên địa chỉ mạng của máy tính họ không cần phải thay đổi. Những thay đổi về vị trí có thể thực hiện một cách dễ dàng bằng cách gắn máy tính vào một cổng mới của switch có hỗ trợ VLAN và cấu hình cho cổng này thuộc VLAN mà trước đó máy tính này thuộc về.



Hình 6.2 – Định nghĩa VLAN

6.4 Hạn chế truyền quảng bá.

Giao thông hình thành từ các cuộc truyền quảng bá xảy ra trên tất cả các mạng. Tần suất truyền quảng bá tùy thuộc vào từng loại ứng dụng, từng loại dịch vụ, số lượng các nhánh mạng luận lý và cách thức mà các tài nguyên mạng này được sử dụng. Mặc dù các ứng dụng đã được tinh chỉnh trong những năm gần đây để giảm bớt số lần truyền quảng bá mà nó tạo ra, nhiều ứng dụng đa phương tiện mới đã được phát triển mà nó tạo ra nhiều cuộc truyền quảng bá hoặc truyền theo nhóm.

Khi thiết kế mạng cần chú ý đến phương pháp để hạn chế lại vấn đề quảng bá. Một trong những phương pháp hiệu quả nhất là thực hiện việc phân đoạn mạng một cách hợp lý với sự bảo vệ của các bức tường lửa (firewall) để tránh những vấn đề như sự hỏng hóc trên một nhánh mạng sẽ ảnh hưởng đến phần còn lại của mạng. Vì thế trong khi một nhánh mạng bị bão hòa do các thông tin quảng bá tạo ra thì phần còn lại sẽ được bảo vệ không bị ảnh hưởng nhờ vào bức tường lửa, thông thường được cài đặt trong các router.

Hình 6.3 – VLAN ngăn ngừa thông tin quảng bá

Phân nhánh mạng bằng tường lửa cung cấp một cơ chế tin cậy và giảm tối thiểu sự bảo hòa tạo ra bởi các thông tin quảng bá nhờ đó cung cấp nhiều hơn băng thông cho các ứng dụng.

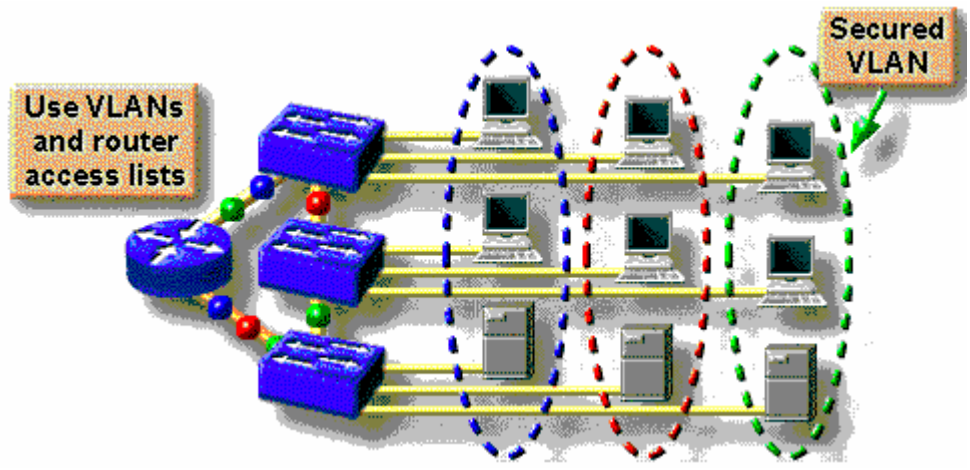
Khi các nhà thiết kế chuyển các mạng của họ sang kiến trúc sử dụng switch, các mạng trở nên mất đi các bức tường lửa và sự bảo vệ mà các router cung cấp. Khi không có router được đặt giữa các switch, các thông tin quảng bá (được thực hiện ở tầng 2) được gởi đi đến tất cả các cổng của switch. Trường hợp này được gọi là mạng phẳng (flat) ở đó tồn tại một vùng quảng bá cho toàn mạng.

VLAN là một cơ chế hiệu quả để mở rộng tính năng của các bức tường lửa trong các router vào trong các giàn hoán chuyển của switch và cung cấp một cơ chế bảo vệ mạng trước các thông tin truyền quảng bá. Các bức tường lửa này được thiết lập bằng cách gán các cổng của switch hoặc người sử dụng mạng vào các VLAN mà nó có thể thuộc một switch hay nằm trên nhiều switch khác nhau. Các thông tin quảng bá trên một VLAN không được truyền ra ngoài VLAN. Nhờ đó các cổng khác không phải nhận các thông tin quảng bá từ các VLAN khác. Kiểu cấu hình này căn bản đã giảm được sự quá tải do các thông tin quảng bá tạo ra trên mạng, dành băng thông cho các giao thông cần thiết cho người sử dụng và tránh được sự tắc nghẽn trên mạng do các cơn bão quảng bá tạo ra.

Bạn có thể dễ dàng điều khiển kích thước của vùng quảng bá bằng cách điều chỉnh lại kích thước tổng thể của các VLAN, hạn chế số lượng cổng của switch trên một VLAN và hạn chế số lượng người sử dụng trên một cổng. Một VLAN có kích thước càng nhỏ thì càng có ít người bị ảnh hưởng bởi các thông tin quảng bá tạo ra trong VLAN đó.

6.5 Thắt chặt vấn đề an ninh mạng

Việc sử dụng mạng LAN gia tăng với tỷ lệ cao trong những năm vừa qua. Điều này dẫn đến có nhiều thông tin quan trọng được lưu hành trên chúng. Các thông tin này cần phải được bảo vệ trước những truy cập không được phép. Một trong những vấn đề đối với mạng LAN chia sẻ đường truyền chung là chúng dễ dàng bị thâm nhập. Bằng cách gắn vào một cổng, một máy tính của người dùng thâm nhập có thể truy cập được tất cả các thông tin được truyền trên nhánh mạng. Nhánh mạng càng lớn thì mức độ bị truy cập thông tin càng cao, trừ khi chúng ta thiết lập các cơ chế an toàn trên Hub.



Hình 6.4 – VLAN tăng cường an ninh mạng

Một trong những kỹ thuật ít tốn kém và dễ dàng quản lý nhất để tăng cường tính bảo mật là phân nhánh mạng thành nhiều vùng quảng bá, để cho phép nhà quản trị mạng hạn chế số lượng người sử dụng trong từng nhóm VLAN và ngăn cấm những người khác thâm nhập vào mà không có sự cấp phép từ ứng dụng quản trị các VLAN. VLAN vì thế cũng cung cấp các bức tường lửa bảo mật, hạn chế những truy cập có tính cá nhân của

người dùng và ghi nhận được những sự thâm nhập không mong muốn cho nhà quản trị mạng.

Cài đặt cơ chế phân đoạn mạng là xu hướng hiện nay. Các cổng của switch được nhóm lại dựa vào kiểu của ứng dụng và quyền truy cập thông tin. Các ứng dụng và các tài nguyên được bảo vệ thường được đặt trong một VLAN an toàn. Các tính năng an toàn cao hơn có thể được đưa vào bằng cách sử dụng danh sách điều khiển truy cập (Access Control List) để hạn chế việc truy cập vào nhóm mạng này dựa vào việc cấu hình trên các switch và router. Các hạn chế này có thể được thực hiện dựa trên địa chỉ của các máy trạm, kiểu ứng dụng hay kiểu của giao thức.

6.6 Vượt qua các rào cản vật lý

VLAN cung cấp một cơ chế mềm dẻo trong việc tổ chức lại cũng như thực hiện việc phân đoạn mạng. VLAN cho phép bạn nhóm các cổng của switch và người sử dụng vào những cộng đồng có cùng một mối quan tâm.

Việc nhóm các cổng và người dùng vào những cộng đồng cùng một mối quan tâm, được biết đến như việc tổ chức các VLAN, có thể được thiết lập với một switch hoặc trên nhiều switch được nối lại với nhau trong một cơ quan xí nghiệp. Bằng việc nhóm các cổng và người sử dụng thuộc các switch khác nhau, một VLAN có thể trải rộng trên một tòa nhà hay nhiều tòa nhà.

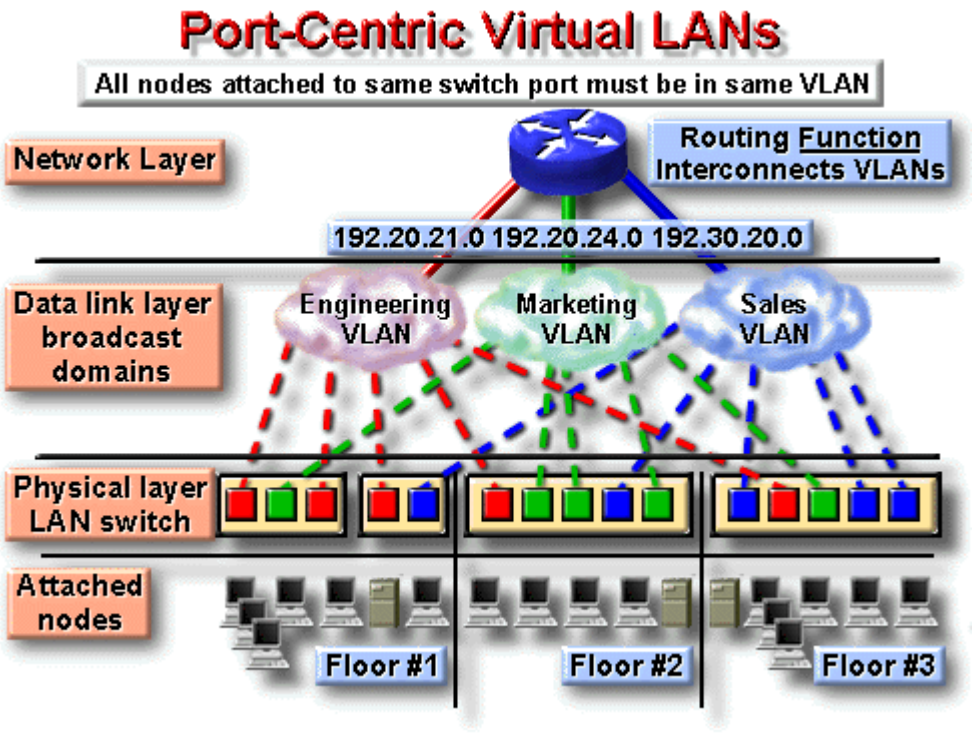
Thêm vào đó, vai trò của router mở ra bên cạnh vai trò truyền thống của một bức tường lửa (firewall) và xóa các thông tin quảng bá dựa trên chính sách, quản lý quảng bá và thực hiện chọn đường và phân phối. Các router duy trì hoạt động cho các kiến trúc switch được cấu hình VLAN bởi vì chúng cung cấp cơ chế giao tiếp giữa các nhóm mạng được định nghĩa. Giao tiếp ở tầng 3 được cài vào trong switch hoặc cung cấp bên ngoài là một bộ phận tích hợp trong của bất kỳ một kiến trúc switch hiệu suất cao nào.

6.7 Các mô hình cài đặt VLAN

6.7.1 Mô hình cài đặt VLAN dựa trên cổng

Trong sơ đồ này, các nút nối cùng một cổng của switch thuộc về cùng một VLAN. Mô hình này tăng cường tối đa hiệu suất của chuyển tải thông tin bởi vì:

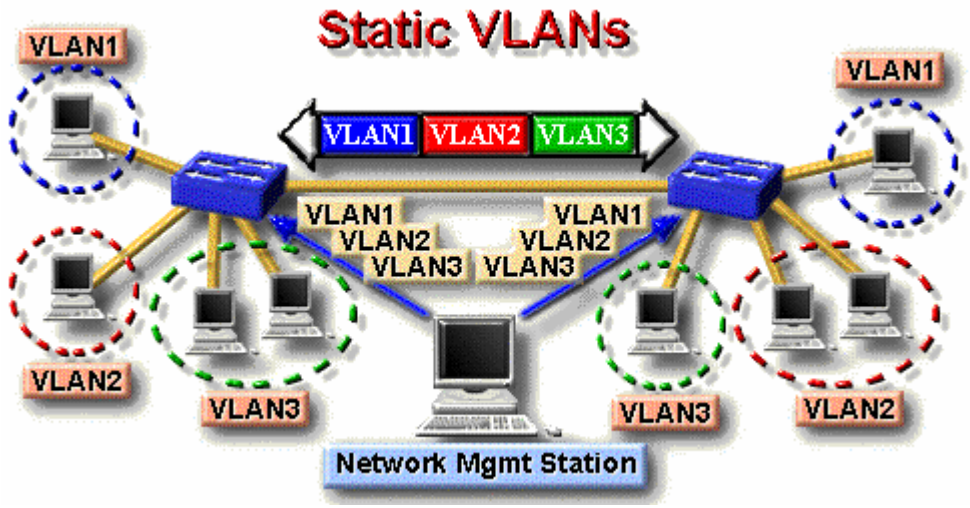
- Người sử dụng được gán dựa trên cổng
- VLANs được quản lý một cách dễ dàng
- Tăng cường tối đa tính an toàn của VLAN
- Các gói tin không rò rỉ sang các vùng khác
- VLANs và các thành phần được điều khiển một cách dễ dàng trên toàn mạng.



Hình 6.5 – Cài đặt VLAN dựa trên cổng

6.7.2 Mô hình cài đặt VLAN tĩnh

VLAN tĩnh là một nhóm cổng trên một switch mà nhà quản trị mạng gán nó vào một VLAN. Các cổng này sẽ thuộc về VLAN mà nó đã được gán cho đến khi nhà quản trị thay đổi. Mặc dù các VLAN tĩnh đòi hỏi những thay đổi bởi nhà quản trị, chúng thì an toàn, dễ cấu hình và dễ dàng để theo dõi. Kiểu VLAN này thường hoạt động tốt trong những mạng mà ở đó những sự di dời được điều khiển và được quản lý.



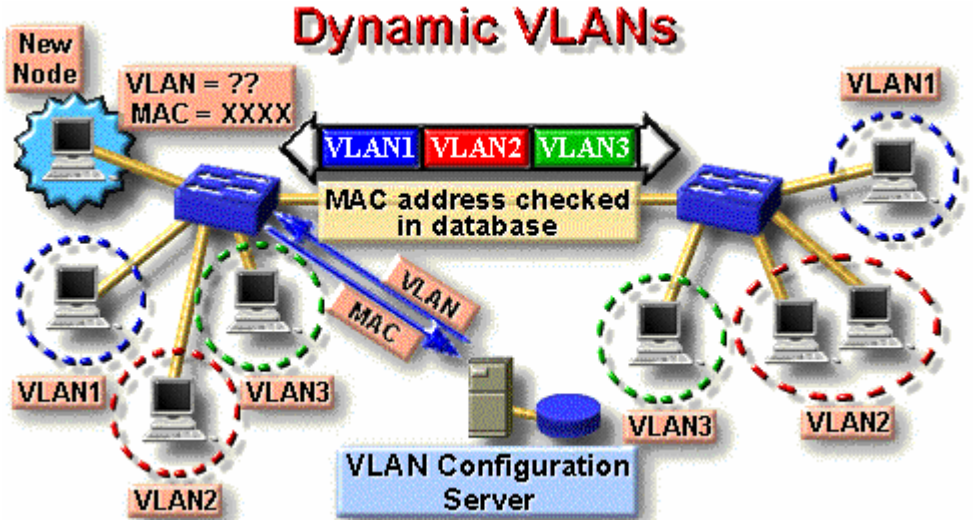
Hình 6.6 – Cài đặt VLAN tĩnh

6.7.3 Mô hình cài đặt VLAN động

VLAN động là nhóm các cổng trên một switch mà chúng có thể xác định một các tự động việc gán VLAN cho chúng. Hầu hết các nhà sản xuất switch đều sử dụng phần mềm quản lý thông minh.

Sự vận hành của các VLAN động được dựa trên địa chỉ vật lý MAC, địa chỉ luận lý hay kiểu giao thức của gói tin.

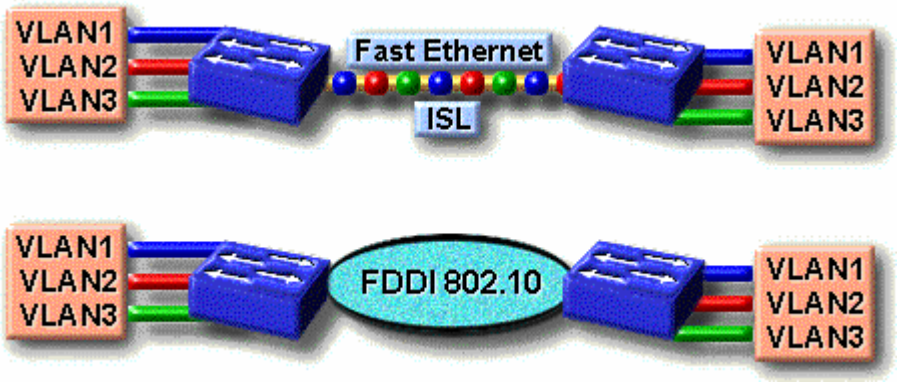
Khi một trạm được nối kết lần đầu tiên vào một cổng của switch, switch tương ứng sẽ kiểm tra mục từ chứa địa chỉ MAC trong cơ sở dữ liệu quản trị VLAN và tự động cấu hình cổng này vào VLAN tương ứng. Lợi ích lớn nhất của tiếp cận này là ít quản lý nhất với việc nối dây khi một người sử dụng được nối vào hoặc di dời và việc cảnh báo được tập trung khi một máy tính không được nhận biết được đưa vào mạng. Thông thường, cần nhiều sự quản trị trước để thiết lập cơ sở dữ liệu bằng phần mềm quản trị VLAN và duy trì một cơ sở dữ liệu chính xác về tất cả các máy tính trên toàn mạng.



Hình 6.7 –Cài đặt VLAN động

6.8 Mô hình thiết kế VLAN với mạng đường trục

Điều quan trọng nhất đối với bất kỳ một kiến trúc VLAN nào là khả năng truyền tải thông tin về VLAN giữa các switch được nối lại với nhau và với các router nằm trên mạng đường trục. Đó là cơ chế truyền tải của VLAN cho phép các cuộc giao tiếp giữa các VLAN trên toàn mạng. Các cơ chế truyền tải này xóa bỏ rào cản về mặt vật lý giữa những người sử dụng và tăng cường tính mềm dẽo cho một giải pháp sử dụngVLAN khi người sử dụng di dời và cung cấp các cơ chế cho khả năng phối hợp giữa các thành phần của hệ thống đường trục.



Hình 6.8 - Thiết kế VLAN xuyên qua Backbone

Đường trục thông thường hoạt động như là một điểm tập hợp của nhiều lượng thông tin lớn. Nó có thể mang thông tin về những người dùng cuối trong VLAN và nhận dạng giữa các switch, các router và các server nối trực tiếp. Với đường trục, băng thông lớn, các đường nối kết có khả năng lớn thường được chọn để chuyển tải thông tin xuyên qua toàn công ty.

Chương 7

Danh sách điều khiển truy cập (Access Control List)

Mục đích

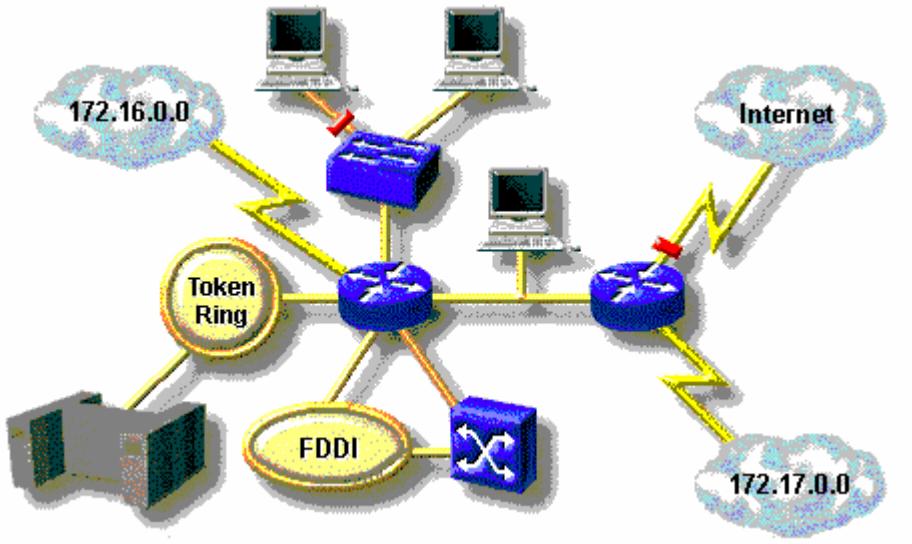
Chương này nhằm giới thiệu cho người đọc những vấn đề sau :

- Danh sách truy cập là gì
- Nguyên tắc hoạt động của danh sách truy cập
- Danh sách truy cập trong chuẩn mạng TCP/IP

7.1 Giới thiệu

Các mạng có sử dụng chọn đường đầu tiên đã nối một tập nhỏ các mạng LAN và các máy tính lại với nhau. Kế tiếp nhà quản trị mạng mở rộng các nối kết của router sang các mạng bên ngoài. Sự gia tăng của việc sử dụng Internet đã mang đến nhiều thách thức đối với việc điều khiển truy cập. Các công nghệ mới hơn như mạng đường trục bằng cáp quang cho đến các dịch vụ băng thông rộng và những bộ hoán chuyển tốc độ cao đã làm gia tăng nhiều hơn các thách thức trong điều khiển truy cập mạng.

Các nhà quản trị đang đối mặt với các vấn đề có tính tiến thoái lưỡng nan như: Làm sao từ chối các nối kết không mong muốn trong khi vẫn cho phép các truy cập hợp lệ ? Mặc dù các công cụ như mật khẩu, các thiết bị phản hồi và các thiết bị an toàn vật lý thì hữu ích, chúng thường thiếu sự diễn giải mềm dẽo và những cơ chế điều khiển mà hầu hết các nhà quản trị mạng mong muốn.



Hình 7.1 – Vấn đề an ninh trong mạng diện rộng

Danh sách truy cập (Access list) hay còn gọi Danh sách điều khiển truy cập (Access Control List) cung cấp một công cụ mạnh cho việc điều khiển mạng. Những danh sách này đưa vào cơ chế mềm dẽo trong việc lọc dòng các gói tin mà chúng đi ra, đi vào các giao diện của các router. Các danh sách này giúp mở rộng việc bảo vệ các tài nguyên mạng mà không làm ảnh hưởng đến những dòng giao tiếp hợp lệ. Danh sách truy cập phân biệt giao thông của các gói tin ra thành nhiều chủng loại mà chúng được phép hay bị từ chối. Danh sách truy cập có thể được sử dụng để:

- Nhận dạng các gói tin cho việc xếp thứ tự ưu tiên hay sắp xếp trong hàng đợi
- Hạn chế hoặc giảm nội dung của thông tin cập nhật chọn đường.

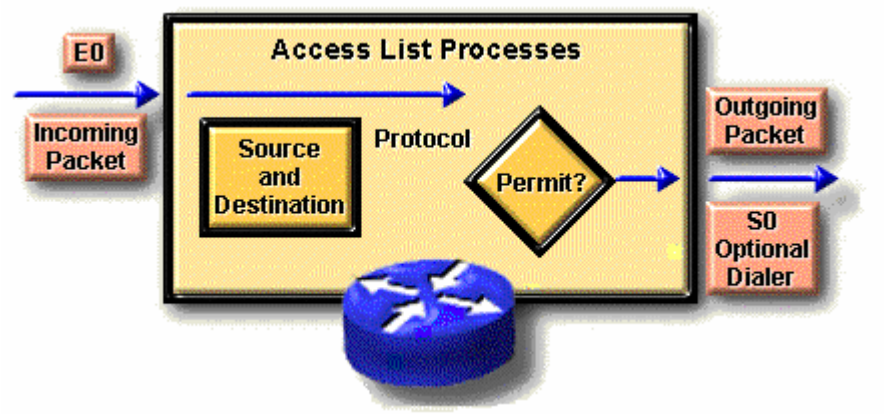
Danh sách truy cập cũng xử lý các gói tin cho các tính năng an toàn khác như:

- Cung cấp cơ chế điều khiển truy cập động đối với các gói tin IP dựa vào cơ chế nhận dạng người dùng nâng cao, sử dụng tính năng chìa và ổng khóa.
- Nhận dạng các gói tin cho việc mã hóa
- Nhận dạng các truy cập bằng dịch vụ Telnet được cho phép để cấu hình router.

7.2 Định nghĩa danh sách truy cập

Danh sách truy cập là những phát biểu dùng để đặc tả những điều kiện mà một nhà quản trị muốn thiết đặt, nhờ đó router sẽ xử lý các cuộc truyền tải đã được mô tả trong danh sách truy cập theo một cách thức không bình thường. Danh sách truy cập đưa vào những điều khiển cho việc xử lý các gói tin đặc biệt theo một cách thức duy nhất. Có hai loại danh sách truy cập chính là:

- Danh sách truy cập chuẩn (standard access list): Danh sách này sử dụng cho việc kiểm tra địa chỉ gởi của các gói tin được chọn đường. Kết quả cho phép hay từ chối gởi đi cho một bộ giao thức dựa trên địa chỉ mạng/mạng con hay địa chỉ máy.
    - Ví dụ: Các gói tin đến từ giao diện E0 được kiểm tra về địa chỉ và giao thức. Nếu được phép, các gói tin sẽ được chuyển ra giao diện S0 đã được nhóm trong danh sách truy cập. Nếu các gói tin bị từ chối bởi danh sách truy cập, tất cả các gói tin cùng chủng loại sẽ bị xóa đi.

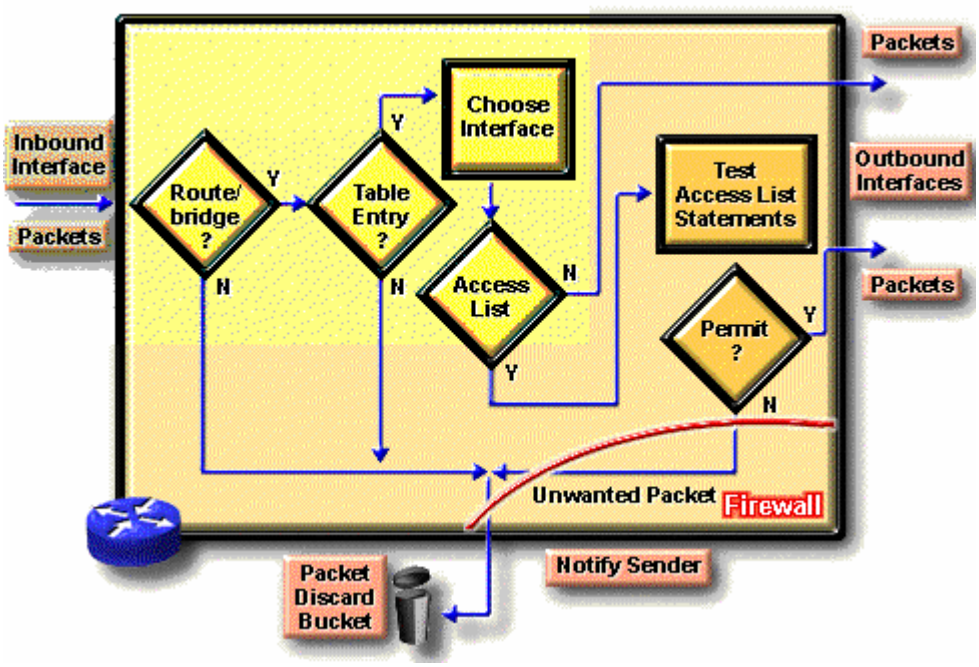


Hình 7.2 – Ý nghĩa của danh sách truy cập chuẩn

- Danh sách truy cập mở rộng (Extended access list): Danh sách truy cập mở rộng kiểm tra cho cả địa chỉ gởi và nhận của gói tin. Nó cũng kiểm tra cho các giao thức cụ thể, số hiệu cổng và các tham số khác. Điều này cho phép các nhà quản trị mạng mềm dẻo hơn trong việc mô tả những gì muốn danh sách truy cập kiểm tra. Các gói tin được phép hoặc từ chối gởi đi tùy thuộc vào gói tin đó được xuất phát từ đâu và đi đến đâu.

7.3 Nguyên tắc hoạt động của Danh sách truy cập

Danh sách truy cập diễn tả một tập hợp các qui luật cho phép đưa vào các điều khiển các gói tin đi vào một giao diện của router, các gói tin lưu lại tạm thời ở router và các gói tin gởi ra một giao diện của router. Danh sách truy cập không có tác dụng trên các gói tin xuất phát từ router đang xét.



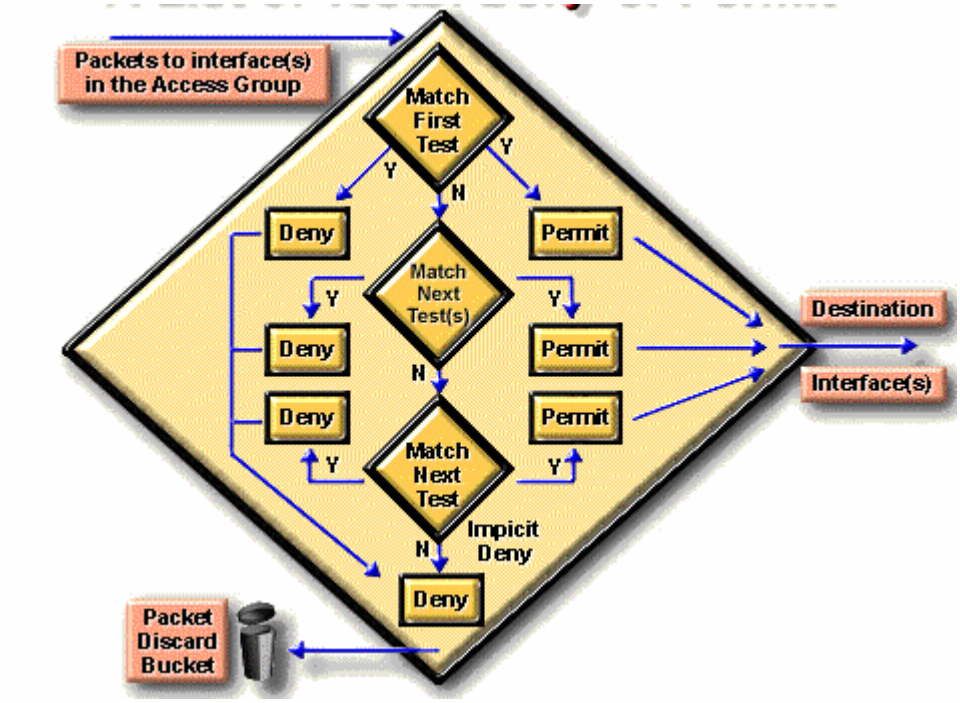
Hình 7.3 – Nguyên tắc hoạt động của danh sách truy cập

Khởi đầu của tiến trình thì giống nhau không phân biệt có sử dụng danh sách truy cập hay không: Khi một gói tin đi vào một giao diện, router kiểm tra để xác định xem có thể chuyển gói tin này đi hay không. Nếu không được, gói tin sẽ bị xóa đi. Một mục từ trong bảng chọn đường thể hiện cho một đích đến trên mạng cùng với chiều dài đường đi đến đích và giao diện của router hướng về đích đến này.

Kế tiếp router sẽ kiểm tra để xác định xem giao diện hướng đến đích đến có trong một danh sách truy cập không. Nếu không, gói tin sẽ được gởi ra vùng đệm cho ngỏ ra tương ứng, mà không bị một danh sách truy cập nào chi phối.

Giả sử giao diện nhận đã được đặt trong một danh sách truy cập mở rộng. Nhà quản trị mạng đã sử dụng các biểu thức luận lý, chính xác để thiết lập danh sách truy cập này. Trước khi một gói tin có thể được đưa đến giao diện ra, nó phải được kiểm tra bởi một tập các quy tắc được định nghĩa trong danh sách truy cập được gán cho giao diện.

Dựa vào những kiểm tra trên danh sách truy cập mở rộng, một gói tin có thể được phép đối với các danh sách vào (inbound list), có nghĩa là tiếp tục xử lý gói tin sau khi nhận trên một giao diện hay đối với danh sách ra (outbound list), điều này có nghĩa là gởi gói tin đến vùng đệm tương ứng của giao diện ra. Ngược lại, các kết quả kiểm tra có thể từ chối việc cấp phép nghĩa là gói tin sẽ bị hủy đi. Khi hủy gói tin, một vài giao thức trả lại gói tin cho người đã gởi. Điều này báo hiệu cho người gởi biết rằng không thể đi đến đích được.



Hình 7.4- Nguyên tăc lọc dựa trên danh sách truy cập

Các lệnh trong danh sách truy cập hoạt động một cách tuần tự. Chúng đánh giá các gói tin từ trên xuống. Nếu tiêu đề của một gói tin và một lệnh trong danh sách truy cập khớp với nhau, gói tin sẽ bỏ qua các lệnh còn lại. Nếu một điều kiện được thỏa mãn, gói tin sẽ được cấp phép hay bị từ chối. Chỉ cho phép một danh sách trên một giao thức trên một giao diện.

Trong ví dụ trên, giả sư có sự trùng hợp với bước kiểm tra đầu tiên và gói tin bị từ chối truy cập giao diện hướng đến đích đến. Gói tin sẽ bị bỏ đi và đưa vào một thùng rác. Gói tin không còn đi qua bất kỳ bước kiểm tra nào khác.

Chỉ các gói tin không trùng với bất kỳ điều kiện nào của bước kiểm tra đầu tiên mới được chuyển vào bước kiểm tra thứ hai. Giả sử rằng một tham số khác của gói tin trùng khớp với bước kiểm tra thứ hai, đây là một lệnh cho phép, gói tin được phép chuyển ra giao diện hướng về đích.

Một gói tin khác không trùng với bất cứ điều kiện nào của bước kiểm tra thứ nhất và kiểm tra bước thứ hai, nhưng lại trùng với điều kiện kiểm tra thứ ba với kết quả là được phép.

Chú ý rằng: Để hoàn chỉnh về mặt luận lý, một danh sách truy cập phải có các điều kiện mà nó tạo ra kết quả đúng cho tất cả các gói tin. Một lệnh cài đặt cuối cùng thì bao trùm cho tất cả các gói tin mà các bước kiểm tra trước đó đều không có kết quả đúng. Đây là bước kiểm tra cuối cùng mà nó khớp với tất cả các gói tin. Nó là kết quả từ chối. Điều này sẽ làm cho tất cả các gói tin sẽ bị bỏ đi.

7.3.1 Tổng quan về các lệnh trong Danh sách truy cập

Trong thực tế, các lệnh trong danh sách truy cập có thể là các chuỗi với nhiều ký tự. Danh sách truy cập có thể phức tạp để nhập vào hay thông dịch. Tuy nhiên chúng ta có thể đơn giản hóa các lệnh cấu hình danh sách truy cập bằng cách đưa chúng về hai loại tổng quát sau:

Loại 1: Bao gồm các lệnh cơ bản để xử lý các vấn đề tổng quát, cú pháp được mô tả như sau:

access-list *access-list- number* *{permit|deny}* *{test conditions}*

- access-list: là từ khóa bắt buộc
- access-list-number: Lệnh tổng thể này dùng để nhận dạng danh sách truy cập, thông thường là một con số. Con số này biểu thị cho loại của danh sách truy cập.
- Thuật ngữ cho phép (permit) hay từ chối (deny) trong các lệnh của danh sách truy cập tổng quát biểu thị cách thức mà các gói tin khớp với điều kiện kiểm tra được xử lý bởi hệ điều hành của router. Cho phép thông thường có nghĩa là gói tin sẽ được phép sử dụng một hay nhiều giao diện mà bạn sẽ mô tả sau.
- *test conditions:* Thuật ngữ cuối cùng này mô tả các điều kiện kiểm tra được dùng bởi các lệnh của danh sách truy cập. Một bước kiểm tra có thể đơn giản như là việc kiểm tra một địa chỉ nguồn. Tuy nhiên thông thường các điều kiện kiểm tra được mở rộng để chứa đựng một vài điều kiện kiểm tra khác. Sử dụng các lệnh trong danh sách truy cập tổng quát với cùng một số nhận dạng để chồng nhiều điều kiện kiểm tra vào trong một chuỗi luận lý hoặc một danh sách kiểm tra.

Loại 2: Xử lý của danh sách truy cập sử dụng một lệnh giao diện. Cú pháp như sau:

{protocol} access-group access-list-number

Với:

Protocol: là giao thức áp dụng danh sách truy cập

Access-group: là từ khóa

Access-list-number: Số hiệu nhận dạng của danh sách truy cập đã được định nghĩa trước

Tất cả các lệnh của danh sách truy cập được nhận dạng bởi một con số tương ứng với một hoặc nhiều giao diện. Bất kỳ các gói tin mà chúng vượt qua được các điều kiện kiểm tra trong danh sách truy cập có thể được gán phép sử dụng bất kỳ một giao diện trong nhóm giao diện được phép.

7.4 Danh sách truy cập trong chuẩn mạng TCP/IP

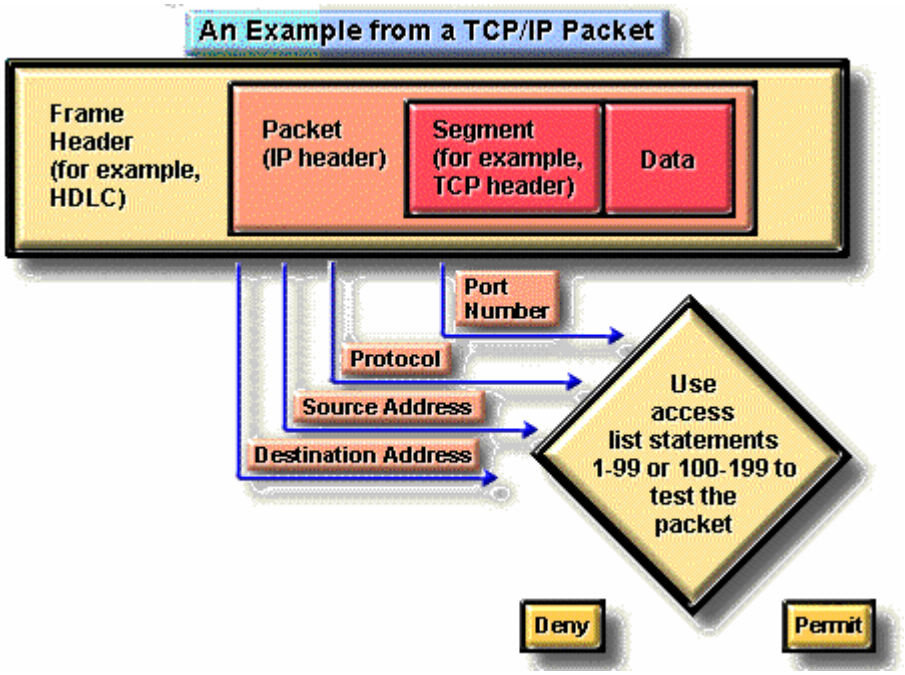
7.4.1 Kiểm tra các gói tin với danh sách truy cập

Để lọc các gói tin TCP/IP, danh sách truy cập trong hệ điều hành liên mạng của Cisco kiểm tra gói tin và phần tiêu đề của giao thức tầng trên.

Tiến trình này bao gồm các bước kiểm tra sau trên gói tin:

- Kiểm tra địa chỉ nguồn bằng danh sách truy cập chuẩn. Nhận dạng những danh sách truy cập này bằng các con số có giá trị từ 1 đến 99
- Kiểm tra địa chỉ đích và địa chỉ nguồn hoặc giao thức bằng danh sách truy cập mở rộng . Nhận dạng các danh sách này bằng các con số có giá trị từ 100 đến 199.

- Kiểm tra số hiệu cổng của các giao thức TCP hoặc UDP bằng các điều kiện trong các danh sách truy cập mở rộng. Các danh sách này cũng được nhận dạng bằng các con số có giá trị từ 100 đến 199.



Hình 7.5 – Ví dụ về danh sách truy cập trong gói tin TCP/IP

Đối với tất cả các danh sách truy cập của giao thức TCP/IP này, sau khi một gói tin được kiểm tra để khớp một lệnh trong danh sách, nó có thể bị từ chối hoặc cấp phép để sử dụng một giao diện trong nhóm các giao diện được truy cập.

Một số lưu ý khi thiết lập danh sách truy cập:

- Nhà quản trị mạng phải hết sức thận trọng khi đặc tả các điều khiển truy cập và thứ tự các lệnh để thực hiện các điều khiển truy cập này. Chỉ rõ các giao thức được phép trong khi các giao thức TCP/IP còn lại thì bị từ chối.
- Chỉ rõ các giao thức IP cần kiểm tra. Các giao thức IP còn lại thì không cần kiểm tra.
- Sử dụng các ký tự đại diện (wildcard) để mô tả luật chọn lọc địa chỉ IP.

7.4.2 Sử dụng các bit trong mặt nạ ký tự đại diện

Mặt nạ ký tự đại hiện (Wildcard mask) là một chuỗi 32 bits được dùng để kết hợp với địa chỉ IP để xác định xem bit nào trong địa chỉ IP được bỏ qua khi so sánh với các địa chỉ IP khác. Các mặt nạ ký tự đại diện này được mô tả khi xây dựng các danh sách truy cập. Ý nghĩa của các bits trong mặt nạ các ký tự đại diện được mô tả như sau:

- Một bits có giá trị là 0 trong mặt nạ đại diện có nghĩa là « hãy kiểm tra bit của địa chỉ IP có vị trí tương ứng với bit này »
- Một bits có giá trị là 1 trong mặt nạ đại diện có nghĩa là « đừng kiểm tra bit của địa chỉ IP có vị trí tương ứng với bit này »

Bằng cách thiết lập các mặt nạ ký tự đại diện, một nhà quản trị mạng có thể chọn lựa một hoặc nhiều địa chỉ IP để các kiểm tra cấp phép hoặc từ chối. Xem ví dụ trong hình dưới đây:

128	64	32	16	8	4	2	1	Vị trí các bit trong byte và giá trị địa chỉ của nó
0	0	0	0	0	0	0	0	Mặt nạ kiểm tra tất cả các bit địa chỉ
0	0	1	1	1	1	1	1	Mặt nạ không kiểm tra 6 bits cuối cùng của địa chỉ
0	0	0	0	1	1	1	1	Mặt nạ không kiểm tra 4 bits cuối cùng của địa chỉ
1	1	1	1	1	1	0	0	Mặt nạ kiểm tra 2 bits cuối cùng của địa chỉ
1	1	1	1	1	1	1	1	Mặt nạ không kiểm tra địa chỉ

Ví dụ: Cho một địa chỉ mạng ở lớp B 172.16.0.0. Mạng này được chia thành 256 mạng con bằng cách sử dụng 8 bit ở bytes thứ 3 của địa chỉ để làm số nhận dạng mạng con. Nhà quản trị muốn định kiểm tra các địa chỉ IP của các mạng con từ 172.16.16.0 đến 172.16.31. Các bước suy luận để đưa ra mặt nạ các ký tự đại diện trong trường hợp này như sau:

- Đầu tiên mặt nạ ký tự đại diện phải kiểm tra hai bytes đầu tiên của địa chỉ (172.16). Như vậy các bits trong hai bytes đầu tiên của mặt nạ ký tự đại diện phải bằng 0. Ta có 0000 0000.0000 0000.-.-
- Do không kiểm tra địa chỉ của các máy tính trong mạng nên các bit của bytes cuối cùng sẽ được bỏ qua. Vì thế các bits của bytes cuối cùng trong mặt nạ ký tự đại diện sẽ là 1. Ta có 0000 0000.0000 0000.-.1111 1111
- Trong byte thứ ba của địa chỉ nơi mạng con được định nghĩa, mặt nạ ký tự đại diện sẽ kiểm tra bit ở vị trí có giá trị thứ 16 của địa chỉ phải được bật (giá trị là 1) và các bits ở phần cao còn lại phải tắt (giá trị là 0). Vì thế các bits tương ứng trong mặt nạ ký tự đại diện phải bằng 0.
- Bốn bits còn lại của bytes thứ 3 không cần kiểm tra để nó có thể tạo nên các giá trị từ 16 đến 31. Vì thế các bits tương ứng trong mặt nạ ký tự đại diện tương ứng sẽ bằng 1.
- Như vậy mặt nạ ký tự đại diện là đầy đủ là:
  0000 0000.0000 0000.0000 1111.1111 1111 hay 0.0.15.255

Để đơn giản, một số router, chẳng hạn CISCO, sử dụng một số từ viết tắt để chỉ một số mặt nạ thường sử dụng:

- any: dùng để chỉ mặt nạ cho phép tất cả địa chỉ (255.255.255.255) hoặc cấm tất cả (0.0.0.0.).
- host: được đặt phía trước một địa chỉ IP của một máy tính để chỉ rằng hãy kiểm tra tất cả các bit của địa chỉ trên. Ví dụ: host 172.16.1.1.

7.4.3 Cấu hình danh sách truy cập chuẩn cho giao thức IP

Phần này giới thiệu một số lệnh được hỗ trợ trong các router của Cisco.

7.4.3.1 Lệnh access list

Lệnh này dùng để tạo một mục từ trong danh sách bộ lọc chuẩn. Cú pháp như sau:

access-list *access-list-No {permit | deny } source {source-mask}*

Ý nghĩa của các tham số:

- access-list-No: Là số nhận dạng của danh sách truy cập, có giá trị từ 1 đến 99
- permit | deny: Tùy chọn cho phép hay không cho phép đối với giao thông của khối địa chỉ được mô tả phía sau.
- source: Là một địa chỉ IP
- source-mask: Là mặt nạ ký tự đại diện áp dụng lên khối địa chỉ source

7.4.3.2 Lệnh ip access-group

Lệnh này dùng để liên kết một danh sách truy cập đã tồn tại vào một giao diện. Cú pháp như sau:

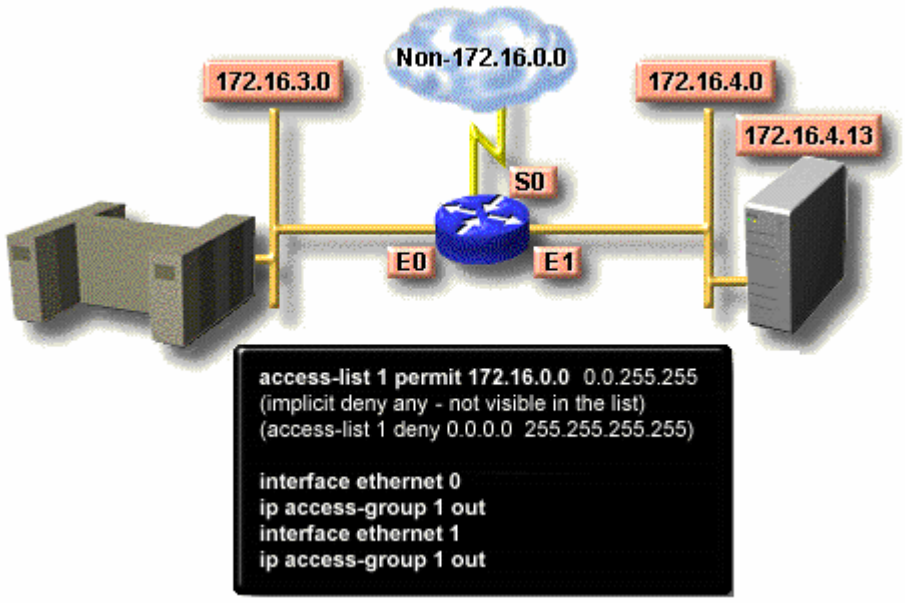
ip access-group *access-list-No {in/out}*

- access-list-no: số nhận dạng của danh sách truy cập được nối kết vào giao diện
- in/out: xác định chiều giao thông muốn áp dụng và vào hay ra.

7.4.3.3 Một số ví dụ

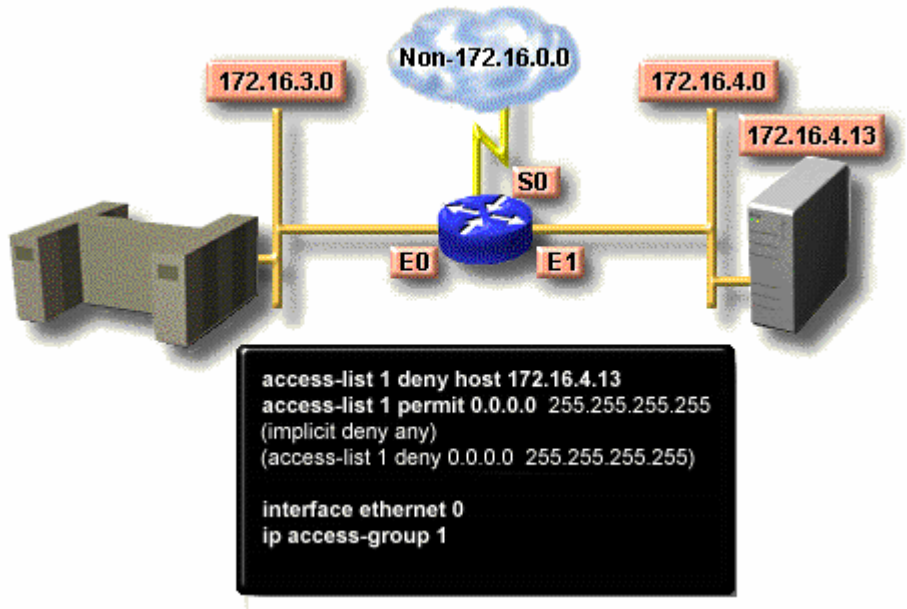
7.4.3.4 Tạo danh sách truy cập chuẩn

7.4.3.4.1 Ví dụ 1



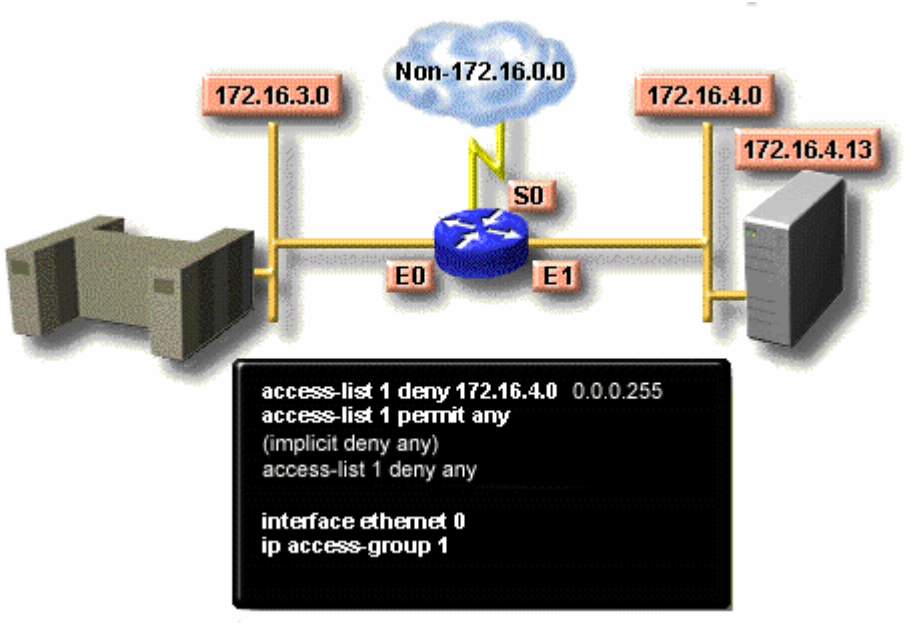
Danh sách truy cập trên chỉ cho phép các giao thông từ mạng nguồn 172.16.0.0 được chuyển tiếp đi qua router. Các giao thông trên các mạng khác đều bị khóa.

7.4.3.4.2 Ví dụ 2



Danh sách truy cập này được thiết kế để khóa các giao thông từ địa chỉ IP 172.16.1.13 và cho phép các luồng giao thông khác được chuyển tiếp qua các giao diện Ethernet (E0 và E1)

7.4.3.4.3 Ví dụ 3



Danh sách truy cập này được thiết kế để khóa luồng giao thông từ mạng con 172.16.4.0 và cho phép các luồng giao thông khác được chuyển tiếp.

7.4.4 Cấu hình danh sách truy cập mở rộng

Để có thể điều khiển việc lọc các luồng giao thông được chính xác hơn ta sử dụng các danh sách điều khiển truy cập mở rộng của giao thức IP. Các lệnh trong danh sách truy cập cho phép kiểm tra địa chỉ nguồn và địa chỉ nhận. Ngoài ra danh sách truy cập mở rộng còn cho phép đặc tả các cổng của các giao thức TCP và UDP. Các danh sách truy cập mở

rộng thường sử dụng các số nhận dạng từ 100 đến 199. Phần kế tiếp sẽ mô tả các lệnh của danh sách truy cập mở rộng thường được hỗ trợ trong bởi các router .

7.4.4.1 Lệnh access-list

Lệnh này được sử dụng để tạo một mục từ để diễn giải một điều kiện lọc phức tạp. Cú pháp như sau:

access-list *access-list-no {permit|deny} protocol source source-mask destination destination-mask [operator operand] [established]*

- *access-list-no:* Số nhận dạng của danh sách, có giá trị từ 100 đến 199
- *permit|deny:* chỉ định danh sách này dùng để cấp phép hay từ chối khối địa chỉ theo sau.
- *protocol:* có thể là một trong các giá trị sau IP, TCP, UDP, ICMP, GRE, IGRP.
- *source và destination:* Xác định địa chỉ IP gởi và nhận
- *source-mask và destination-mask:* là mặt nạ ký tự đại diện cho địa chỉ nguồn và địa chỉ đích.
- *operator và operand:* là một trong các phép toán sau lt, gt, eq, neq (nhỏ hơn, lớn hơn, bằng, không bằng), và một số hiệu cổng.
- *established*: Cho phép giao thức TCP duy trì nối kết

7.4.4.2 Lệnh ip access-group

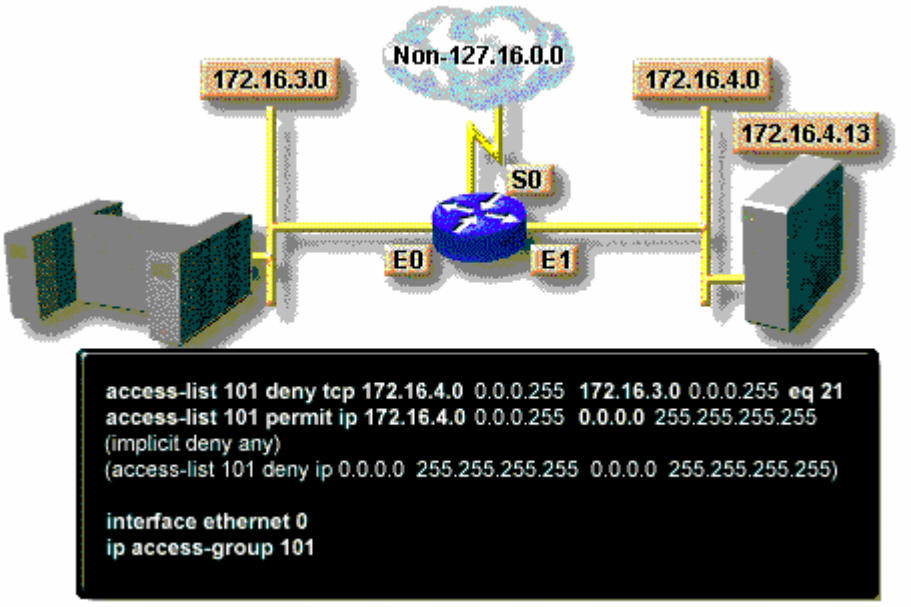
Nối kết một danh sách điều khiển nối kết mở rộng với một giao diện mạng ngỏ ra. Chỉ cho phép một danh sách điều khiển truy cập trên một cổng của một giao thức. Cú pháp như sau:

ip access-group *access-list-no {in|out}*

- access-list-no: là số nhận dạng của danh sách điều khiển truy cập mở rộng
- in|out: để xác định danh sách điều khiển truy cập này áo dụng cho giao diện vào hay ra.

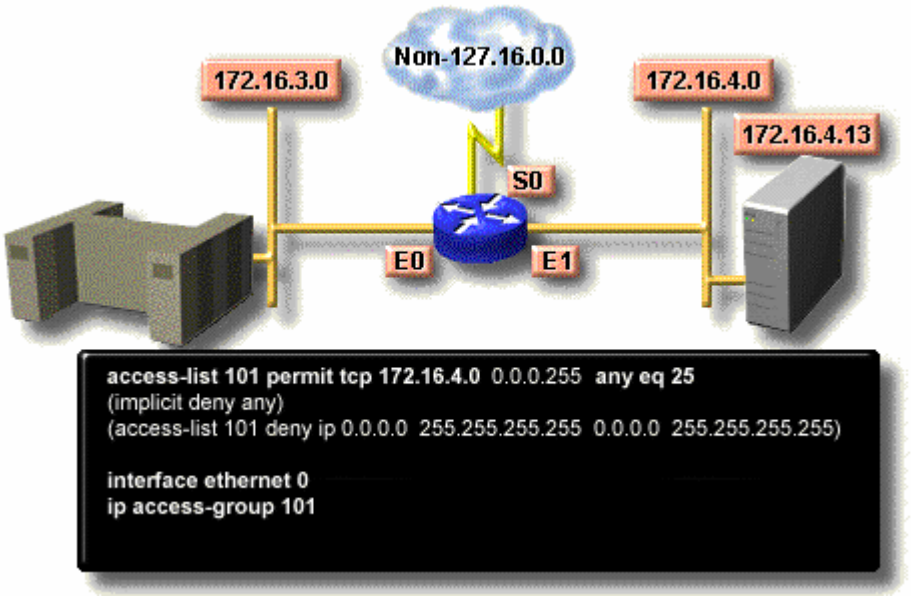
7.4.4.3 Một số ví dụ về danh sách điều khiển truy cập mở rộng

Ví dụ 1:



Danh sách điều khiển truy cập này được thiết kế để cho phép luồng giao thông từ mạng con 172.16.4.0 được chuyển đến bất kỳ một mạng hoặc mạng con khác thông qua giao diện E0.

Ví dụ 2:



Danh sách điều khiển truy cập này được thiết kế để chi cho phép thư điện tử từ mạng con 172.16.4.0 được gởi qua giao diện E0. Các luồng giao thông từ các mạng khác đều bị từ chối.

7.4.4.4 Nguyên tắc sử dụng danh sách điều khiển truy cập

Như vậy ta có hai loại danh sách điều khiển truy cập là danh sách điều khiển truy cập chuẩn và danh sách điều khiển truy cập mở rộng. Danh sách điều khiển truy cập chuẩn chỉ các gói tin dựa vào địa chỉ địa chỉ nguồn. Chính vì thế trong một mạng có nhiều router, nó cần được thiết lập ở router nằm gần thế giới bên ngoài nhất. Ngược lại, danh sách điều khiển truy cập mở rộng cho phép lọc dựa trên đích đến của các gói tin, vì thế chúng thường được đặt ở các router gần các máy nguồn nhất để ngăn chặn sớm các gói tin đến các đích đến không được phép.

Chương 8

Vấn đề quản trị mạng

Mục đích

Chương này nhằm giới thiệu cho người đọc những vấn đề sau :

- Các vấn đề của quản trị mạng: Quản lý hiệu suất, cấu hình, tài khoản, quản lý lỗi, an ninh
- Mô hình của một hệ thống quản trị mạng
- Giao thức quản trị mạng
- Giao thức quản trị mạng SNMP

8.1 Giới thiệu

Quản trị mạng thường được hiểu theo nhiều nghĩa khác nhau. Một số người cho rằng đó là việc theo dõi các hoạt động trên mạng, thêm người dùng mới vào hệ thống, xóa người dùng không còn tồn tại trong cơ quan hay thực hiện việc phân quyền sử dụng các tài nguyên trên mạng như máy in, thư mục, truy cập Internet cho những người dùng trên mạng. Một số người khác lại cho rằng đó là công việc nặng nhọc hơn, phải thực hiện việc thêm vào các thiết bị mạng mới, cài đặt thêm dịch vụ mới vào hệ thống, làm cho tất cả các máy trong mạng đều vận hành tốt, theo dõi lưu thông trên mạng bằng các chương trình mô phỏng, ... Theo ISO, về mặt quan niệm quản trị mạng có thể được phân chia thành năm lĩnh vực sau:

- Quản lý hiệu suất mạng (Performance management)
- Quản lý cấu hình (Configuration management)
- Quản lý tài khoản (Accounting manangement)
- Quản lý lỗi (Fault management)
- Quản lý an ninh mạng (Security management)

8.1.1 Quản lý hiệu suất mạng (Performance management)

Mục đích của việc quản lý hiệu suất là đo đạt và đảm bảo sự hiện diện của các tiêu chí về hiệu suất mạng nhờ đó hiệu suất của liên mạng được duy trì ở mức có thể chấp nhận được. Các tham số để đo hiệu suất mạng có thể là thông lượng tổng của mạng (network throughput), thời gian đáp ứng người dùng, ...

Quản lý hiệu suất mạng gồm 3 bước. Đầu tiên là các dữ liệu liên quan đến hiệu suất được thu thập dựa trên các tham số quan tâm của nhà quản trị mạng. Kế tiếp, dữ liệu sẽ được phân tích để xác định được các mức độ bình thường (baseline). Cuối cùng, xác định các giá trị ngưỡng cho mỗi tham số quan trọng nhờ đó mỗi khi các giá trị này vượt quá giá trị ngưỡng thì xem như mạng đang có vấn đề cần lưu ý. Thông thường các phần mềm dùng để quản lý mạng cho phép thiết lập các cơ chế cảnh báo tự động khi nó phát hiện có sự vượt quá ngưỡng cho phép của một số tham số.

Mỗi bước trong các bước được mô tả ở trên là một phần của tiến trình thiết lập hệ thống tự phản ứng. Khi hiệu suất trở nên không thể chấp nhận được vì có sự vượt quá các ngưỡng được thiết đặt, hệ thống tự phản ứng bằng cách gởi một thông điệp cảnh báo.

8.1.2 Quản lý cấu hình mạng

Mục đích của việc quản lý cấu hình mạng là để theo dõi mạng và các thông tin cấu hình hệ thống mạng nhờ đó sự ảnh hưởng tác động do sự khác nhau về các phiên bản của phần cứng, phần mềm có thể được theo dõi và quản lý.

Mỗi một thiết bị mạng có một vài thông tin về phiên bản gắn liền với nó. Các hệ thống quản lý cấu hình con lưu các thông tin này vào các cơ sở dữ liệu để dễ dàng truy cập. Khi có một sự cố xảy ra, các thông tin này sẽ được sử dụng để tìm ra nguyên nhân của sự việc.

8.1.3 Quản lý tài khoản (Account management)

Mục đích của việc quản lý tài khoản là để đo các thông số về mức độ sử dụng mạng nhờ đó sự sử dụng mạng của các cá nhân hay những nhóm người dùng được qui định một cách phù hợp.

Những qui định này hạn chế tối thiểu các vấn đề về mạng và tối đa sự hợp lý về việc truy cập mạng của tất cả người dùng.

8.1.4 Quản lý lỗi (Fault Management)

Mục đích của việc quản lý lỗi là để dò tìm, ghi nhận và cánh báo cho người dùng và tự động sửa chữa những vấn đề về mạng giữ cho mạng vận hành một cách hiệu quả. Bởi vì các lỗi có thể làm cho ngưng trệ hoạt động của mạng, việc quản lý lỗi được cài đặt trong phần lớn các thiết bị mạng đã được chuẩn hóa bởi ISO.

Việc quản lý lỗi được bắt đầu với việc xác định các triệu chứng và cô lập vấn đề phát sinh. Kế đó, vấn đề được khắc phục và một giải pháp được kiểm tra trên tất cả các hệ thống con. Cuối cùng việc phát hiện được lỗi cũng như các giải pháp khắc phục thì được ghi nhận lại.

8.1.5 Quản lý an ninh (Security management)

Mục đích của việc quản an ninh mạng là để điều khiển các truy cập vào các tài nguyên trên mạng dựa theo một nguyên tắc chỉ đạo nội bộ nhờ đó mạng không bị phá hoại (từ bên trong hoặc từ bên ngoài) và các thông tin nhạy cảm không bị truy cập bởi những người không được phép.Ví dụ như các hệ thống quản lý an ninh con có thể theo dõi những người dùng đăng nhập vào mạng và có thể từ chối các truy cập của những người mà mã nhập vào của họ thì không hợp lệ.

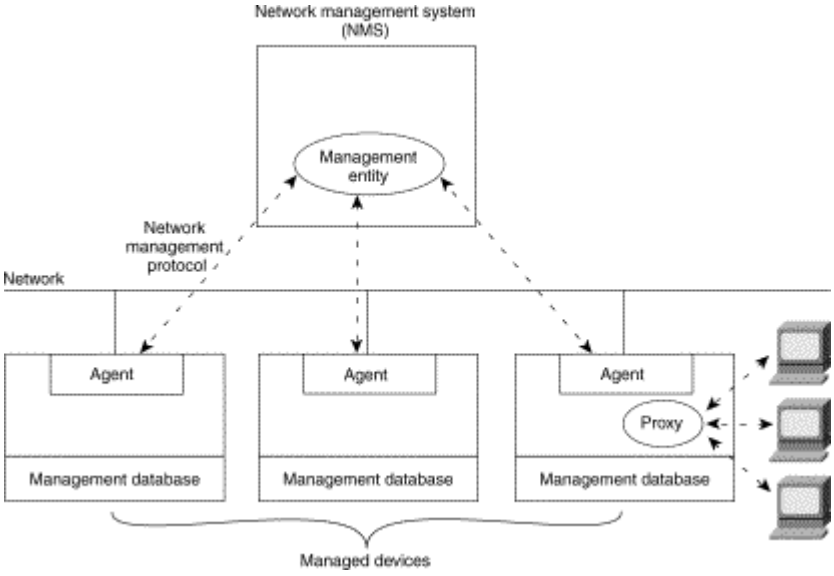
Các hệ thống quản trị an ninh cấp dưới hoạt động bằng cách chia tài nguyên mạng thành những vùng được phép và không được phép. Đối với một số người dùng, truy cập vào bất cứ tài nguyên mạng nào đều là không hợp lệ, hầu hết bởi vì những người dùng này thông thường là bên ngoài công ty. Đối với một số người dùng mạng khác, truy cập vào một số thông tin được tạo ra từ một số bộ phận được xem là không hợp lệ. Chẳng hạn truy cập vào các tập tin của phòng quản lý nhận sự là không hợp lệ đối với những người dùng không thuộc phòng quản lý nhân sự.

Các hệ thống quản lý an ninh con thực hiện một số các chức năng. Chúng nhận dạng các tài nguyên nhạy cảm như hệ thống, các tập tin, các thực thể khác và xác định mối tương quan giữa các tài nguyên mạng nhạy cảm và tập hợp các người dùng. Chúng cũng theo dõi các điểm truy cập đến các tài nguyên nhạy cảm trong mạng và việc đăng nhập không hợp lệ vào các tài nguyên nhạy cảm của mạng.

8.2 Hệ thống quản trị mạng

Để giúp nhà quản trị mạng có thể theo dõi được tất cả các lĩnh vực liên quan đến công tác quản trị mạng, các thiết bị phần cứng và phần mềm mạng cần được thiết kế và cài đặt theo hướng hỗ trợ công tác quản trị mạng cho nhà quản trị. Sau đó, người ta thiết kế các phần mềm chuyên dùng cho công tác quản trị mạng. Sự phối hợp giữa phần cứng và phần mềm quản trị mạng này hình thành nên một hệ thống quản trị mạng.

Hiện nay có nhiều hệ thống quản trị mạng khác nhau, tuy nhiên hầu hết chúng đều có kiến trúc chung giống như hình dưới đây:



Hình 8.1 – Kiến trúc của một hệ thống quản trị mạng

Trong kiến trúc này, các trạm làm việc đầu cuối (End station) như là máy tính, máy in mạng, các thiết bị nối mạng như Hub, switch, router, ... cần thiết phải theo dõi trạng thái hay điều khiển. Chúng được gọi là các thiết bị được quản trị (Managed Device).

Máy tính mà trên đó ta cài phần mềm cho phép nhà quản trị mạng thực hiện các thao tác quản trị mạng được gọi là Trạm quản trị mạng (NMS-Network Management Station), đôi khi còn gọi là Hệ thống quản trị mạng (Network Management System). Phần mềm cài đặt trên trạm quản trị này được gọi là Thực thể quản trị mạng (Management Entity).

Mỗi thiết bị được quản trị có chạy một chương trình để cho phép chúng gởi thông báo về thực thể quản trị mạng các sự kiện bất thường xảy ra trên chúng (ví dụ như một giá trị ngưỡng nào đó bị vượt qua) cũng như nhận và thi hành các mệnh lệnh do thực thể quản trị mạng gởi đến. Phần mềm chạy bên trong các thiết bị được quản trị này được gọi là các Tác nhân (agent).

Nhiệm vụ của các agent là thường xuyên theo dõi trạng thái của thiết bị mà nó đang chạy trên đó. Agent sẽ thường xuyên ghi nhận lại các giá trị của các thông số phản ánh tình trạng của thiết bị mà nhà quản trị quan tâm vào một cơ sở dữ liệu nằm bên trong thiết bị. Cơ sở dữ liệu này được gọi là Cơ sở thông quản trị (MIB-Management Information Base).

Mỗi khi nhà quản trị mạng muốn biết thông tin về trạng thái của một thiết bị nào đó, nhà quản trị mạng sẽ gọi thực hiện một chức năng tương ứng trên phần mền quản trị mạng. Khi đó, thực thể quản trị mạng sẽ gởi một lệnh đến tác nhân trên thiết bị tương ứng. Tác nhân sẽ dò trong cở sở thông tin quản trị thông tin mà nhà quản trị mong muốn để gởi ngược về cho thực thể quản trị mạng. Phần mềm quản trị mạng sẽ hiển thị lên màn hình, thường dưới dạng đồ họa, cho nhà quản trị xem.

Việc giao tiếp giữa thực thể quản trị mạng và tác nhân quản trị mạng đòi hỏi phải tuân thủ một giao thức nào đó. Giao thức này được gọi là giao thức quản trị mạng (Network Managment Protocol). Một phần mềm quản trị mạng chỉ quản lý được các thiết bị khi chúng sử dụng cùng giao thức quản trị mạng với phần mềm quản trị mạng. Để một

phần mềm quản trị mạng có thể quản trị được các thiết bị của các nhà sản xuất khác nhau, cần thiết phải chuẩn hóa giao thức quản trị mạng. Hiện tại có một số giao thức sử dụng phổ biến như:

- Giao thức quản trị mạng đơn giản (SNMP – Simple Network Management Protocol)
- Giao thức theo dõi mạng từ xa (RMON – Remote Monitoring)

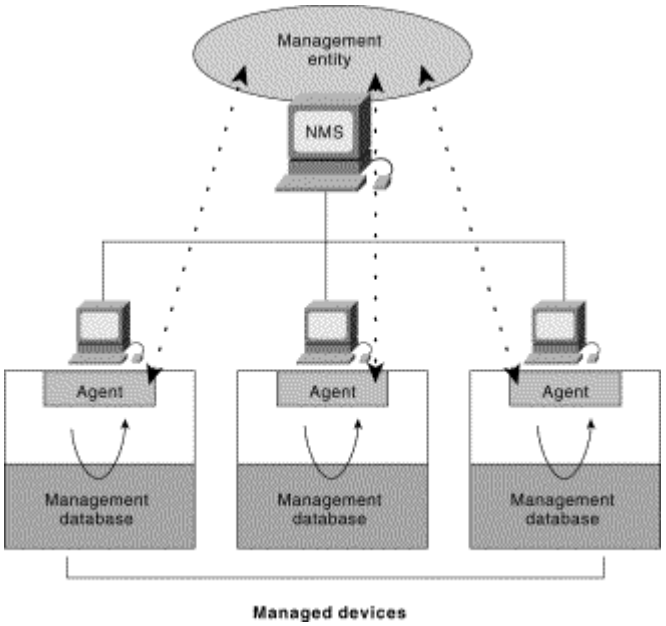
8.3 Giao thức quản trị mạng đơn giản (SNMP – Simple Network Management Protocol)

8.3.1 Giới thiệu

SNMP là giao thức hoạt động trên tầng ứng dụng được định nghĩa để cho phép sự trao đổi thông tin quản trị giữa các thiết bị diễn ra một cách thuận tiện. SNMP được xem như là một phần của bộ giao thức TCP/IP. Nó cho phép các nhà quản trị mạng quản lý hiệu suất mạng, tìm và giải quyết các sự cố trên mạng cũng như lập kế hoạch cho sự mở rộng mạng.

SNMP có hai phiên bản SNMP v.1 (RFC1157) và SNMP v.2 (RFC1902). Cả hai đều có một số đặc điểm chung. Tuy nhiên SNMP v.2 cung cấp nhiều tính năng nổi bật hơn, cũng như thêm vào nhiều tác vụ trên giao thức. Phiên bản thứ ba hiện vẫn chưa được chuẩn hóa.

Theo SNMP một hệ thống quản trị mạng gồm các thành phần cơ bản như:Thiết bị được quản trị (Managed device), tác nhân và Hệ thống quản trị mạng (Network Management System)



Hình 8.2 – Kiến trúc của hệ thống quản trị mạng theo SNMP

8.3.2 Các lệnh cơ bản trong giao thức SNMP

Các thiết bị được theo dõi và bị điều khiển bằng cách dùng bốn lệnh cơ bản được hỗ trợ bởi giao thức SNMP là read, write, trap và các tác vụ ngược.

- Lệnh read được sử dụng bởi một NMS để theo dõi các thiết bị được quản trị. NMS khảo sát các tham số khác nhau được lưu trữ bởi thiết bị được quản trị.
- Lệnh write được sử dụng bởi một NMS để điều khiển các thiết bị được quản trị. NMS thay đổi giá trị của các tham số được lưu trên thiết bị được quản trị.
- Lệnh trap được sử dụng bởi các thiết bị được quản trị để báo hiệu về NMS những sự kiện bất thường mà nó phát hiện được.
- Traversal operation được sử dụng bởi NMS để xác định các tham số nào được hỗ trợ bởi một thiết được quản trị và từ đó tập hợp các thông tin trong các bảng.

8.3.3 Cơ sở thông tin quản trị của SNMP

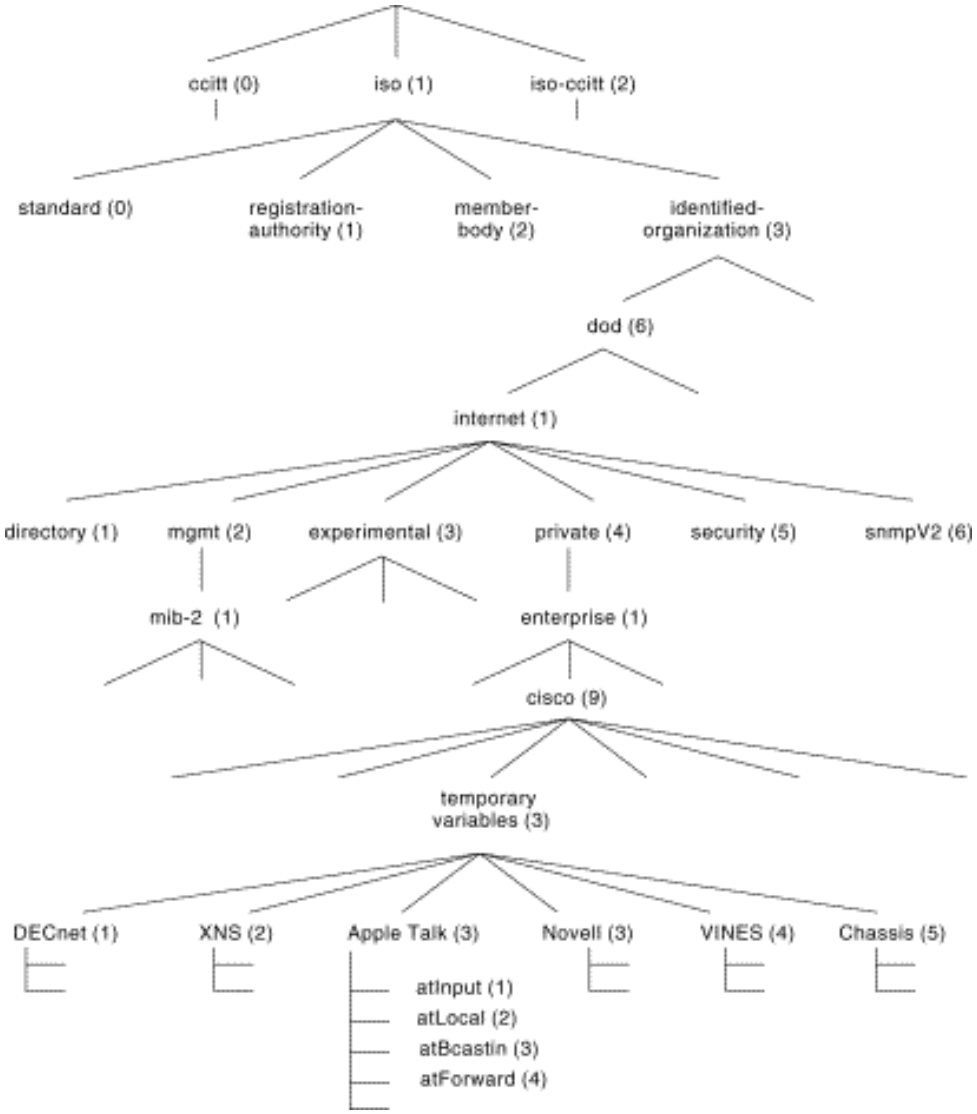
MIB là một tập hợp thông tin được tổ chức theo dạng phân cấp. MIB được truy cập bằng cách sử dụng các giao thức quản trị mạng như SNMP chẳng hạn. MIB chứa thông tin về các đối tượng được quản lý dưới dạng các đối tượng, và mỗi đối tượng được nhận dạng bằng một số nhận dạng.

Một đối tượng được quản lý trong MIB (đôi khi còn gọi là một đối tượng MIB) là một trong những thuộc tính đặc trưng của một thiết bị được quản trị. Các đối tượng được quản lý bao gồm một hoặc nhiều thể hiện của đối tượng, thông thường chúng là các biến.

Có hai loại đối tượng được quản lý là đối tượng vô hướng (scalar) và đối tượng dạng ống (tubular). Đối tượng vô hướng định nghĩa chỉ một thể hiện của đối tượng. Đối tượng hình ống định nghĩa nhiều thể hiện của các đối tượng có liên quan nhau và chúng được nhóm lại thành các bảng trong MIB.

Ví dụ về một đối tượng được quản lý là lượng gói tin đi vào của một giao diện trên một router. Đây là đối tượng vô hướng vì nó có giá trị chỉ là một con số nguyên.

Số nhận dạng của một đối tượng nhận dạng duy nhất một đối tượng được quản lý trong cấu trúc thứ bậc của MIB. Cấu trúc có thứ bậc của MIB có thể được mô tả như là một cây mà gốc của nó không có nhản và các cấp thì được gán cho các tổ chức khác nhau.



Hình 8.3 – Cây đăng ký chung

Số nhận dạng của các đối tượng cấp đầu tiên thuộc về các tổ chức chuẩn hóa khác nhau. Trong khi cấp thấp hơn thì được gán bởi các tổ chức tương ứng ở mức trên. Các nhà sản xuất có thể định nghĩa các nhánh riêng để định nghĩa cho các đối tượng được quản lý trên các sản phẩm riêng của họ. MIB vẫn chưa được chuẩn hóa cho nên nó được đặt trong nhánh thử nghiệm (experimental).

Ví dụ: đối tượng được quản lý atInput định vị tại đường dẫn được mô tả theo dạng tên là: « iso.IDentified-organization.dod.internet.private.enterprise.cisco.temporaryvariables.AppleTalk.atInput » hoặc theo dạng số là chuỗi số « 1.3.6.1.4.1.9.3.3.1 ».

Chương 9

Thiết kế mạng cục bộ LAN

Mục đích

Chương này nhằm giới thiệu cho người đọc những vấn đề sau :

- Tiến trình thiết kế mạng LAN
- Lập sơ đồ thiết kế mạng LAN
    - Sơ đồ mạng tầng vật lý
    - Nối kết tầng 2 bằng switch
    - Thiết kế mạng ở tầng 3
    - Xác định vị trí đặt Server
- Cách làm tài liệu, hồ sơ mạng

9.1 Giới thiệu tiến trình thiết kế mạng LAN

Một trong những bước quan trọng nhất để đảm bảo một hệ thống mạng nhanh và ổn định chính là khâu thiết kế mạng. Nếu một mạng không được thiết kế kỹ lưỡng, nhiều vấn đề không lường trước sẽ phát sinh và khi mở rộng mạng có thể bị mất ổn định. Thiết kế mạng bao gồm các tiến trình sau:

- Thu thập thông tin về yêu cầu và mong muốn của người sử dụng mạng.
- Xác định các luồng dữ liệu hiện tại và trong tương có hướng đến khả năng phát triển trong tương lai và vị trí đặt các server.
- Xác định tất cả các thiết bị thuộc các lớp 1,2 và 3 cần thiết để cho sơ đồ mạng LAN và WAN.
- Làm tài liệu cài đặt mạng ở mức vật lý và mức luận lý.

Sẽ có nhiều giải pháp thiết kế cho cùng một mạng. Việc thiết kế mạng cần hướng đến các mục tiêu sau:

- Khả năng vận hành: Tiêu chí đầu tiên là mạng phải hoạt động. Mạng phải đáp ứng được các yêu cầu về công việc của người sử dụng, phải cung cấp khả năng kết nối giữa những người dùng với nhau, giữa người dùng với ứng dụng với một tốc độ và độ tin cậy chấp nhận được.
- Khả năng mở rộng: Mạng phải được mở rộng. Thiết kế ban đầu phải được mở rộng mà không gây ra một sự thay đổi lớn nào trong thiết kế tổng thể.
- Khả năng tương thích: Mạng phải được thiết kế với một cặp mặt luôn hướng về các công nghệ mới và phải đảm bảo rằng không ngăn cản việc đưa vào các công nghệ mới trong tương lai.
- Có thể quản lý được: Mạng phải được thiết kế sao cho dễ dàng trong việc theo dõi và quản trị để đảm bảo sự vận hành suôn sẻ của các tính năng.

Chương này chủ yếu tập trung vào tiến trình thiết kế mạng và vấn đề làm tài liệu.

9.2 Lập sơ đồ thiết kế mạng

Sau khi các yêu cầu cho một mạng tổng thể đã được thu thập, bước kế tiếp là xây dựng sơ đồ mạng (topology) hay mô hình mạng cần được thiết lập. Việc thiết kế sơ đồ mạng được chia ra thành 3 bước:

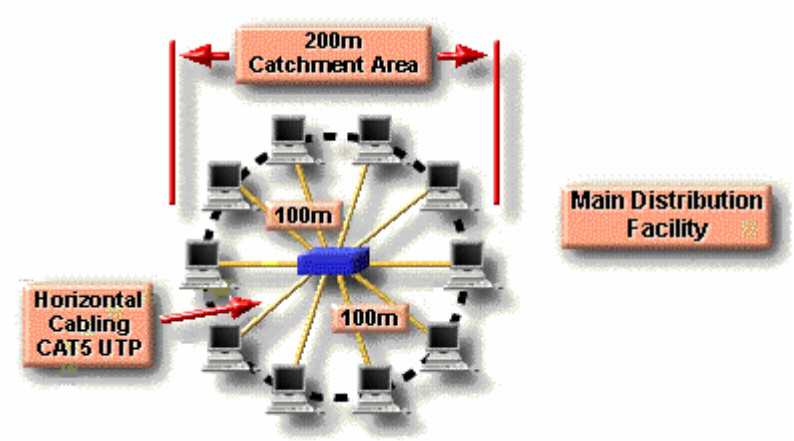
- Thiết kế sơ đồ mạng ở tầng vật lý
- Thiết kế sơ đồ mạng ở tầng liên kết dữ liệu
- Thiết kế sơ đồ mạng ở tầng mạng.

9.2.1 Phát triển sơ đồ mạng ở tầng vật lý

Sơ đồ đi dây là một trong những vấn đề cần phải được xem xét khi thiết kế một mạng. Các vấn đề thiết kế ở mức này liên quan đến việc chọn lựa loại cáp được sử dụng, sơ đồ đi dây cáp phải thỏa mãn các ràng buộc về băng thông và khoảng cách địa lý của mạng.

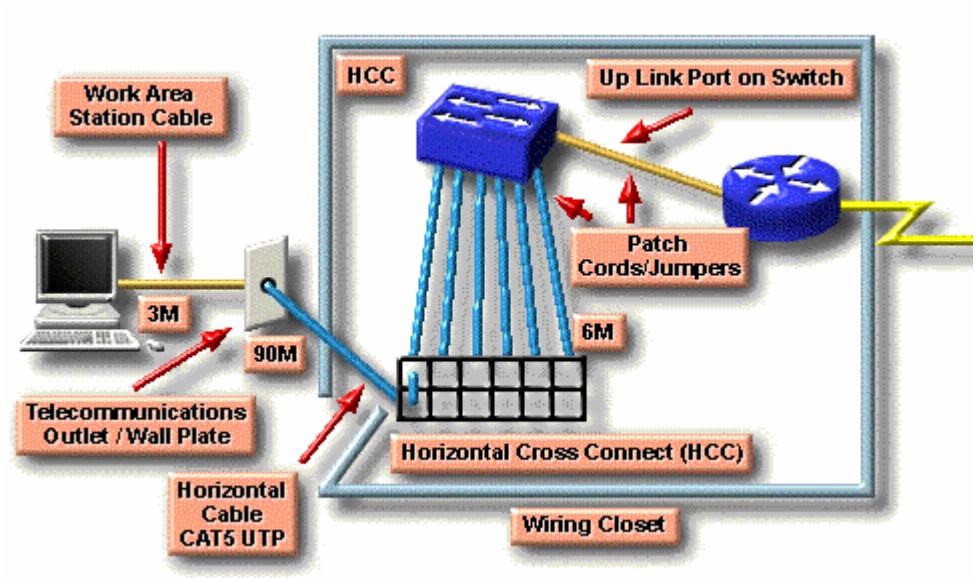
Sơ đồ mạng hình sao sử dụng cáp xoắn đôi CAT 5 thường được dùng hiện nay. Đối với các mạng nhỏ, chỉ cần một điểm tập trung nối kết cho tất cả các máy tính với điều kiện rằng khoảng cách từ máy tính đến điểm tập trung nối kết là không quá 100 mét.

Thông thường, trong một tòa nhà người ta chọn ra một phòng đặc biệt để lắp đặt các thiết bị mạng như Hub, switch, router hay các bảng cấm dây (patch panels). Người ta gọi phòng này là đi Nơi phân phối chính MDF (Main distribution facility).



Hình 9.1 – Sử dụng MDF cho các mạng có đường kính nhỏ hơn 200 mét

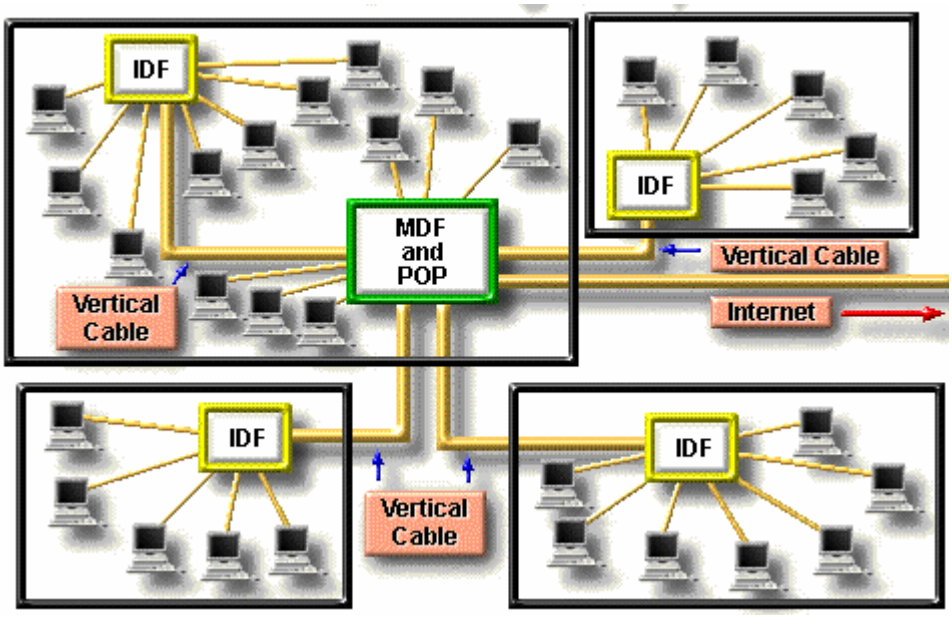
Đối với các mạng nhỏ với chỉ một điểm tập trung nối kết, MDF sẽ bao gồm một hay nhiều các bảng cấm dây nối kết chéo nằm ngang (HCC – Horizontal Cross Connect patch panel).



Hình 9.2 – Sử dụng HCC patch panel trong MDF

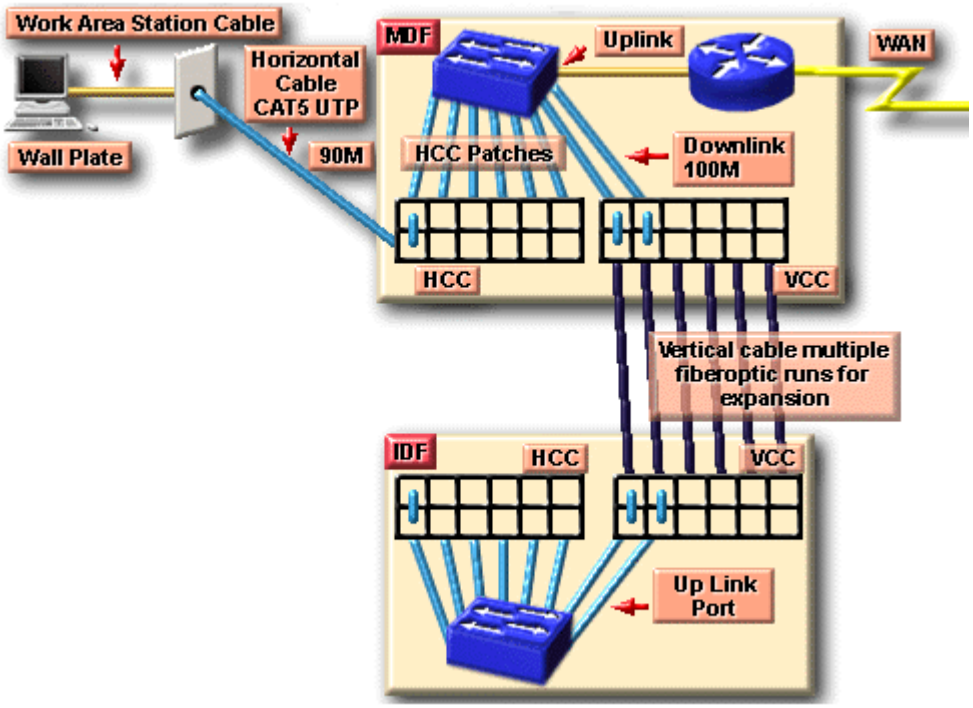
Số lượng cáp chiều ngang (Hirizontal Cable) và kích thước của HCC patch panel (số lượng cổng) phụ thuộc vào số máy tính nối kết vào mạng.

Khi chiều dài từ máy tính đến điểm tập trung nối kết lớn hơn 100 mét, ta phải cần thêm nhiều điểm tập trung nối kết khác. Điểm tập trung nối kết ở mức thứ hai được gọi là Nơi phân phối trung gian (IDF –Intermediate Distribution Facility). Dây cáp để nối IDF về MDF được gọi là cáp đứng (Vertical cabling).



Hình 9.3 – Sử dụng thêm các IDF cho các mạng có đường kính lớn hơn 200 mét

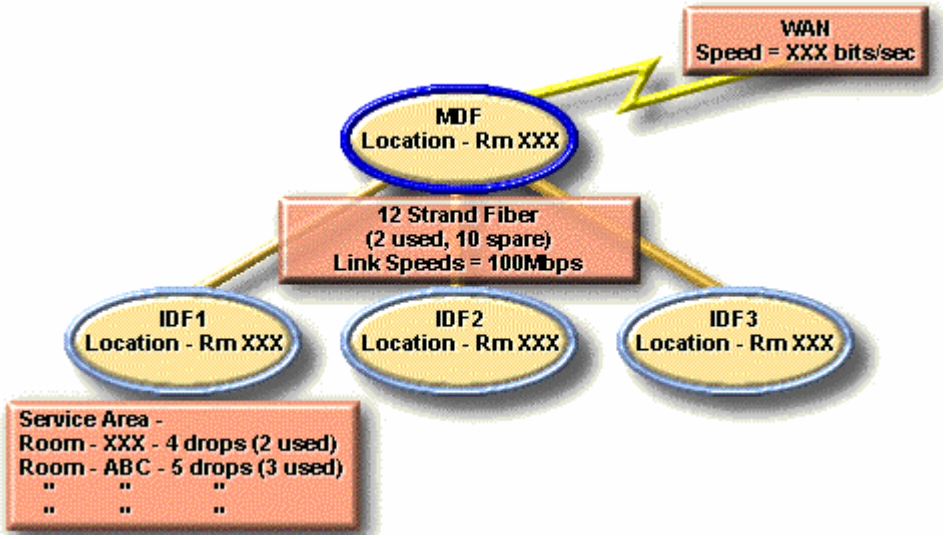
Để có thể nối các IDF về một MDF cần sử dụng thêm các patch panel nối kết chéo chiều đứng (VCC – Vertical Cross Connect Patch Panel). Dây cáp nối giữa hai VCC patch panel được gọi là cáp chiều đứng (Vertical Cabling). Chúng có thể là cáp xoắn đôi nếu khoảng cách giữa MDF và IDF không lớn hơn 100 mét. Ngược lại phải dùng cáp quang khi khoản cách này lớn hơn 100 mét. Tốc độ của cáp chiều đứng thường là 100 Mbps hoặc 1000 Mbps.



Hình 9.4 – Sử dụng VCC patch panel để nối IDF với MDF

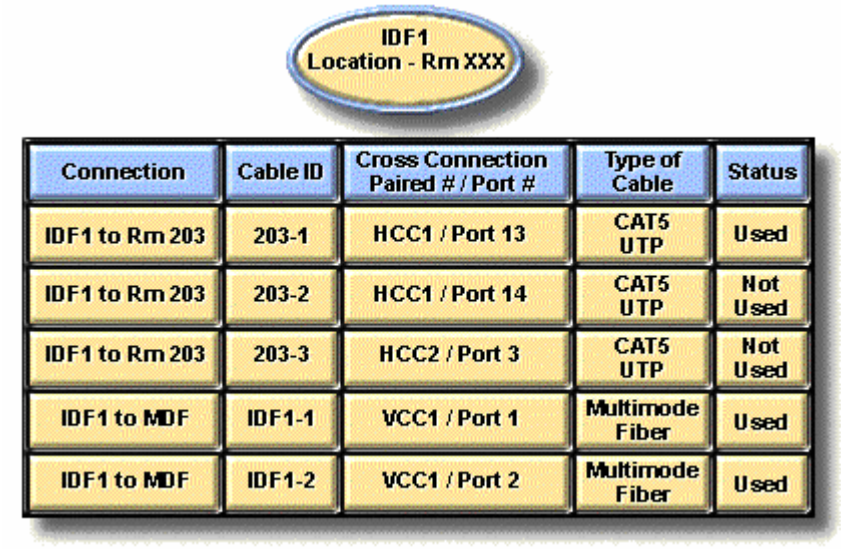
Sản phẩm của giai đoạn này là một bộ tài liệu đặc tả các thông tin sau:

- Vị trí chính xác của các điểm tập trung nối kết MDF và IDFs.
- Kiểu và số lượng cáp được sử dụng để nối các IDF về MDF



Hình 9.5 – Tài liệu về vị trí của MDF và các IDF

- Các đầu dây cáp phải được đánh số và ghi nhận sự nối kết giữa các cổng trên HCC và VCC patch panel. Ví dụ dưới đây ghi nhận về thông tin các sợi cáp được sử dụng tại IDF số 1

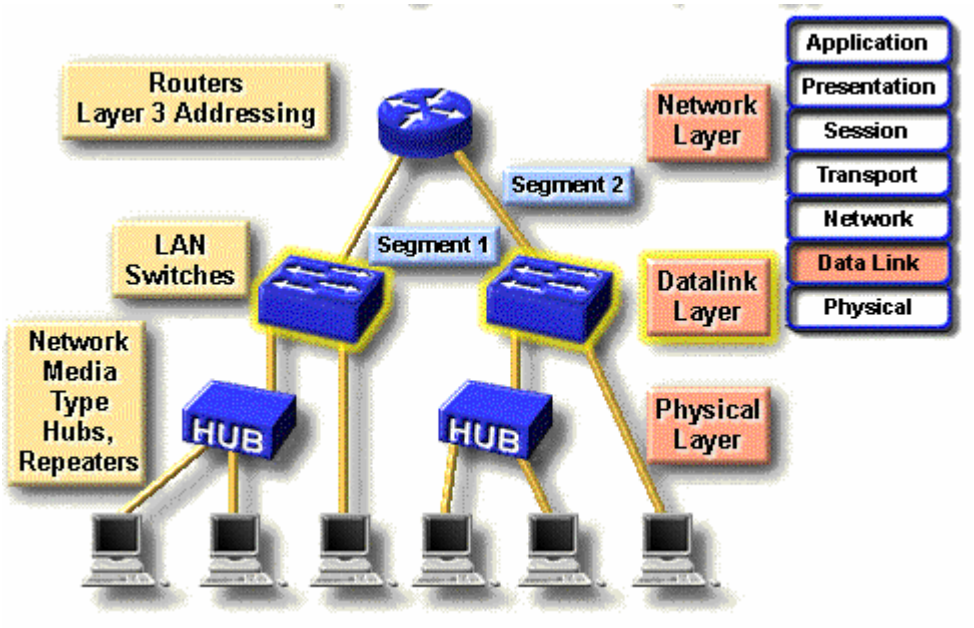


Connection	Cable ID	Cross Connection Paired # / Port #	Type of Cable	Status
IDF1 to Rm 203	203-1	HCC1 / Port 13	CAT5 UTP	Used
IDF1 to Rm 203	203-2	HCC1 / Port 14	CAT5 UTP	Not Used
IDF1 to Rm 203	203-3	HCC2 / Port 3	CAT5 UTP	Not Used
IDF1 to MDF	IDF1-1	VCC1 / Port 1	Multimode Fiber	Used
IDF1 to MDF	IDF1-2	VCC1 / Port 2	Multimode Fiber	Used

Hình 9.6 – Tài liệu về dây nối tại một IDF

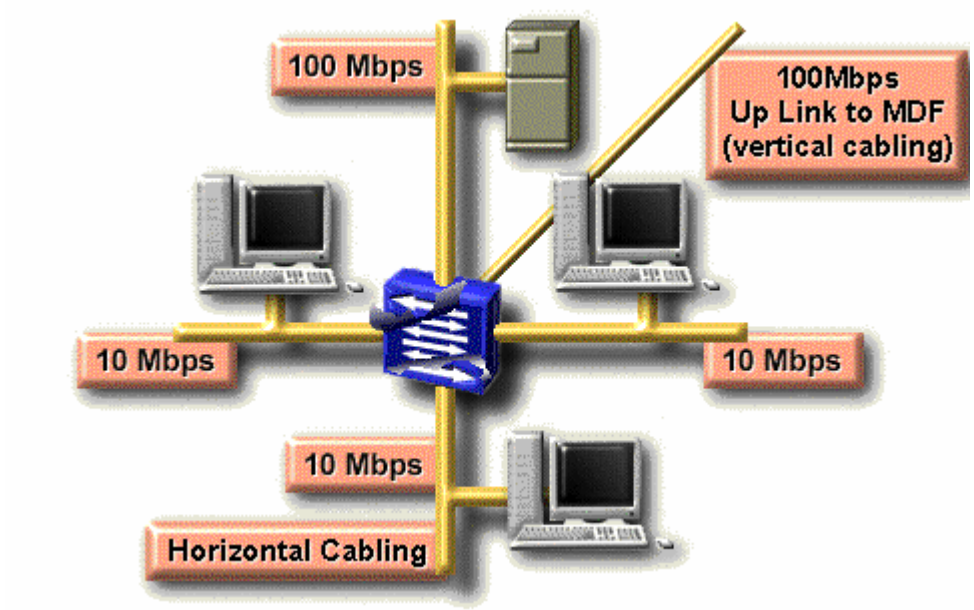
9.2.2 Nối kết tầng 2 bằng switch

Sự đụng độ và kích thước vùng đụng độ là hai yếu tố ảnh hưởng đến hiệu năng của mạng. Bằng cách sử dụng các switch chúng ta có thể phân nhỏ các nhánh mạng nhờ đó có thể giảm bớt được tuần suất đụng độ giữa các máy tính và giảm được kích thước của vùng đụng độ trong mạng.



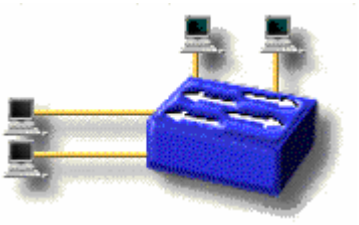
Hình 9.7 – Sử dụng Switch để mở rộng băng thông mạng

Một ưu thế nữa đối với các switch bất đối xứng là nó có hỗ trợ một số cổng có thông lượng lớn dành cho các server hoặc các cáp chiều dứng để nối lên các switch / router ở mức cao hơn.



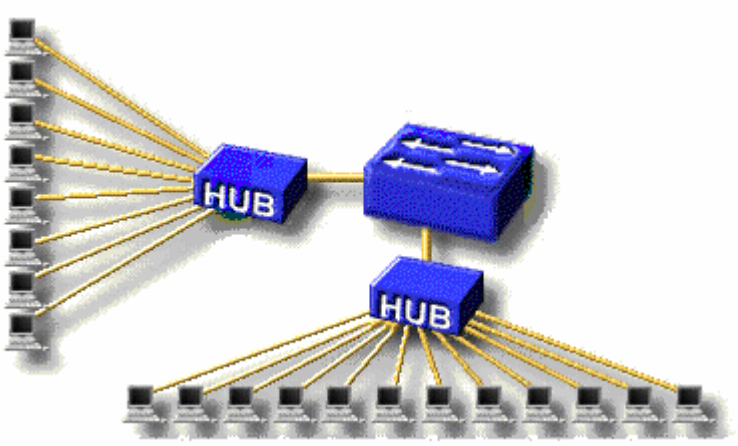
Hình 9.8 – Sử dụng cổng tốc độ cao trong switch

Để xác định kích thước của vùng đụng độ bạn cần phải xác định bao nhiêu máy tính được nối kết vật lý trên từng cổng của switch. Trường hợp lý tưởng mỗi cổng của switch chỉ có một máy tính nối vào, khi đó kích thước của vùng đụng độ là 2 vì chỉ có máy gởi và máy nhận tham gia vào mỗi cuộc giao tiếp.



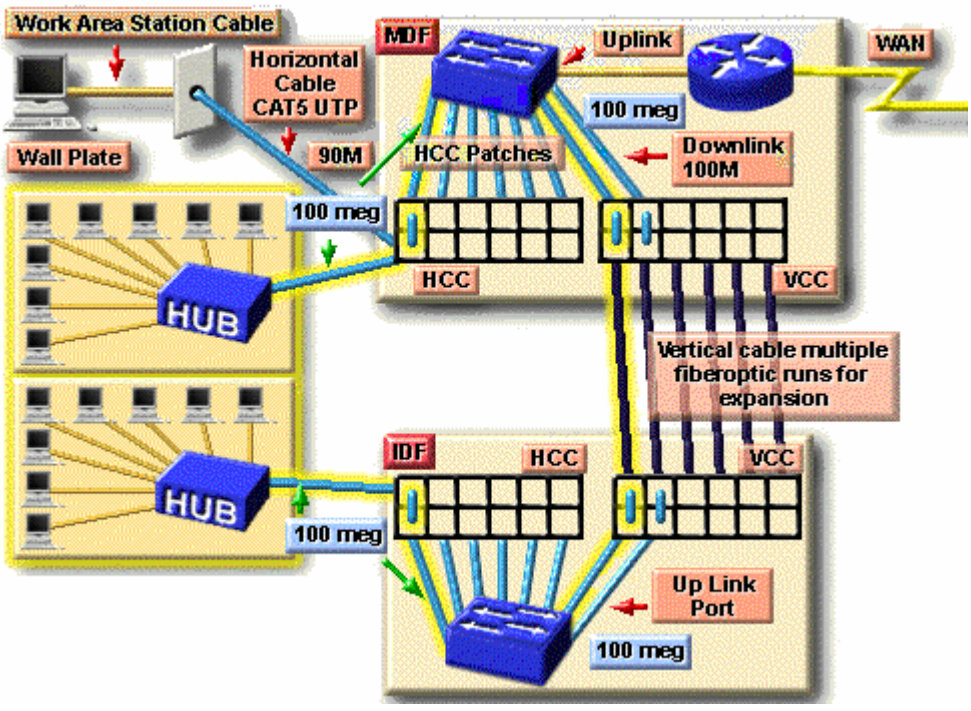
Hình 9.9 – Nối trực tiếp các máy tính vào switch

Trong thực tế ta thường dùng switch để nối các Hub lại với nhau. Khi đó mỗi Hub sẽ tạo ra một vùng đụng độ và các máy tính trên mỗi Hub sẽ chia sử nhau băng thông trên Hub.



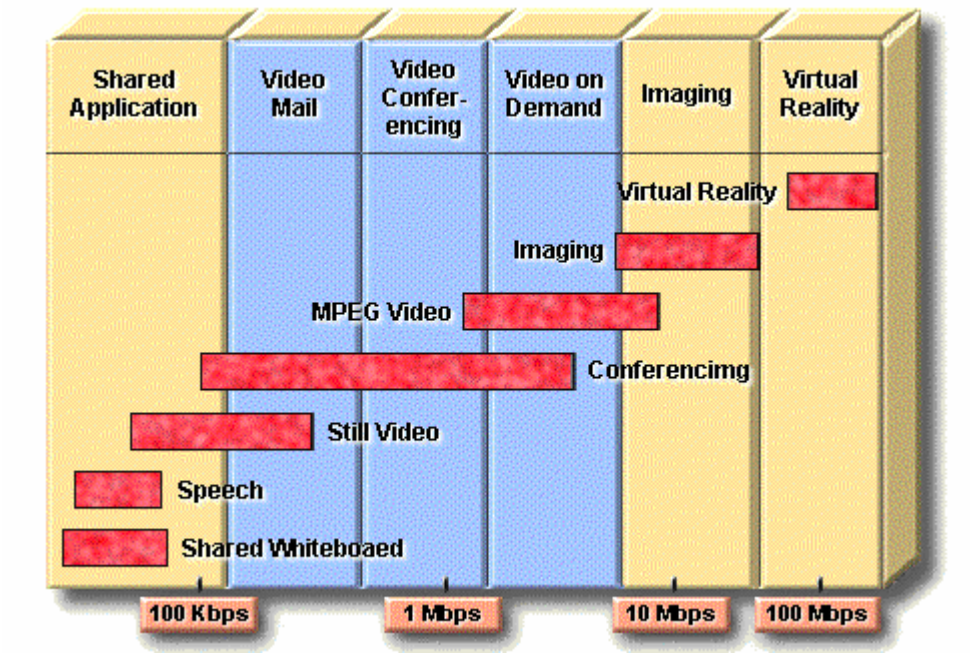
Hình 9.10 – Nối HUB vào switch

Thông thường người ta sử dụng Hub để tăng số lượng các điểm nối kết vào mạng cho máy tính. Tuy nhiên cần phải đảm bảo số lượng máy tính trong từng vùng đụng độ phải nhỏ và đảm bảo băng thông cho từng máy tính một. Đa số các Hub hiện nay đều có hỗ trợ một cổng tốc độ cao hơn các cổng còn lại (gọi là up-link port) dùng để nối kết với switch để tăng băng thông chung cho toàn mạng.



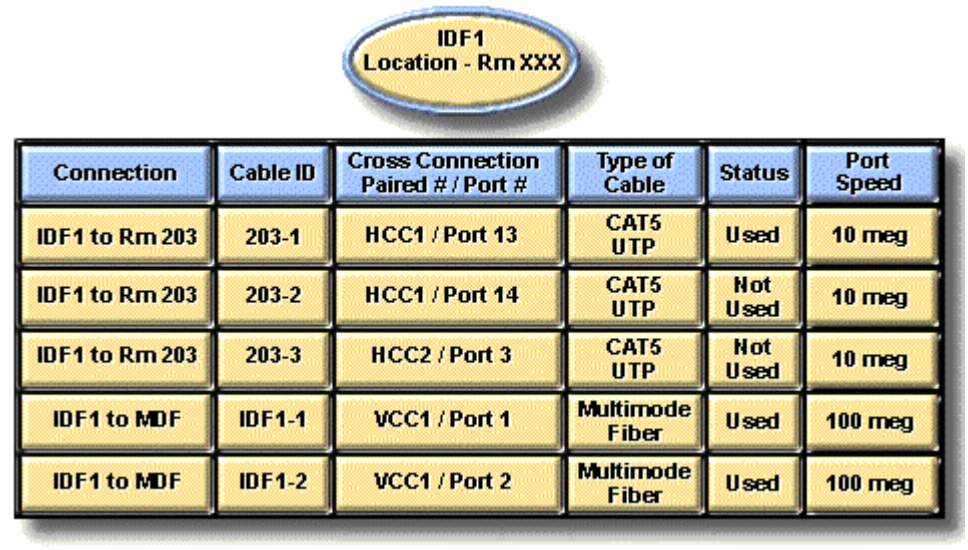
Hình 9.11 – Sử dụng cổng tốc độ cao của HUB để nối với Switch

Băng thông cần thiết cho các ứng dụng được mô tả như hình dưới đây:



Hình 9.12 – Nhu cầu băng thông của các ứng dụng

Sau khi đã thiết kế xong sơ đồ mạng ở tầng hai, cần thiết phải ghi nhận lai thông tin về tốc độ của các cổng nối kết cáp như hình dưới đây:

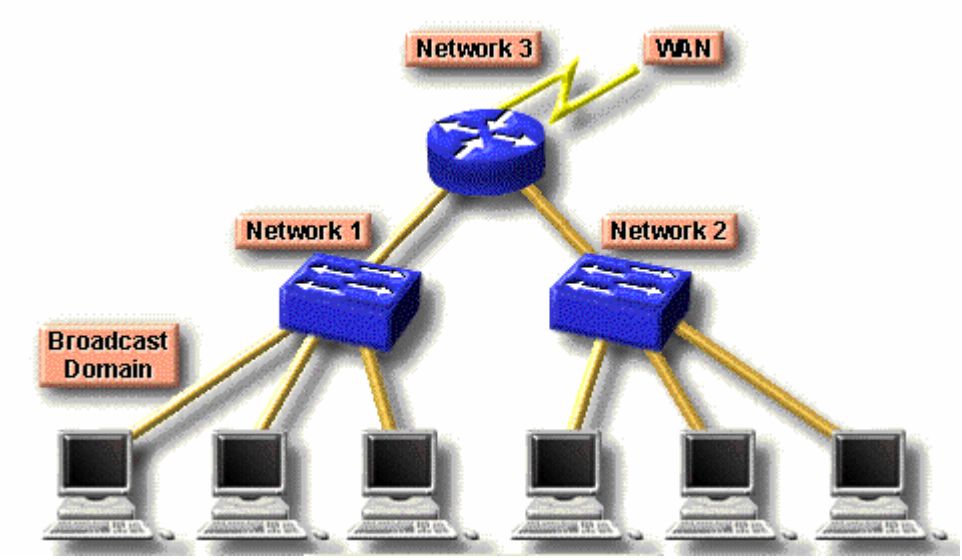


Connection	Cable ID	Cross Connection Paired # / Port #	Type of Cable	Status	Port Speed
IDF1 to Rm 203	203-1	HCC1 / Port 13	CAT5 UTP	Used	10 meg
IDF1 to Rm 203	203-2	HCC1 / Port 14	CAT5 UTP	Not Used	10 meg
IDF1 to Rm 203	203-3	HCC2 / Port 3	CAT5 UTP	Not Used	10 meg
IDF1 to MDF	IDF1-1	VCC1 / Port 1	Multimode Fiber	Used	100 meg
IDF1 to MDF	IDF1-2	VCC1 / Port 2	Multimode Fiber	Used	100 meg

Hình 9.13 – Tài liệu về tốc độ trên từng cổng

9.2.3 Thiết kế mạng ở tầng 3

Sử dụng các thiết bị nối kết mạng ở tầng 3 như router, cho phép phân nhánh mạng thành các mođun tách rời nhau về mặt vật lý cũng như luận lý. Router cũng cho phép nối kết mạng với mạng diện rộng như mạng Internet chẳng hạn.

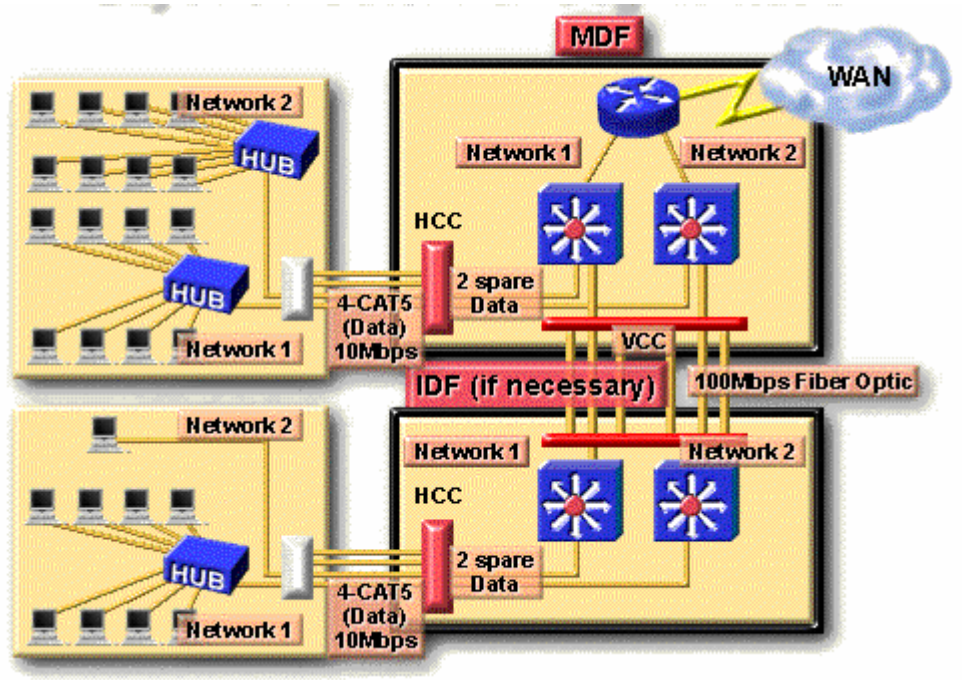


Hình 9.14 – Sử dụng router trong mạng

Router cho phép hạn chế được các cuộc truyền quảng bá xuất phát từ một vùng đụng độ này lan truyền sang các vùng đụng độ khác. Nhờ đó tăng băng thông trên toàn mạng. Đối với switch, gói tin gởi cho một máy tính mà nó chưa biết sẽ được truyền đi ra tất cả các cổng để đến tất cả các nhánh mạng khác.

Ngoài ra, router còn được sử dụng để giải quyết các vấn đề như: một số giao thức không thích hợp khi mạng có kích thước lớn, vấn đề anh ninh mạng và vấn đề về đánh địa chỉ mạng. Tuy nhiên sử dụng router thì đắt tiền và khó khăn hơn trong việc cấu hình nếu so với switch.

Trong ví dụ sau, mạng có nhiều nhánh mạng vật lý, tất cả các thông tin đi trao đổi giữa mạng Network 1 và mạng Network 2 đều phải đi qua router. Router đã chia mạng thành hai vùng đụng độ riêng rời. Mỗi vùng đụng độ có địa chỉ mạng và mặt nạ mạng con riêng.



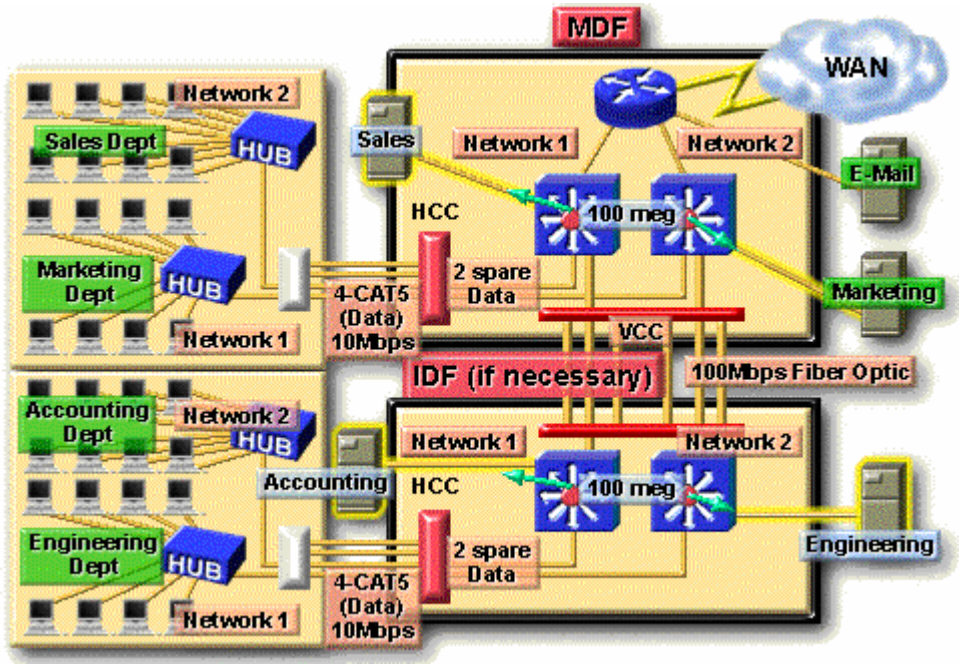
Hình 9.15 – Sử dụng router để phân chia vùng đụng độ trong mạng

9.2.4 Xác định vị trí đặt Server

Các server được chia thành 2 loại: Server cho toàn công ty (Enterprise Server) và server cho nhóm làm việc (Workgroup server).

Enterprise server phục vụ cho tất cả người sử dụng trong công ty, ví dụ như Mail server, DNS server. Chúng thường được đặt tại MDF.

Workgroup server thì chỉ phục vụ cho một số người dùng và thường được đặt tại IDF nơi gần nhóm người sử dụng server này nhất.

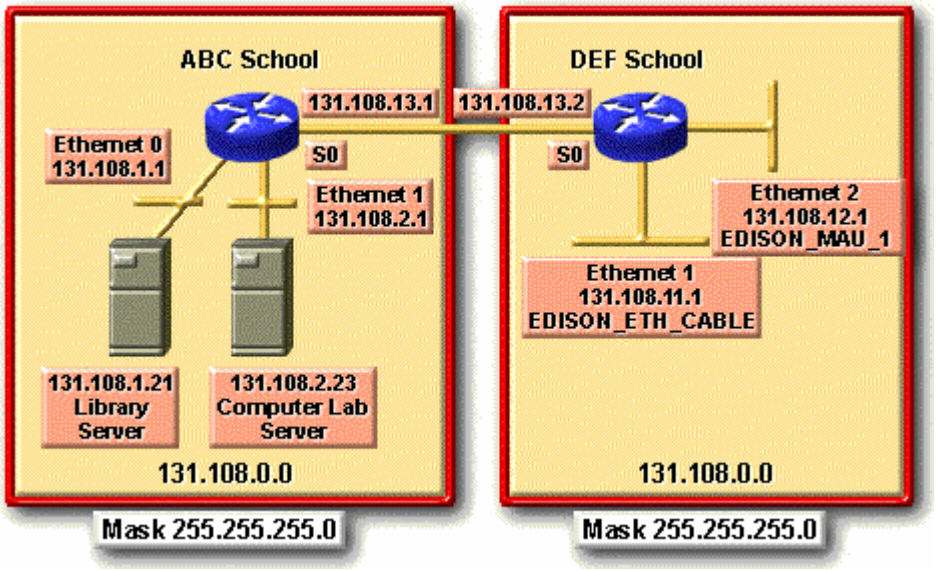


Hình 9.16 – Tài liệu về vị trí đặt các server

9.2.5 Lập tài liệu cho tầng 3

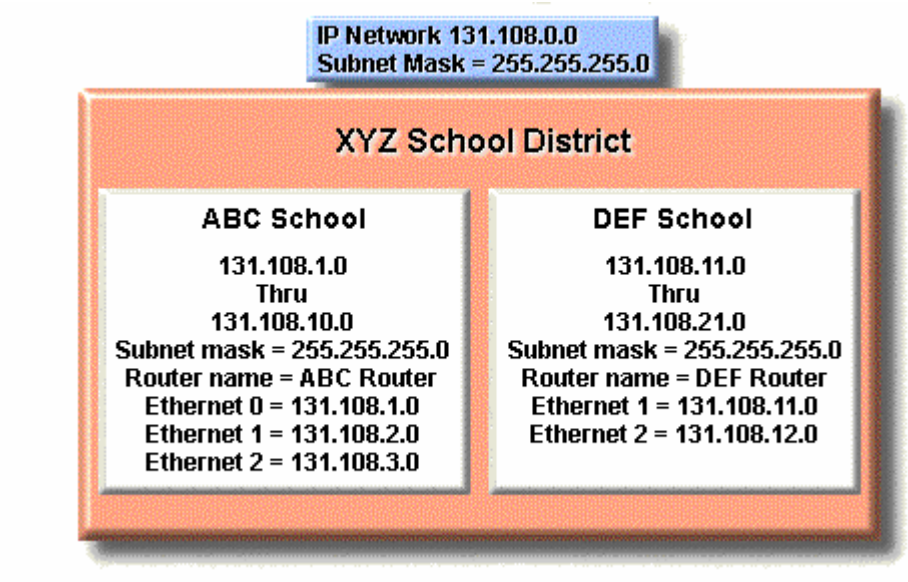
Sau khi xây dựng sơ đồ cấp phát địa chỉ, bạn cần ghi nhận lại chiến lược cấp phát địa chỉ. Một số các tài liệu cần tạp ra bao gồm:

- Bảng đồ phân bố địa chỉ



Hình 9.17 – Bảng đồ phân bố địa chỉ IP

- Bảng tóm tắt về các mạng đã được phân bố, địa chỉ các giao diện của từng router và bảng chọn đường của các router.



Hình 9.18 – Bảng tóm tắt về địa chỉ đã phân bố

MỤC LỤC