

ĐẠI HỌC DUY TÂN

Đại học Tư thục đầu tiên & lớn nhất Miền Trung



Hệ đào tạo:

Thạc sĩ
Cử nhân Đại học, Cử nhân Cao đẳng
Trung cấp

Ngành Đào tạo:

Ngành Công nghệ Thông tin
Ngành Hệ thống Thông tin Kinh tế
Ngành Điện - Điện tử
Ngành Kế toán
Ngành Quản trị Kinh doanh
Ngành Tài chính Ngân hàng
Ngành Du lịch
Ngành Ngoại ngữ
Ngành Công nghệ Môi trường (bậc Kỹ sư)
Ngành Xây dựng (bậc Kỹ sư)
Ngành Kiến trúc (bậc Kiến trúc sư)
Ngành Khoa học Xã hội & Nhân văn

Loại hình Đào tạo:

Chính quy
Liên thông
Bằng hai
Từ xa
Vừa làm vừa học



ĐẠI HỌC DUY TÂN

NGUYỄN GIA NHƯ - LÊ TRỌNG VĨNH
(Đồng chủ biên)

GIÁO TRÌNH THIẾT KẾ MẠNG

Giáo trình thiết kế mạng



Giá: 30.000đ

NXB TT&TT

NXB THÔNG TIN & TRUYỀN THÔNG

ĐẠI HỌC DUY TÂN
Nguyễn Gia Như - Lê Trọng Vĩnh
(Đồng chủ biên)

Giao trình thiết kế mạng

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

Mã số: GD 07 ĐM 11

LỜI NÓI ĐẦU

Sự bùng nổ của Internet trong vài thập kỷ qua đã làm cho khái niệm *Mạng máy tính* ngày càng trở nên thân thuộc với moi người. Internet là một hệ thống thông tin toàn cầu có thể được truy nhập công cộng, gồm các mạng máy tính được liên kết với nhau và truyền thông tin theo phương thức chuyển mạch gói (Packet Switching) dựa trên một giao thức liên mạng đã được chuẩn hóa (giao thức IP). Hệ thống này bao gồm hàng triệu triệu mạng máy tính nhỏ hơn của các doanh nghiệp, viện nghiên cứu, trường đại học, các chính phủ trên toàn cầu và cả người dùng cá nhân...

Với mục đích trang bị cho Sinh viên, Học viên Cao học chuyên ngành Công nghệ Thông tin, Khoa học Máy tính, Tin học, Người sử dụng... những kiến thức cơ bản về mạng máy tính để thiết kế các mạng máy tính trong thực tiễn; Nhóm tác giả Khoa Công nghệ Thông tin, Trường Đại học Duy Tân; Khoa Toán – Cơ – Tin học, Trường Đại học Khoa học Tự nhiên, Đại học Quốc gia Hà Nội đã phối hợp với Nhà xuất bản Thông tin và Truyền thông xuất bản cuốn “**Giáo trình Thiết kế Mạng**”. Nội dung giáo trình gồm 4 chương, cụ thể như sau:

Chương 1: Tổng quan về Thiết kế mạng

Chương 2: Thiết kế Mạng cục bộ

Chương 3: Mạng cục bộ không dây

Chương 4: Thiết kế Mạng diện rộng

Sau khi nghiên cứu giáo trình này, người đọc có thể nắm vững về vai trò, nguyên lý trao đổi thông tin giữa các thành phần tham gia vào

mạng. Điều đó sẽ giúp ích rất nhiều cho công việc thiết kế các mạng nhằm triển khai dễ dàng, quản lý và khai thác hiệu quả theo đúng mục đích, nhu cầu đặt ra.

Do thời gian có hạn, mặc dù đã có nhiều cố gắng trong công tác biên soạn song giáo trình được xuất bản lần đầu sẽ khó tránh khỏi các sai sót. Các tác giả rất mong nhận được sự đóng góp ý kiến của bạn đọc để giáo trình được hoàn thiện hơn trong lần tái bản sau.

Mọi góp ý xin được gửi email về địa chỉ vinhlt@vnu.edu.vn hoặc nguyengianhu@duytan.edu.vn.

Để hoàn thành cuốn sách này, chúng tôi đã nhận được những góp ý quý báu của các Anh chị đồng nghiệp. Xin gửi lời cảm ơn đến ThS. Nguyễn Minh Nhật, bạn Võ Nhân Văn đã có nhiều ý kiến đóng góp xác đáng về nội dung và cách trình bày của cuốn giáo trình này.

Dà Nẵng, tháng 4, năm 2011

NHÓM TÁC GIẢ

Chương 1

TỔNG QUAN VỀ THIẾT KẾ MẠNG



Chương này nhằm giới thiệu tổng quan về tiến trình thiết kế mạng máy tính. Tiến trình xây dựng một mạng máy tính cũng trải qua các giai đoạn như việc xây dựng và phát triển một phần mềm. Đó là các quá trình 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 (thiết kế mô hình logic, thiết kế mô hình vật lý), Cài đặt mạng, Kiểm thử và cuối cùng là Bảo trì mạng.

Chương 1 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. 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 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*.

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 về 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 ban 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 gửi 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, lộn xộn... vì 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

Quá trình phân tích yêu cầu mạng máy tính đòi hỏi phải hiểu được người dùng cần gì, hiểu biết các ứng dụng sẽ được triển khai cũng như các thiết bị cần thiết khác cho mạng sẽ triển khai.

Phân tích mạng là quá trình định nghĩa, xác định và mô tả mối quan hệ giữa người sử dụng, ứng dụng, thiết bị trong mạng. Trong quá trình đó, phân tích mạng cung cấp nền tảng cho tất cả các quyết định kiến trúc và thiết kế để làm theo.

Mục đích của phân tích mạng là hiểu người dùng cần gì và hiểu được hệ thống sẽ như thế nào. Trong quá trình phân tích một mạng phải kiểm tra trạng thái của mạng hiện có, bao gồm bất cứ vấn đề có thể gặp phải.

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? (Workgroup 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

Thiết kế giải pháp mạng cung cấp chi tiết giải pháp về vật lý cho kiến trúc mạng. Thiết kế mạng là khâu quan trọng tiếp nối các bước phân tích và kiến trúc mạng. Quá trình thiết kế bao gồm các tài liệu và bản vẽ kỹ thuật của hệ thống mạng, lựa chọn nhà cung cấp thiết bị và dịch vụ, lựa chọn thiết bị (bao gồm loại thiết bị và cấu hình tương ứng).

Trong quá trình thiết kế mạng, nên sử dụng qui trình đánh giá đối với nhà cung cấp thiết bị, nhà cung cấp dịch vụ cũng như lựa chọn thiết bị dựa trên đầu vào của qui trình phân tích và kiến trúc mạng.

Chúng ta sẽ tìm hiểu làm thế nào để thiết lập mục tiêu thiết kế, chẳng hạn như giảm thiểu chi phí mạng nhưng lại tối ưu hóa hiệu năng mạng, cũng như làm thế nào để đạt được các mục tiêu này, thông qua hiệu suất mạng và chức năng với mục tiêu thiết kế mạng.

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 logic

Thiết kế sơ đồ mạng ở mức logic 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 email 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 mức vật lý

Căn cứ vào sơ đồ thiết kế mạng ở mức logic, 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, Windows 2003, Windows 2008, 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 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 phần 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 logic 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. CÂU HỎI ÔN TẬP

Câu 1: Trình bày các công đoạn thiết kế một mạng máy tính? Theo bạn thì công đoạn nào là quan trọng nhất?

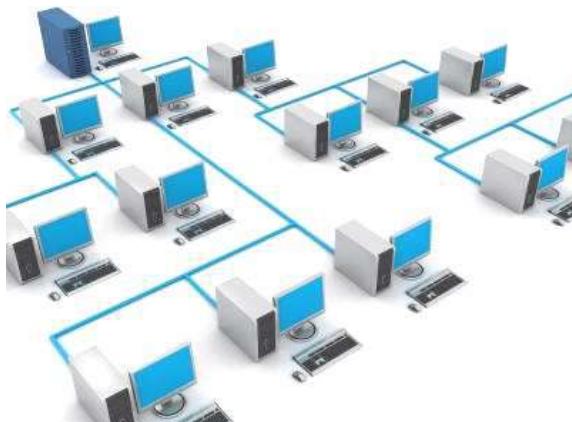
Câu 2: Bạn hãy cho một ví dụ về thu thập các yêu cầu của khách hàng?

Câu 3: Tại sao việc tìm hiểu về đường lối kinh doanh của khách hàng là quan trọng?

Câu 4: Hiện nay, một số mục tiêu kinh doanh điển hình trong các tổ chức là gì?

Chương 2

THIẾT KẾ MẠNG CỤC BỘ



Chương này giới thiệu các vấn đề cơ bản về mạng cục bộ (LAN), các công nghệ mạng LAN thông dụng. Đồng thời, đi sâu giới thiệu về thiết kế hạ tầng cáp mạng, thiết kế mạng LAN trên lớp 2 và lớp 3. Phần cuối chương có các bài tập ứng dụng để người đọc hiểu rõ thêm về thiết kế LAN cũng như thực hành thiết kế LAN.

2.1. PHÂN LOẠI MẠNG

Có nhiều cách để phân loại các mạng khác nhau, phần này chỉ nêu những cách thức phân loại mạng thường dùng trong thực tế

2.1.1. Phân loại mạng theo vùng địa lý

Mạng cục bộ LAN (Local Area Network): là một hệ thống mạng dùng để kết nối các máy tính trong một phạm vi nhỏ (nhà ở, phòng làm việc, trường học...). Các máy tính trong mạng LAN có thể chia sẻ tài nguyên với nhau (chia sẻ tập tin, máy in, máy quét và một số thiết bị khác).

- Phạm vi địa lý nhỏ
- Tốc độ cao và đáng tin cậy
- Ethernet, Wifi, FDDI, ATM ...

Mạng đô thị MAN (Metropolitan Area Network): là mạng dữ liệu băng rộng được thiết kế cho phạm vi trong thành phố, thị xã. Khoảng cách thường nhỏ hơn 50 km. Xét về quy mô địa lý, MAN lớn hơn mạng LAN nhưng nhỏ hơn mạng WAN, MAN đóng vai trò kết nối 2 mạng LAN và WAN với nhau hoặc kết nối giữa các mạng LAN. Kết nối giữa các phần tử của mạng MAN thường sử dụng loại không dây (Wireless) hoặc sử dụng cáp quang (Optical Fiber).

Mạng diện rộng WAN (Wide Area Network): là mạng dữ liệu được thiết kế để kết nối giữa các mạng đô thị (mạng MAN), giữa các khu vực địa lý cách xa nhau.

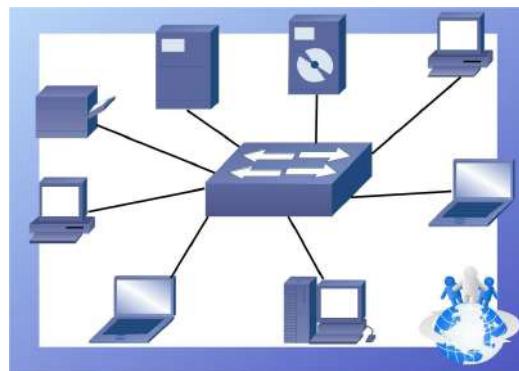
- Phạm vi địa lý rộng lớn
- Tốc độ đảm bảo tỉ lệ lỗi chấp nhận được
- Công nghệ chuyển mạch

Mạng LAN sử dụng kỹ thuật mạng quảng bá (Broadcast network), trong đó các thiết bị cùng chia sẻ 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 vật lý, trong mạng WAN còn sử dụng các kỹ thuật đa hợp và phân hợp.

2.1.2. Phân loại mạng máy tính theo topology mạng

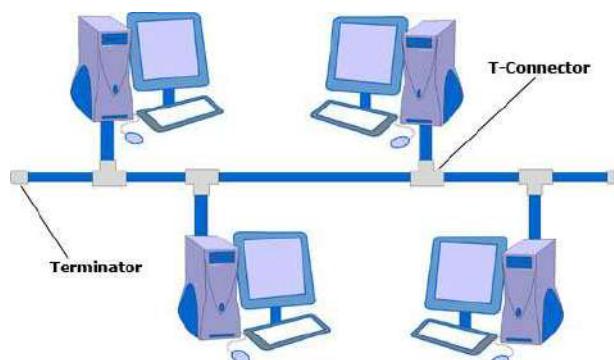
Mạng dạng hình sao (Star topology): Ở dạng hình sao, tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ

các trạm và chuyển tín hiệu đến trạm đích với phương thức kết nối là "điểm - điểm".



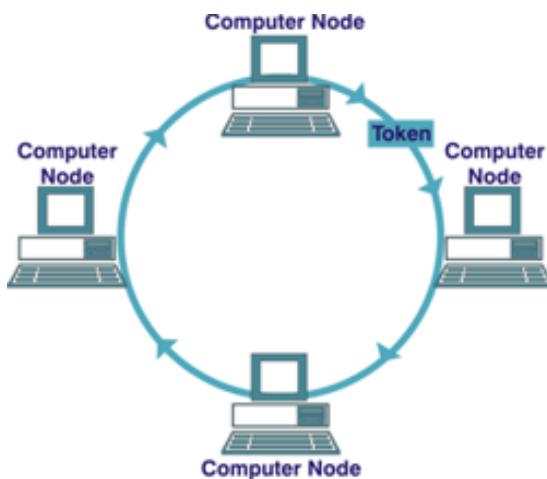
Hình 2.1. Star Topology

Mạng hình tuyén (Bus Topology): Trong dạng hình tuyén, các máy tính đều được nối vào một đường truyền chính (bus). Đường truyền chính này được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là Terminator (dùng để nhận biết là đầu cuối để kết thúc đường truyền tại đây). Mỗi trạm được nối vào bus qua một đầu nối chữ T (T_connector) hoặc một bộ thu phát (transceiver).



Hình 2.2. Bus Topology

Mạng dạng vòng (Ring Topology): Các máy tính được liên kết với nhau thành một vòng tròn theo phương thức "điểm - điểm", qua đó mỗi một trạm có thể nhận và truyền dữ liệu theo vòng một chiều và dữ liệu được truyền theo từng gói một.



Hình 2.3. Ring Topology

Mạng dạng kết hợp: Trong thực tế tùy theo yêu cầu và mục đích cụ thể ta có thể thiết kế mạng kết hợp các dạng sao, vòng, tuyến để tận dụng các điểm mạnh của mỗi dạng.

2.1.3. Phân loại mạng máy tính theo chức năng

Mạng khách chủ (Client-Server): Một hay một số máy tính được thiết lập để cung cấp các dịch vụ như file server, mail server, Web server, Printer server,... Các máy tính được thiết lập để cung cấp các dịch vụ này được gọi là Server, còn các máy tính truy cập và sử dụng dịch vụ thì được gọi là Client.

Mạng ngang hàng (Peer-to-Peer): Các máy tính trong mạng có thể hoạt động vừa như một Client vừa như một Server.

Mạng kết hợp: Các mạng máy tính thường được thiết lập theo cả hai chức năng Client-Server và Peer-to-Peer.

2.2. MẠNG CỤC BỘ VÀ GIAO THỨC ĐIỀU KHIỂN TRUY CẬP ĐƯỜNG TRUYỀN

Khi được cài đặt vào mạng, các máy trạm phải tuân theo những quy tắc định trước để có thể sử dụng đường truyền, đó là phương thức truy nhập. Phương thức truy nhập được định nghĩa là các thủ tục điều hướng

trạm làm việc làm thế nào và lúc nào có thể thâm nhập vào đường dây cáp để gửi hay nhận các gói thông tin. Có 3 phương thức cơ bản.

2.2.1. Giao thức CSMA/CD

Giao thức CSMA/CD (Carrier Sense Multiple Access with Collision Detection) thường dùng cho mạng có cấu trúc hình tuyến, các máy trạm cùng chia sẻ một kênh truyền chung, các trạm đều có cơ hội thâm nhập đường truyền như nhau (Multiple Access).

Tuy nhiên tại một thời điểm thì chỉ có một trạm được truyền dữ liệu mà thôi.

Trước khi truyền dữ liệu, mỗi trạm phải lắng nghe đường truyền để chắc chắn rằng đường truyền rỗng (Carrier Sense).

Trong trường hợp hai trạm thực hiện việc truyền dữ liệu đồng thời, xung đột dữ liệu sẽ xảy ra, các trạm tham gia phải phát hiện được sự xung đột (Collision Detection) và thông báo tới các trạm khác gây ra xung đột, đồng thời các trạm phải ngừng thâm nhập, chờ đợi lần sau trong khoảng thời gian ngẫu nhiên nào đó rồi mới tiếp tục truyền.

Khi lưu lượng các gói dữ liệu cần di chuyển trên mạng quá cao, thì việc xung đột có thể xảy ra với số lượng lớn dẫn đến làm chậm tốc độ truyền tin của hệ thống.

2.2.2. Giao thức truyền thẻ bài (Token passing)

Giao thức này được dùng trong các LAN có cấu trúc vòng sử dụng kỹ thuật chuyển thẻ bài (token) để cấp phát quyền truy nhập đường truyền tức là quyền được truyền dữ liệu đi.

Thẻ bài ở đây là một đơn vị dữ liệu đặc biệt, có kích thước và nội dung (gồm các thông tin điều khiển) được quy định riêng cho mỗi giao thức. Trong đường cáp liên tục có một thẻ bài chạy quanh trong mạng.

Phần dữ liệu của thẻ bài có một bit biểu diễn trạng thái sử dụng của nó (bận hoặc rỗng). Trong thẻ bài có chứa một địa chỉ đích và được luân chuyển tới các trạm theo một trật tự đã định trước. Đối với cấu hình mạng dạng vòng thì trật tự của sự truyền thẻ bài tương đương với trật tự vật lý của các trạm xung quanh vòng.

Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài rồi. Khi đó trạm sẽ đổi bit trạng thái của thẻ bài thành bận, nén gói dữ liệu có kèm theo địa chỉ nơi nhận vào thẻ bài và truyền đi theo chiều của vòng, thẻ bài lúc này trở thành khung mang dữ liệu. Trạm đích sau khi nhận khung dữ liệu này, sẽ copy dữ liệu vào bộ đệm rồi tiếp tục truyền khung theo vòng nhưng thêm một thông tin xác nhận. Trạm nguồn nhận lại khung của mình (theo vòng) đã được nhận đúng, đổi bit bận thành bit rỗi và truyền thẻ bài đi.

Vì thẻ bài chạy vòng quang trong mạng kín và chỉ có một thẻ nên việc đụng độ dữ liệu không thể xảy ra, do vậy hiệu suất truyền dữ liệu của mạng không thay đổi.

Trong các giao thức này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống. Một là việc mất thẻ bài làm cho trên vòng không còn thẻ bài lưu chuyển nữa. Hai là một thẻ bài bận lưu chuyển không dùng trên vòng.

Ưu điểm của giao thức là vẫn hoạt động tốt khi lưu lượng truyền thông lớn. Giao thức truyền thẻ bài tuân thủ đúng sự phân chia của môi trường mạng, hoạt động dựa vào sự xoay vòng tới các trạm.

Việc truyền thẻ bài sẽ không thực hiện được nếu việc xoay vòng bị đứt đoạn. Giao thức phải chứa các thủ tục kiểm tra thẻ bài để cho phép khôi phục lại thẻ bài bị mất hoặc thay thế trạng thái của thẻ bài và cung cấp các phương tiện để sửa đổi logic (thêm vào, bớt đi hoặc định lại trật tự của các trạm).

2.2.3. Giao thức FDDI

FDDI (Fiber Distributed Data Interface) là kỹ thuật dùng trong các mạng cấu trúc vòng, chuyển thẻ bài tốc độ cao bằng phương tiện cáp sợi quang.

FDDI sử dụng hệ thống chuyển thẻ bài trong cơ chế vòng kép. Lưu thông trên mạng FDDI bao gồm 2 luồng giống nhau theo hai hướng ngược nhau.

FDDI thường được sử dụng với mạng trực trên đó những mạng LAN công suất thấp có thể nối vào. Các mạng LAN đòi hỏi tốc độ truyền dữ liệu cao và dải thông lớn cũng có thể sử dụng FDDI.

2.3. 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 khuếch đại (Repeater)
- Bộ tập trung nối kết (HUB)
- Cầu nối (Bridge)
- Bộ chuyển mạch (Switch)
- Bộ chọn đường (Router)

2.3.1. Network Adapter



Hình 2.4. Card mạng

Thành phần đầu tiên nên đề cập tới trong số các thiết bị phần cứng mạng là bộ điều hợp mạng (network adapter). Thiết bị này còn được biết đến với nhiều tên khác nhau như card mạng (network card), card giao diện mạng (NIC - Network Interface Card), , LAN Adapter. Tất cả đều là thuật ngữ chung của cùng một thiết bị phần cứng. Công việc của card mạng là gắn một cách vật lý máy tính để nó có thể tham gia hoạt động truyền thông trong mạng đó.

Điều đầu tiên chúng ta cần biết đến khi nói về card mạng là nó phải được ghép nối phù hợp với phương tiện truyền dẫn mạng (network medium). Network medium chính là kiểu cáp dùng trên mạng. Các mạng

không dây là một mảng khác và không được đề cập chi tiết trong mục này.

Để card mạng ghép phù hợp với phương tiện truyền dẫn mạng là một vấn đề thực sự vì chúng đòi hỏi phải đáp ứng được lượng lớn tiêu chuẩn cạnh tranh bắt buộc. Chẳng hạn, trước khi xây dựng một mạng và bắt đầu mua card mạng, dây cáp, chúng ta phải quyết định xem liệu nên dùng Ethernet, Ethernet đồng trục, Token Ring, Arcnet hay một tiêu chuẩn mạng nào khác. Mỗi tiêu chuẩn mạng có ưu và nhược điểm riêng. Áp dụng loại nào phù hợp nhất với tổ chức mình là điều hết sức quan trọng.

Ngày nay, hầu hết công nghệ mạng được đề cập đến ở trên đều nhanh chóng trở nên mai một. Bây giờ chỉ có một kiểu mạng sử dụng dây nối còn được dùng trong các doanh nghiệp vừa và nhỏ là Ethernet (Fast Ethernet hoặc Gigabit Ethernet).

Card mạng hoạt động ở lớp 1 (Physical Layer: Lớp vật lý) và lớp 2 (Data Link Layer: Lớp liên kết dữ liệu) trong mô hình OSI. Trên NIC địa chỉ MAC Address (layer 2) 48 bit có dạng FF-FF-FF- FF-FF-FF.

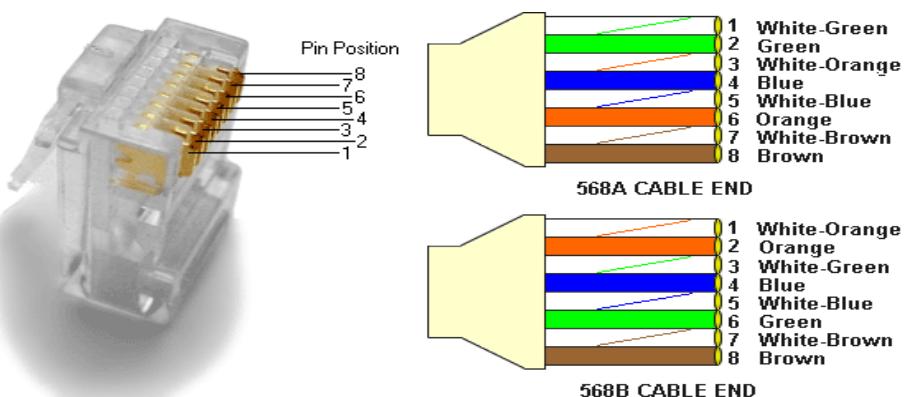
Ví dụ: 00-1B-77-09-BF-1E là một Mac Address.

Các mạng Ethernet hiện đại đều sử dụng cáp xoắn đôi xoắn 8 dây. Các dây này được sắp xếp theo thứ tự đặc biệt và đầu nối RJ-45 được gắn vào phần cuối cáp. Cáp RJ-45 trông giống như bộ kết nối ở phần cuối dây điện thoại, nhưng lớn hơn. Các dây điện thoại dùng chuẩn kết nối RJ-11, tương phản với chuẩn kết nối RJ-45 dùng trong cáp Ethernet.

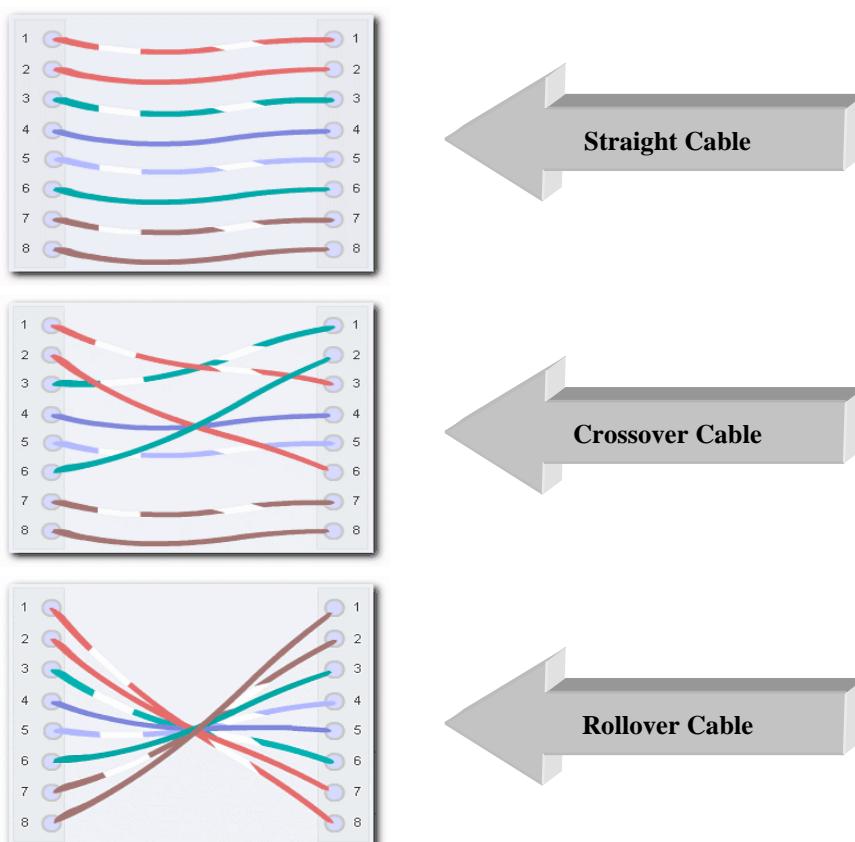


Hình 2.5. Cáp Ethernet với một đầu kết nối RJ-45

Đầu nối RJ-45 và các chuẩn bấm cáp



Hình 2.6. Đầu nối RJ-45 và 2 chuẩn bấm cáp T-568A, T-568B

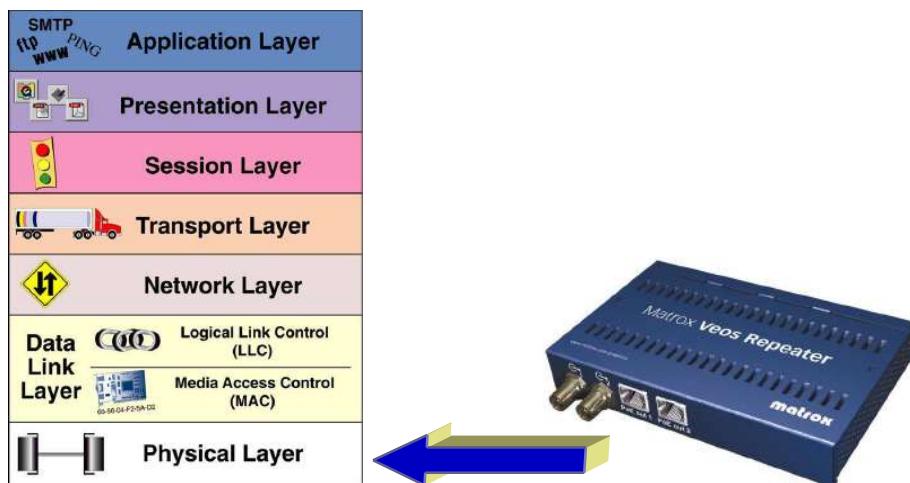


Hình 2.7. Các kiểu cáp mạng

2.3.2. Repeater

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

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



Hình 2.8. Hoạt động của Repeater trong mô hình OSI

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

- Repeater điện nối với đường dây điện ở cả hai phía của nó, nó nhận tín hiệu điện từ một phía và phát lại về phía kia. Khi một mạng sử dụng Repeater điện để nối các phần của mạng lại thì có thể làm tăng khoảng cách của mạng, nhưng khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu. Ví

dụ với mạng sử dụng cáp đồng trực 50 thì khoảng cách tối đa là 2,8km, khoảng cách đó không thể kéo thêm cho dù sử dụng thêm Repeater.

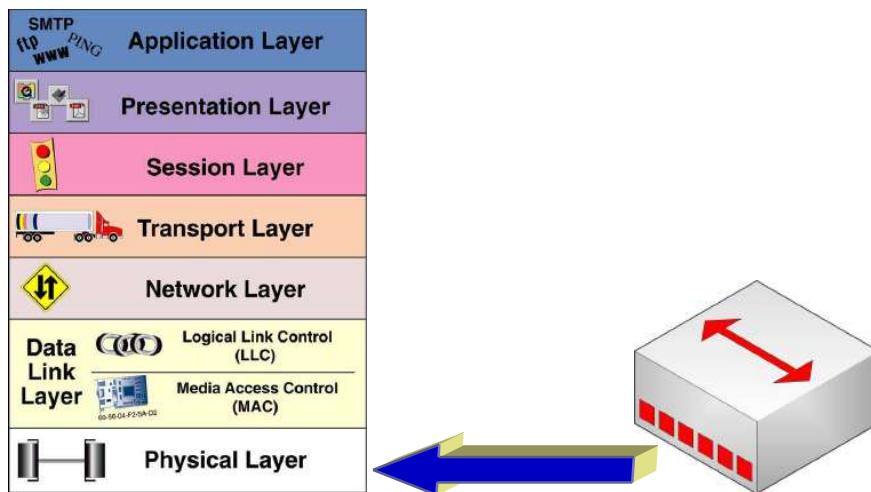
- Repeater điện quang liên kết với một đầu cáp quang và một đầu là cáp điện, nó chuyển một tín hiệu điện từ cáp điện ra tín hiệu quang để phát trên cáp quang và ngược lại. Việc sử dụng Repeater điện quang cũng làm tăng thêm chiều dài của mạng.
- Việc sử dụng Repeater không thay đổi nội dung các tín hiệu đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa Repeater không làm thay đổi khối lượng chuyển vận trên mạng nên việc sử dụng không tính toán nó trên mạng lớn sẽ hạn chế hiệu năng của mạng. Khi lựa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ chuyển vận phù hợp với tốc độ của mạng.

2.3.3. Hub



Hình 2.9. Hub

- Hub hoạt động như một multiport repeater, lắp lại và chuyển tín hiệu điện sang tất cả các cổng có kết nối đến nó.
- Một Hub có từ 4 đến 24 cổng và có thể còn nhiều hơn.
- Khi cấu hình mạng là hình sao (Star topology), Hub đóng vai trò là trung tâm của mạng.



Hình 2.10. Hoạt động của Hub trong mô hình OSI

Hub có hai nhiệm vụ khác nhau:

- Cung cấp một điểm kết nối trung tâm cho tất cả máy tính trong mạng. Mọi máy tính đều được cắm vào hub. Các hub đa cổng có thể được đặt xích lại nhau nếu cần thiết để cung cấp thêm cho nhiều máy tính.
- Sắp xếp các cổng theo cách để nếu một máy tính thực hiện truyền tải dữ liệu, dữ liệu đó phải được gửi đến đích.

Có 3 loại: Passive Hub, Active Hub và Intelligent Hub.

Hub hoạt động ở Layer 1 trong mô hình OSI (Trừ Intelligent Hub - hoạt động ở Layer 2).

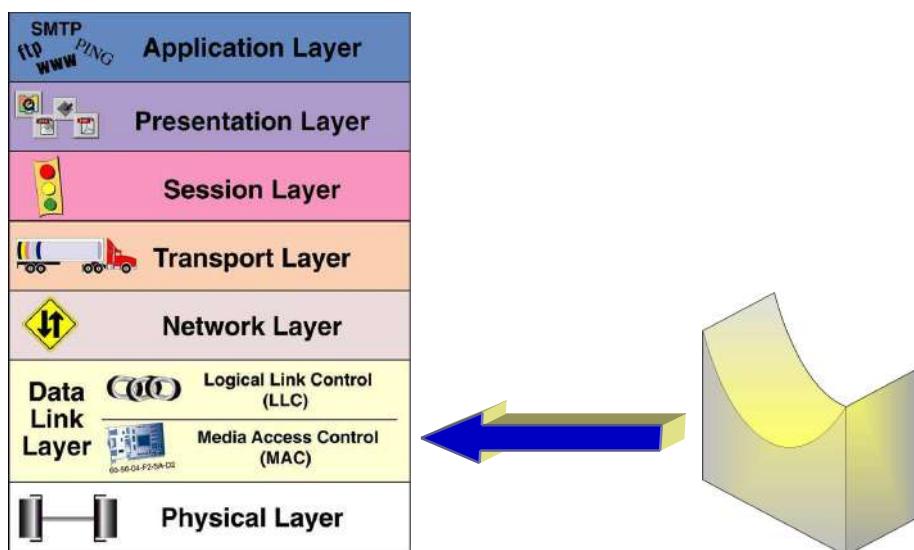
Các port của Hub nằm trong một miền đụng độ và một miền quảng bá (1 Collision Domain & 1 Broadcast Domain).

3.3.4. Bridge

Bridge là một thiết bị được dùng để nối hai mạng giống nhau hoặc khác nhau, nó có thể được dùng với các mạng có các giao thức khác nhau. Cầu nối hoạt động trên tầng liên kết dữ liệu (Layer 2) nên không như Repeater phải phát lại tất cả những gì nó nhận được thì cầu nối đọc được các frame của tầng liên kết dữ liệu trong mô hình OSI và xử lý chúng trước khi quyết định có chuyển đi hay không.

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

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



Hình 2.11. Hoạt động của Bridge trong mô hình OSI

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

Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch.

- Bridge vận chuyển dùng để nối hai mạng cục bộ cùng sử dụng một giao thức truyền thông của tầng liên kết dữ liệu, tuy nhiên mỗi mạng có thể sử dụng loại dây nối khác nhau. Bridge vận chuyển

không có khả năng thay đổi cấu trúc các frame mà nó nhận được mà chỉ quan tâm tới việc xem xét và chuyển vận frame đó đi.

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

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

Tuy nhiên chú ý ở đây cầu nối không thể chia một frame ra làm nhiều frame cho nên phải hạn chế kích thước tối đa các frame phù hợp với cả hai mạng. Ví dụ như kích thước tối đa của frame trên mạng Ethernet là 1500 byte và trên mạng Token ring là 6000 byte do vậy nếu một trạm trên mạng tokenring gửi một gói tin cho trạm trên mạng Ethernet với kích thước lớn hơn 1500 byte thì khi qua cầu nối số lượng byte dư sẽ bị chặt bỏ.



Hình 2.12. Bridge của NETGEAR

Người ta sử dụng Bridge trong các trường hợp sau:

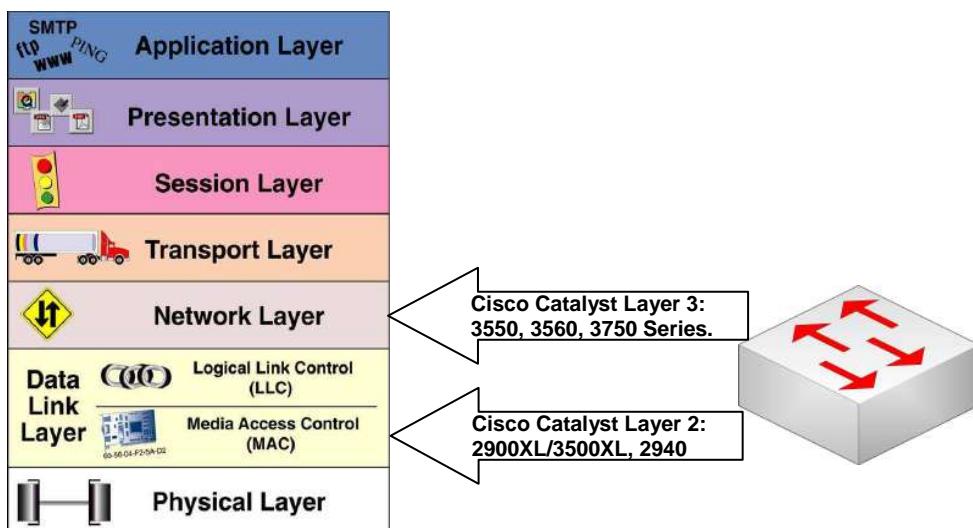
- Mở rộng mạng hiện tại khi đã đạt tới khoảng cách tối đa do Bridge sau khi xử lý frame đã phát lại frame trên phần mạng còn lại nên tín hiệu tốt hơn bội tiếp sức.
- Giảm bớt tắc nghẽn mạng khi có quá nhiều trạm bằng cách sử dụng Bridge, khi đó chúng ta chia mạng ra thành nhiều phần bằng các Bridge, các frame trong nội bộ từng phần mạng sẽ không được phép qua phần mạng khác.

- Để nối các mạng có giao thức khác nhau.
- Một vài Bridge còn có khả năng lựa chọn đối tượng vận chuyển. Nó có thể chỉ chuyển vận những frame của những địa chỉ xác định.

Một số Bridge được chế tạo thành một bộ riêng biệt, chỉ cần nối dây và bật. Các Bridge khác chế tạo như card chuyên dùng cắm vào máy tính, khi đó trên máy tính sẽ sử dụng phần mềm Bridge. Việc kết hợp phần mềm với phần cứng cho phép uyển chuyển hơn trong hoạt động của Bridge.

2.3.5. Switch

Switch hoạt động ở Layer 2&3 trong mô hình OSI.



Hình 2.13. Hoạt động của Switch trong mô hình OSI

Các port của Switch khác Collision Domain nhưng cùng Broadcast Domain.

Nhiệm vụ của Switch

- Quyết định khi nào chuyển tiếp một frame hay khi nào phải lọc (không chuyển tiếp) frame đó, dựa trên địa chỉ MAC.
- Học các địa chỉ MAC bằng cách kiểm tra địa chỉ MAC nguồn của mỗi frame nhận được.

- Tạo môi trường không có vòng lặp (lớp 2) sử dụng giải thuật Cây Bao trùm - Spanning Tree Protocol (STP).



Hình 2.14. Cisco Catalyst Switch 2950 series

2.3.5.1. Lọc hay chuyển tiếp frame

Để quyết định lọc hay chuyển tiếp một frame, switch sử dụng một bảng được xây dựng tự động có liệt kê các địa chỉ MAC và các giao tiếp đầu ra.

Switch so sánh địa chỉ MAC đích của một frame với bảng này để quyết định lọc hay chuyển tiếp nó.

Nếu địa chỉ MAC đích được tìm thấy trong bảng địa chỉ của switch, nó sẽ chuyển tiếp.

Nếu địa chỉ MAC không thấy hoặc chính là địa chỉ giao tiếp gửi, nó sẽ lọc gói tin.

2.3.5.2. Học các địa chỉ MAC và tìm giao tiếp ra phù hợp

Switches tạo bảng địa chỉ bằng cách lắng nghe trên các frame đến và kiểm tra địa chỉ MAC nguồn trong frame đó. Nếu frame vào switch và MAC nguồn không có trong bảng MAC. Switch tạo một giá trị cho bảng này. Địa chỉ MAC được đặt trong bảng này, cùng với giao tiếp mà từ đó frame đã đến.

Nếu switch không tìm thấy giao tiếp ra phù hợp với địa chỉ MAC đích, switch tiến hành đẩy các frame ra tất cả các giao tiếp (trừ giao tiếp

đến). Switch chuyển tiếp tất cả các frame unicast chưa biết này ra tất cả các giao tiếp, chờ phản hồi để xây dựng bảng địa chỉ đúng theo yêu cầu.

Bảng 2.1. Mac Address Table

Mac Address Table				
Vlan	Mac Address	Type	Ports	
1	0001.97d9.d701	DYNAMIC	Fa0/6	
1	0060.47a3.9eca	DYNAMIC	Fa0/5	
1	0090.0c89.e41a	DYNAMIC	Gig1/2	
1	00d0.ff7d.0904	DYNAMIC	Fa0/1	

2.3.6. Router

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



Hình 2.15. Cisco Router 2800 Series

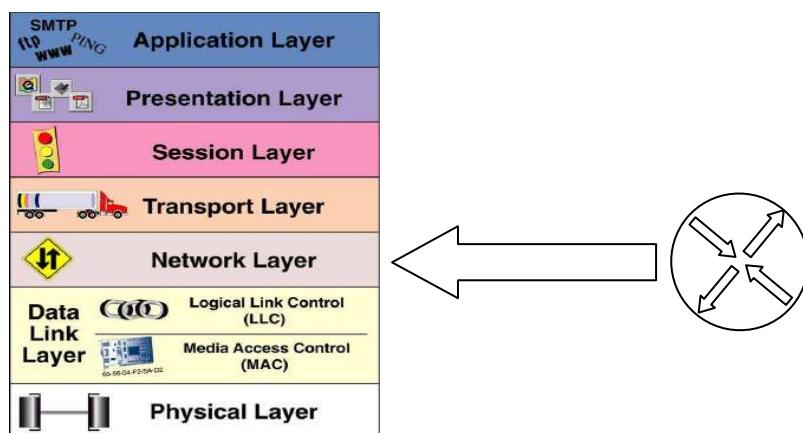
Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn

gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong gói tin đó phải chứa các thông tin khác về đích đến) và khi gói tin đến Router mới xử lý và gửi tiếp.

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

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

- Router có phụ thuộc giao thức: Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác chứ không chuyển đổi phương cách đóng gói của gói tin cho nên cả hai mạng phải dùng chung một giao thức truyền thông.
- Router không phụ thuộc vào giao thức: Có thể liên kết các mạng dùng giao thức truyền thông khác nhau và có thể chuyển đổi gói tin của giao thức này sang gói tin của giao thức kia, Router cũng chấp nhận kích thước các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước khi truyền trên mạng).



Hình 2.16. Hoạt động của Router trong mô hình OSI

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

Mục đích sử dụng Router:

- Router thường được sử dụng để nối các mạng thông qua các đường dây thuê bao đất liền.
- Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.
- Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.
- Trong một mạng phức hợp khi các gói tin luân chuyển giữa các đường và dễ xảy ra tình trạng tắc nghẽn của mạng thì các Router có thể được cài đặt các phương thức nhằm tránh được tắc nghẽn.

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

- Phương thức véc-tơ khoảng cách (Distance Vector): Mỗi Router luôn luôn truyền đi thông tin về bảng định tuyến của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng định tuyến của mình.
- Phương thức trạng thái đường liên kết (Link state): Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng và chỉ khi đó các Router khác mới cập nhật lại bảng định tuyến.

Một số giao thức hoạt động chính của Router: RIP, IGRP, EIGRP, OSPF ...

2.4. 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 - Hiệp hội Công nghiệp điện tử)
- Được thành lập năm 1924, EIA là một tổ chức của Mỹ sản xuất các thiết bị điện tử. EIA đã công bố một số tiêu chuẩn liên quan đến viễn thông và truyền thông điện toán và hoạt động kết hợp chặt chẽ với các hiệp hội khác như ANSI (American National Standards Institute: Học viện tiêu chuẩn quốc gia Hoa Kỳ) và ITU (International Telecommunication Union: Hiệp hội viễn thông quốc tế).
- Website của EIA: <http://www.eia.org>

TIA (Telecommunications Industry Association)

- TIA là Hiệp hội Công nghiệp viễn thông - một hiệp hội thương mại toàn cầu đặt trụ sở chính tại Hoa Kỳ và đại diện cho khoảng 600 công ty viễn thông.
- Với sự hỗ trợ từ 600 thành viên, TIA tăng cường môi trường kinh doanh cho các công ty tham gia vào viễn thông, điện thoại di động băng thông rộng không dây, công nghệ thông tin, mạng lưới, dây cáp, vệ tinh, truyền thông hợp nhất, liên lạc khẩn cấp và công nghệ xanh. TIA được công nhận bởi ANSI.
- Website của TIA: <http://www.tiaonline.org>

ISO (International Standard Organization)

- ISO là Tổ chức chuẩn hóa quốc tế, là một tổ chức quốc tế thực hiện việc thống nhất và đưa ra các chuẩn kết nối dùng chung cho các thiết bị viễn thông, máy tính,...
- Một trong những chuẩn nổi tiếng của ISO là mô hình kết nối OSI.

ANSI (American National Standard Institute)

- ANSI là Viện Tiêu chuẩn quốc gia Hoa Kỳ, là cơ quan đầu mối để điều phối việc xây dựng và sử dụng các tiêu chuẩn đồng

thuận tự nguyện và đồng thời là đại diện cho nhu cầu và quan điểm của các bên liên quan của Hoa Kỳ trên diễn đàn tiêu chuẩn hóa ở phạm vi toàn thế giới.

IEEE (Institute of Electrical and Electronics Engineers)

- IEEE là Viện các kỹ sư điện và điện tử, là một tổ chức khoa học nghề nghiệp được xây dựng nhằm mục đích hỗ trợ các hoạt động nghiên cứu khoa học, thúc đẩy sự phát triển khoa học công nghệ trong các lĩnh vực điện tử, viễn thông, công nghệ thông tin, khoa học máy tính,... IEEE hiện có trên 350.000 thành viên là các kỹ sư, các nhà khoa học gia và sinh viên.

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.

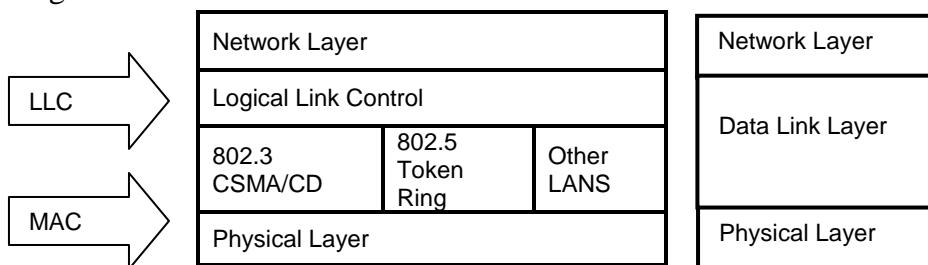
IEEE có nhiều tiêu ban (Committee). Trong đó Tiêu ban 802 phụ trách về các chuẩn cho mạng cục bộ. Một số chuẩn mạng cục bộ quan trọng do tiêu ban này đưa ra như:

- IEEE 802.1: Các giao thức LAN tầng cao
- IEEE 802.2: Điều khiển liên kết lôgic
- IEEE 802.3: Ethernet
- IEEE 802.4: Token bus (đã giải tán)
- IEEE 802.5: Token Ring
- IEEE 802.6: Metropolitan Area Network (đã giải tán)
- IEEE 802.7: Broadband LAN using Coaxial Cable (đã giải tán)
- IEEE 802.8: Fiber Optic TAG (đã giải tán)
- IEEE 802.9: Integrated Services LAN (đã giải tán)
- IEEE 802.10: Interoperable LAN Security (đã giải tán)
- IEEE 802.11: Wireless LAN (Wi-Fi certification)
- IEEE 802.12: Công nghệ 100 Mbit/s plus
- IEEE 802.13: (không sử dụng)
- IEEE 802.14: Modem cáp (đã giải tán)
- IEEE 802.15: Wireless PAN

- IEEE 802.15.1: Bluetooth certification
- IEEE 802.15.4: ZigBee certification
- IEEE 802.16: Broadband Wireless Access (WiMAX certification)
 - IEEE 802.16e: (Mobile) Broadband Wireless Access
- IEEE 802.17: Resilient packet ring
- IEEE 802.18: Radio Regulatory TAG
- IEEE 802.19: Coexistence TAG
- IEEE 802.20: Mobile Broadband Wireless Access
- IEEE 802.21: Media Independent Handoff
- IEEE 802.22: Wireless Regional Area Network
- IEEE 802.23: Broadband ISDN system (Đang thử nghiệm)

Các chuẩn do IEEE 802 định nghĩa thực hiện chức năng của tầng 2 trong mô hình tham chiếu OSI. Tuy nhiên, chúng chia tầng 2 thành hai tầng con (sublayer) là Tầng con điều khiển nối kết logic (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 logic cung cấp dịch vụ truyền tải thông tin theo kiểu định hướng nối kết.



Hình 2.17. Kiến trúc mạng cục bộ theo IEEE 802

2.5. MẠNG ETHERNET

2.5.1. Lịch sử hình thành

Ethernet là một giao thức mạng chuẩn hóa việc truyền thông tin trong mạng cục bộ. Giao thức Ethernet được xếp vào lớp thứ hai trong mô hình OSI tức là tầng Data Link.

Ngày nay, Ethernet đã trở thành công nghệ mạng cục bộ được sử dụng rộng rãi. Sau hơn 30 năm ra đời, công nghệ Ethernet vẫn đang được tiếp tục phát triển những khả năng mới đáp ứng những nhu cầu mới và trở thành công nghệ mạng phổ biến, tiện dụng.

Ngày 22 tháng 5 năm 1973, Robert Metcalfe thuộc Trung tâm Nghiên cứu Palo Alto của hãng Xerox – PARC, bang California, đã đưa ra ý tưởng hệ thống kết nối mạng máy tính cho phép các máy tính có thể truyền dữ liệu với nhau và với máy in laser. Lúc này, các hệ thống tính toán lớn đều được thiết kế dựa trên các máy tính trung tâm đắt tiền (mainframe). Điểm khác biệt lớn mà Ethernet mang lại là các máy tính có thể trao đổi thông tin trực tiếp với nhau mà không cần qua máy tính trung tâm. Mô hình mới này làm thay đổi thế giới công nghệ truyền thông.

Chuẩn Ethernet 10 Mbit/s đầu tiên được xuất bản năm 1980 bởi sự phối hợp phát triển của 3 hãng: DEC, Intel và Xerox. Chuẩn này có tên DIX Ethernet (lấy tên theo 3 chữ cái đầu của tên các hãng).

Ủy ban 802.3 của IEEE đã lấy DIX Ethernet làm nền tảng để phát triển. Năm 1985, chuẩn 802.3 đầu tiên đã ra đời với tên IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method versus Physical Layer Specification. Mặc dù không sử dụng tên Ethernet nhưng hầu hết mọi người đều hiểu đó là chuẩn của công nghệ Ethernet. Ngày nay chuẩn IEEE 802.3 là chuẩn chính thức của Ethernet.

IEEE đã phát triển chuẩn Ethernet trên nhiều công nghệ truyền dẫn khác nhau vì thế có nhiều loại mạng Ethernet.

Với sự phát triển mạnh mẽ của công nghệ, tốc độ kết nối trong Ethernet không ngừng được nâng lên. Vào năm 1995, Fast Ethernet ra

đời. IEEE dùng 802.3u để quy chuẩn cho các tiêu chí có liên quan đến Fast Ethernet. Tiếp đến là 802.3z, 802.3ab, 802.3ae ...

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 Mbit/s
- Hỗ trợ 4 chuẩn vật lý là 10Base-5 (cáp đồng trục dày), 10Base-2 (Cáp đồng trục mỏng), 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 Mbit/s
- 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 Gbit/s
- Hỗ trợ 3 chuẩn vật lý là 1000Base-LX (cáp quang), 1000Base-SX (cáp quang), 1000Base-CX (cáp đồng bọc kim)

Chuẩn mạng 802.3ab

- Có tên là mạng Giga Ethernet over UTP
- Tốc độ truyền tải dữ liệu là 1 Gbit/s
- Hỗ trợ chuẩn vật lý 1000Base-TX sử dụng dây cáp xoắn đôi không bọc kim.

Chuẩn mạng 802.3ae (10 Gigabit Ethernet)

2.5.2. Một số chuẩn mạng Ethernet phổ biến

2.5.2.1. 10- Mbit/s Ethernet

10BASE-2:

- Còn gọi là ThinNet hoặc Cheapernet.
- Sơ đồ mạng dạng Bus.
- Sử dụng dây cáp đồng trục mỏng (thin coaxial cable), chiều dài tối đa của mỗi đoạn mạng (network segment) là 185m.
- Tốc độ truyền dữ liệu là 10 Mbit/s.
- Tối đa cho phép 30 nút (máy tính) trên một đoạn mạng.
- Chiều dài tối thiểu giữa 2 node mạng 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.

10BASE-T:

- Sơ đồ mạng dạng Star.
- Sử dụng cáp xoắn đôi (STP- Shielded Twisted Pair hoặc UTP - Unshielded Twisted Pair), Cat3 trở lên. Chiều dài tối đa của một segment là 100 m.
- Có tốc độ truyền dữ liệu là 10 Mbit/s.
- Sử dụng Hub hoặc Switch làm thiết bị trung tâm để nối các máy tính lại với nhau.
- So với chuẩn 10 BASE-2 thì chuẩn 10 BASE-T đắt hơn, nhưng nó có tính ổn định cao hơn: Sự cố trên một node mạng không ảnh hưởng đến toàn mạng.

FOIRL (Fiber-optic inter-repeater link): Các tiêu chuẩn gốc cho Ethernet qua cáp quang.

10BASE-F: Thuật ngữ chung cho họ Ethernet 10 Mbit/s qua cáp quang: *10BASE-FL*, *10BASE-FB*, *10BASE-FP*. Trong số này thì 10BASE-FL được sử dụng rộng rãi.

2.5.2.2. Fast Ethernet

100BASE-T: Một thuật ngữ chung cho họ ba chuẩn Ethernet 100 Mbit/s qua cáp xoắn đôi. Bao gồm: 100BASE-TX, 100BASE-T4 và 100BASE-T2. Năm 2009, [\[cập nhật\]](#), 100BASE-TX đã hoàn toàn chi phối thị trường và thường được coi là đồng nghĩa với 100BASE-T.

- 100BASE-TX: Tốc độ 100Mbit/s qua cáp xoắn đôi Cat5 (Chỉ dùng 2 trong 4 cặp).
- 100BASE-T4: Tốc độ 100Mbit/s qua cáp xoắn đôi Cat3 (Dùng cả 4 cặp), hoạt động ở chế độ bán song công.
- 100BASE-T2: Tốc độ 100Mbit/s qua cáp xoắn đôi Cat3 (chỉ dùng 2 trong 4 cặp), có hỗ trợ chế độ song công.

100Base-FX: Tốc độ 100Mbit/s, sử dụng cáp sợi quang đa mode.

2.5.2.3. Gigabit Ethernet

1000BASE-T: Tốc độ truyền dữ liệu là 01 Gbps qua cáp UTP (Cat5 trở lên, nên dùng Cat5e).

1000BASE-SX: Tốc độ truyền dữ liệu là 01 Gbps qua cáp quang với sóng ngắn.

1000BASE-LX: Tốc độ truyền dữ liệu là 01 Gbps qua cáp quang với sóng dài. Tối ưu cho khoảng cách lớn hơn qua cáp quang đơn mode.

1000BASE-CX: 01 Gbps Ethernet qua cáp đồng đặc biệt. Ra đời trước 1000BASE-T, và bây giờ đã lỗi thời.

2.5.2.4. 10-Gigabit Ethernet

10 Gigabit Ethernet (hoặc 10GE, 10GbE hay tiêu chuẩn GigE 10) lần đầu tiên được công bố vào năm 2002 như IEEE 802.3ae-2002 và là chuẩn Ethernet nhanh nhất lúc bấy giờ. Tốc độ truyền dữ liệu lý thuyết là 10 Gbps, gấp mười lần so với Gigabit Ethernet.

2.5.2.5. 100-Gigabit Ethernet

100 Gigabit Ethernet, hoặc 100GbE hiện đang được phát triển bởi IEEE (tính đến 9/2009).

2.6. THIẾT KẾ HẠ TẦNG CÁP MẠNG

Các sự cố về mạng thường do nhiều nguyên nhân. Các nghiên cứu chỉ ra rằng trong nhiều trường hợp, mạng xảy ra sự cố chủ yếu do sự yếu kém của hệ thống cáp. Và những thiết lập tiêu chuẩn – khuyến cáo cấu trúc hệ thống cáp chuẩn có thể loại bỏ đáng kể thời gian chết này. Một yếu tố quan trọng là hệ thống cable có cấu trúc cần phải được đưa vào danh mục quan trọng, mặc dù nó tồn tại như các thành phần mạng khác và chỉ đại diện cho 5% tổng số vốn đầu tư mạng.

Cáp có cấu trúc là những chỉ dẫn cần phải thiết lập tiêu chuẩn để đáp ứng với nhu cầu thoại và truyền dữ liệu ngày nay và trong tương lai. Đây là một hệ thống cung cấp cách tiếp cận "có cấu trúc" toàn bộ hệ thống cáp - một hợp đồng hỗn các phương tiện truyền thông mạng mà trong đó nó xử lý tất cả lưu lượng truy cập thông tin như thoại, dữ liệu, video, và thậm chí xây dựng hệ thống quản lý phức tạp. Nói tóm lại, nó được mô tả như một hệ thống bao gồm bộ các sản phẩm truyền dẫn, áp dụng với quy tắc thiết kế kỹ thuật cho phép người dùng sử dụng các ứng dụng thoại, dữ liệu, và tín hiệu theo cách ước lượng tối đa hóa dữ liệu.

Cáp có cấu trúc chia cơ sở hạ tầng toàn bộ thành các khối quản lý và sau đó tích hợp các khối để cấu thành mạng có hiệu năng cao. Cấu trúc cáp cũng cung cấp khả năng quản trị và quản lý. Tất cả các loại cáp đảm đương các công việc nội bộ khác nhau, chấm dứt sự tập trung thụ động- kết nối trong phòng mạng. Tập hợp nhãn đơn giản và cơ cấu màu nhằm xác định dễ dàng và nhanh chóng trạng thái của công việc. Do đó, nó cung cấp một điểm duy nhất cho tất cả các yêu cầu về quản trị và quản lý. Một yếu tố khác là quản lý thay đổi, kiến trúc hệ thống liên tục thay đổi khi hệ thống tăng trưởng. Và kiến trúc cáp phải đáp ứng yêu cầu này với mức phức tạp tối thiểu. Việc cung cấp một bảng điều khiển trung tâm, cung cấp tính linh hoạt để bổ sung, di chuyển, và thay đổi. Những

thay đổi có thể tạo điều kiện cho sự đơn giản hóa chuyển đổi trên cáp nối. Ngoài ra, cấu trúc cáp cũng là công nghệ độc lập.

Những lợi thế của cáp cấu trúc là:

- Tính thống nhất : Một hệ thống cáp có cấu trúc phải giống nhau cho hệ thống cáp dữ liệu, thoại và video.
- Hỗ trợ cho nhiều nhà cung cấp thiết bị - Một tiêu chuẩn dựa trên hệ thống cáp sẽ hỗ trợ ứng dụng và phần cứng, ngay cả với nhiều nhà cung cấp.
- Đơn giản hóa di chuyển / bổ sung / thay đổi - hệ thống cáp cấu trúc có thể hỗ trợ bất kỳ thay đổi trong hệ thống.
- Đơn giản hóa xử lý sự cố - Với hệ thống cáp cấu trúc, các vấn đề khiến mạng gặp sự cố ít khả năng xảy ra, dễ dàng hơn để cô lập và sửa chữa.
- Hỗ trợ cho các ứng dụng tương lai - hệ thống cáp cấu trúc hỗ trợ các ứng dụng trong tương lai như đa phương tiện, hội nghị truyền hình, v..v với chi phí nâng cấp ít hoặc không có.

Một ưu điểm chính của hệ thống cáp có cấu trúc là cô lập lỗi. Bằng cách chia toàn bộ cơ sở hạ tầng thành những khối quản lý đơn giản, rất dễ dàng để kiểm tra và cô lập những vị trí lỗi cụ thể và sửa chữa chúng với ảnh hưởng tối thiểu đến hệ thống mạng, điều này làm giảm chi phí bảo trì.

Cấu trúc hệ thống cáp đang nhanh chóng trở thành chuẩn cho các mạng nhỏ, vừa và lớn.

2.6.1. Các tiêu chuẩn về cáp mạng

2.6.1.1. Các tiêu chuẩn quốc tế

TIA không phải là cơ quan tiêu chuẩn duy nhất xem xét hiệu suất cáp mở rộng. Tổ chức tiêu chuẩn quốc tế (ISO) đã tiến hành định nghĩa tiêu chuẩn của CAT 6 và CAT 7. Thể loại CAT 6 chỉ định các thông số truyền dẫn tối đa 200 MHz trong khi đó cáp CAT 7 mở rộng đến 600 MHz. Những chỉ dẫn của CAT 6 và 7 về thông số kỹ thuật sẽ được bao gồm trong án bản thứ hai của tiêu chuẩn ISO/IEC 11801 . Tuy nhiên, định nghĩa của CAT 6 và 7 đang ở giai đoạn đầu, chưa được xét duyệt ở

Hoa Kỳ vào lúc này. Sự phê duyệt cuối cùng dự kiến đến năm 2000. Tham khảo tài liệu hướng dẫn tiêu chuẩn EIA /TIA trong Phụ lục I.

2.6.1.2. Tiêu chuẩn công nghiệp

Lợi thế của tiêu chuẩn công nghiệp là những hiểu biết làm cho cáp tương thích được với các ứng dụng tiêu chuẩn. Điểm bất lợi chính nằm ở thời gian phê duyệt các tiêu chuẩn. Tiêu chuẩn cuối cùng cũng có thể khác với đề nghị ban đầu, nhưng thường thì sự khác biệt này ở mức tối thiểu. Ví dụ, tiêu chuẩn đề xuất cho CAT 6 là 250 MHz, và tiêu chuẩn đề nghị cho CAT 7 là 600 MHz.

Điều quan trọng cần nhớ là: tiêu chuẩn đề xuất được cải tiến hơn cáp CAT 5 và CAT 5e, phục vụ tốc độ tốt hơn cho các ứng dụng trong tương lai.

2.6.1.3. Các tiêu chuẩn cho cấu trúc cáp

Các nhà quản lý mạng đôi mặt với một thử thách khó khăn khi lắp đặt một cơ sở mới của công ty. Họ phải đảm bảo rằng tất cả các vị trí nhân viên có thể truy cập vào mạng LAN doanh nghiệp, và chắc chắn các vị trí này có thể tương tác thành công với tiềm năng phạm vi rộng lớn của công nghệ mạng LAN tốc độ cao mới, từ đó những công nghệ này nhanh chóng đạt được tầm quan trọng với chi phí hiệu quả.

Giải pháp cho những thách thức này nằm trong việc thực hiện một hệ thống cáp cấu trúc tại một cơ sở mới. Một hệ thống như phải mở rộng đến tất cả các khu vực làm việc của nhân viên và có khả năng hỗ trợ tất cả các công nghệ mạng LAN hiện có và tất cả các công nghệ mới, công nghệ mạng LAN tốc độ cao đang phát triển, vì chúng ta không thể dự đoán năng lực cao nhất sẽ đạt được tại bất cứ lúc nào trong tương lai.

Một nhóm, trong đó tập hợp tiêu chuẩn đối với dây dữ liệu có cấu trúc ở Hoa Kỳ, là Hiệp hội Công nghiệp viễn thông, hay TIA. Tiêu chuẩn TIA 568A định nghĩa nhiều loại CAT hoặc đánh giá về hiệu suất của cấu trúc hệ thống dây, với CAT 5 là cao nhất hiện đang được chuẩn hóa. Chuẩn TIA 568A CAT 5 là cơ sở cho nhiều công nghệ LAN mới tốc độ cao.

2.6.1.4. Điểm nổi bật của các tiêu chuẩn EIA/TIA-568A

Mục đích:

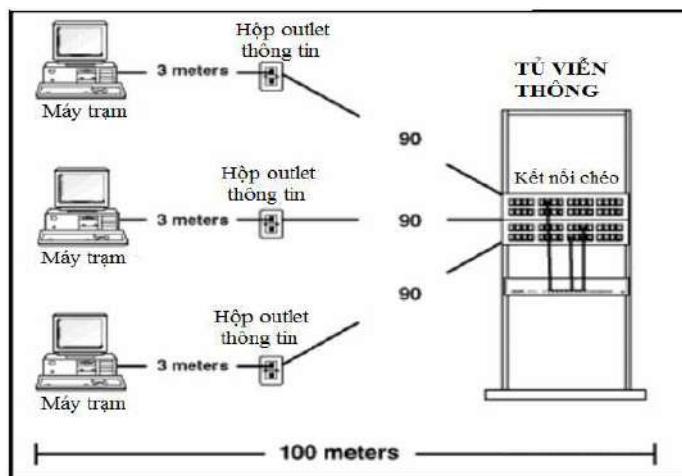
- Để xác định một nguyên tắc chung về hệ thống cáp viễn thông dành cho thoại và dữ liệu nhằm hỗ trợ môi trường đa sản phẩm, đa nhà cung cấp.
- Để định hướng cho việc thiết kế các thiết bị viễn thông và sản xuất cáp nhằm phục vụ cho các doanh nghiệp thương mại
- Để cho phép lập kế hoạch, lắp đặt một hệ thống cấu trúc cáp cho tòa nhà thương mại có khả năng hỗ trợ đa dạng các nhà mạng.
- Để thiết lập hiệu suất và tiêu chuẩn kỹ thuật cho các loại hình kết nối cáp và phần cứng, cho việc thiết kế và lắp đặt hệ thống cáp

Phạm vi:

- Các yêu cầu cho một hệ thống cáp có cấu trúc có thể sử dụng hơn 10 năm
- Đặc điểm địa chỉ:
 - (a) Phương tiện công nhận - cáp và phần cứng kết nối
 - (b) Hiệu suất
 - (c) Hình trạng
 - (d) Khoảng cách cable
 - (e) Thực hành cài đặt
 - (f) Giao diện người dùng
 - (g) Hiệu suất kênh

Các yếu tố của cable :

- Cáp ngang:
 - a) Đầu kết nối ngang (HC)
 - b) Cable ngang
 - c) Điểm chuyển tiếp (tùy chọn)
 - d) Điểm cung cấp (tùy chọn)
 - e) Viễn thông-Outlet (Đầu kết nối (TO))
- Khoảng cách tối đa cho cáp ngang



Hình 2.17. Cáp ngang

90m là khoảng cách từ trạm viễn thông tới hộp Outlet, 10m từ hộp outlet tới máy trạm.

- Cable đường xương sống:
 - a) Cổng kết nối chính (MC)
 - b) Đường trực cáp nội vi
 - c) Đầu kết nối trung gian (IC)
 - d) Đường trực cáp ngoại vi

Vùng làm việc (WA)

Hộp viễn thông (TS)

Thiết bị trong phòng (ER)

Điều kiện đi vào (EF)

Quản trị **

** Mặc dù quản trị chỉ ở mức độ hạn chế, đặc trị trên quản trị viễn thông là ANSI/EIA/TIA-606.

2.6.2. Cấu trúc cáp

Thiết kế đánh giá hệ thống cáp: Sáu hệ thống con của một hệ thống cáp có cấu trúc như sau:

2.6.2.1. Điều kiện xây dựng

Điều kiện xây dựng cung cấp các cơ sở cho lối vào mà tại đó cable bên ngoài giao diện với cable xương sống nội vi. Những yêu cầu vật lý của giao tiếp mạng được định nghĩa trong tiêu chuẩn EIA/TIA-569.

2.6.2.2. Trang thiết bị phòng

Các khía cạnh thiết kế của phòng thiết bị được quy định trong tiêu chuẩn EIA/TIA-569. Thiết bị phòng thường là thiết bị nhà phức tạp cao hơn hộp viễn thông. Một thiết bị phòng có thể cung cấp bất kỳ hoặc tất cả các chức năng của hộp viễn thông.

2.6.2.3. Cable đường trực

Cáp xương sống cung cấp kết nối giữa các hộp viễn thông với thiết bị phòng và các lối vào cơ sở. Nó bao gồm các loại cáp đường trực, trung gian và đầu kết nối chính, thiết bị đầu cuối và dây nối hoặc jumpe, được sử dụng cho kết nối đường tới đường trực. Điều này bao gồm:

- Kết nối dọc giữa các tầng (risers)
- Cáp giữa một phòng thiết bị và cổng vào cơ sở cáp tòa nhà
- Cáp giữa các tòa nhà

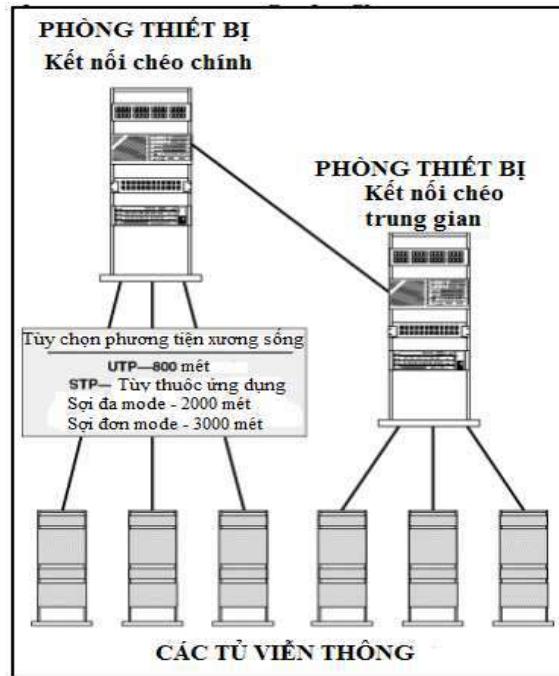
Các loại cáp Được công nhận	Khoảng cách đường trực tối đa
100 ohm UTP (24 hoặc 22 AWG)	800 m (2625 ft) Voice *
150 ohm STP	90 mét (295 ft) liệu *
Cáp quan đa ché độ 62.5/125 µm	2.000 m (6560 ft)
Cáp quan đơn ché độ 8.3/125 µm	3.000 m (9840 ft)

Lưu ý: khoảng cách đường trực phụ thuộc ứng dụng. Khoảng cách tối đa nêu trên dựa trên truyền dẫn bằng giọng nói cho UTP và truyền dữ liệu cho STP và quang. Khoảng cách 90m STP áp dụng cho các ứng dụng băng thông với quang phổ từ 20 MHz đến 300 MHz. Khoảng cách 90m cũng áp dụng cho UTP ở băng thông quang phổ như 5 MHz - 16 MHz cho 3 CAT, 10 MHz 20 MHz cho Cat 4 và 20 MHz 100 MHz cho CAT 5.

Yêu cầu thiết kế khác:

- Mô hình Star
- Bridge và tap không được cho phép

- Kết nối jumper chính và qua trung gian hoặc chiều dài dây nối không được vượt quá 20 mét (66 feet)
- Mặt đất phải đáp ứng các yêu cầu quy định tại EIA/TIA 607
- Thiết bị kết nối vào mạng trực cáp dài 30m (98ft) hoặc ít hơn
- Cáp xương sống phải được cấu hình trong mô hình Star. Mỗi kết nối chéo ngang- được kết nối trực tiếp đến một chéo chính hoặc kết nối vào một kết nối qua trung gian, sau đó tới kết nối chính.
- Các xương sống được giới hạn không quá hai bậc cấp độ của kết nối chéo (chính và trung gian). Không có nhiều hơn một kết nối chéo có thể tồn tại giữa kết nối chính và kết nối ngang, không quá ba kết nối có thể tồn tại giữa hai kết nối chéo ngang.
- Tổng số khoảng cách đường trực tối đa là 90m (295ft) được chỉ định cho băng thông cao trên trực đồng. Khoảng cách này là dành cho xương sống chạy không gián đoạn. (Kết nối không qua trung gian).
- Khoảng cách giữa các đầu cuối vào phòng chính và qua kết nối cần được được tiêu chuẩn hóa và tạo sẵn cho các nhà cung cấp dịch vụ.
- Phương tiện truyền thông được công nhận có thể được sử dụng riêng lẻ hoặc kết hợp, do yêu cầu của tiến trình cài đặt. Số lượng sửa chữa và vật liệu cần thiết trong xương sống phụ thuộc vào khu vực phục vụ.
- Tránh cài đặt nơi có nguồn cao có thể khi tồn tại EMI /RFI



Hình 2.18. Kết nối chéo chính

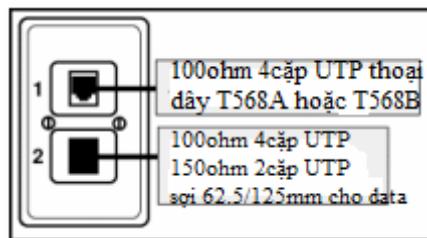
Xác định cable đường trực theo mạng hình sao

Khoảng cách cáp đường trực TIA (MC tới HC)

- Singlemode Fiber 3000m (9840ft)
- 62,5/125um Multimode Fiber 2000m (6560ft)
- Cable đồng UTP ứng dụng <5MHz 800m (2625ft)

2.6.2.4. Hộp viễn thông

Một hộp viễn thông là khu vực chứa trong một ngôi nhà mà tại đó tập hợp hệ thống thiết bị cáp viễn thông. Điều này bao gồm cấu trúc đầu cuối và / hoặc kết nối chéo cho hệ thống cáp ngang và đường trực.



Hình 2.19. Hộp viên thông

2.6.2.5. Cable ngang

Hệ thống cáp ngang kéo dài từ hộp outlet viễn thông trong khu vực làm việc kết nối ngang qua hộp viễn thông. Nó bao gồm các hộp outlet viễn thông, một điểm hợp nhất hoặc tùy chọn kết nối điểm chuyển tiếp, cáp ngang, thiết bị đầu cuối, dây nối (hoặc jumper) bao gồm các kết nối chéo ngang.

- Bao gồm thiết bị khách hàng
- Dây thiết bị HC
- Dây nối / jumper kết nối chéo sử dụng trong HC, bao gồm thiết bị cáp / dây, không nên vượt quá 6m (20ft)
- Cáp ngang tối đa 90m (295ft)
- TP hoặc CP (tùy chọn)
- Outlet viễn thông / đầu nối (TO)
- Thiết bị dây WA

Lưu ý: Thực hiện phụ cấp cho các thiết bị dây WA là 3m (9.8ft). Phụ cấp 10m (33ft) đã được cung cấp cho chiều dài kết hợp của các dây nối/jumper kết nối chéo và thiết bị cáp/dây trong HC, bao gồm trang thiết bị dây WA.

Một số đặc điểm cụ thể cho hệ thống cáp ngang phụ bao gồm:

- Chỉ rõ các thành phần ứng dụng không được cài đặt như một phần của hệ thống cáp ngang. Khi cần thiết, chúng được đặt bên ngoài các outlet viễn thông hoặc kết nối ngang - (ví dụ splitters, baluns)

- Những nơi gần nhau của cáp ngang tới nguồn EMI sẽ được đưa vào danh mục
- Điều kiện công nhận là Cables ngang:
 - a) Một điểm chuyển đổi (TP) được cho phép giữa các hình thức khác nhau của cùng một loại cáp (tức là nơi cáp kết nối vào vòng dây cáp)
 - b) Cáp đồng trục 50Ω được công nhận bởi 568-A nhưng không nên dùng cho cáp mới cài đặt.
 - c) Các outlet có thể cung cấp. Những outlet này được bổ sung vào mà không thể thay thế các yêu cầu tối thiểu của tiêu chuẩn.
 - d) Bridge và Splices không được phép sử dụng trên cáp ngang đồng trục

2.6.2.6. Vùng làm việc

Các outlet viễn thông phục vụ như giao tiếp khu vực làm việc tới hệ thống cáp. Một vài chi tiết kỹ thuật liên quan đến khu vực cáp bao gồm:

- Thiết bị dây được giả định có hiệu năng giống dây nối cùng loại và category
- Khi sử dụng, các adapter được coi là tương thích với khả năng truyền dẫn của thiết bị mà nó kết nối.
- Độ dài cáp ngang được quy định với giả định rằng chiều dài cáp tối đa là 3m (10ft)

Những thành phần vùng làm việc:

- Trạm thiết bị máy vi tính, dữ liệu đầu cuối, điện thoại,...
- Môđun lõi cáp nối, bộ tương thích cáp PC, jumper,...
- Bộ điều chế, phải được mở rộng tới Outlet viễn thông,..

Ghi chú: Cho việc thiết lập khoảng cách liên kết ngang cực đại, chiều dài tối đa kết hợp 10m (33ft) kết hợp với cáp nối (hoặc jumper) và (hoặc cáp thiết bị trong vùng làm việc và trạm viễn thông).

2.6.3. Cáp mạng

Cáp là phương tiện qua đó thông tin được di chuyển từ một thiết bị mạng này tới mạng khác. Một số loại cáp, thường được dùng với mạng LAN. Trong một số trường hợp, một mạng sẽ sử dụng chỉ một loại cáp; các mạng khác sẽ sử dụng nhiều loại cáp khác nhau. Các loại cáp chọn cho một mạng lõi liên quan đến topology của mạng, giao thức, và kích cỡ. Sự hiểu biết đặc điểm của loại cáp và làm thế nào liên kết đến các vùng khác của một mạng là cần thiết cho sự phát triển thành công của một mạng.

2.6.3.1. Cable xoắn đôi không vỏ bọc

Cable UTP có thể khác nhau từ điện thoại, lớp dây để đạt tới tốc độ cao. Loại cable này có 4 cặp bên trong vỏ bọc. Mỗi cặp xoắn được đánh số khác nhau/inch để giúp loại bỏ sự nhiễu từ cặp bên cạnh và các thiết bị điện khác.

UTP có thể hỗ trợ điện thoại, 4 & 16 Mbit/s Token Ring, Ethernet, 100 Mbit/s Ethernet, FDDI lõi đồng (CDDI), 155 Mbit/s ATM. Cáp UTP được EIA/TIA chuẩn hóa. Trong số những giá trị tốt nhất về giá cả là CAT 3 và CAT 5. Tuy nhiên, CAT 3 được xếp vào loại 10 MHz, phù hợp với Ethernet (10 Mbit/s), và CAT 5 100 MHz, thích hợp cho Fast Ethernet (100 Mbit/s) và ATM (155 Mbit/s).

Ngoài ra còn có CAT5e (Enhanced Category 5). Đây là tiêu chuẩn được phê duyệt gần đây, thiết kế cho việc trao đổi an toàn hơn khi truyền Fast Ethernet song công. Sự khác biệt chính giữa CAT 5 và CAT 5e có thể thấy trên các thông số kỹ thuật và hiệu suất được nâng lên một chút. Cáp UTP nói chung là có dây trong topology star vì những lợi thế xử lý sự cố liên kết trong topology star.

2.6.3.2. Cáp xoắn đôi bọc lõi

Một bất lợi của UTP là nó dễ bị nhiễu sóng tần số vô tuyến điện. Cáp xoắn đôi bọc lõi phù hợp cho các môi trường có sự ảnh hưởng của điện. Nó có một màng che chắn có thể chặn các nhiễu điện, nhưng điều này khiến cho cáp cồng kềnh và thường rất khó để giao tiếp với một kết nối dữ liệu. Tuy nhiên, một phiên bản mới của STP cáp được giới thiệu

của công ty như ITT Datacomm sử dụng RJ-45 connector. Không nhưng không phức tạp mà còn rất dễ dàng để làm việc và mang lại khả năng truyền tải nhiều dữ liệu hơn UTP.

2.6.3.3. *Cable quang*

Cáp sợi quang bao gồm một lõi thủy tinh bao quanh bởi nhiều lớp vật liệu bảo vệ. Cáp quang có khả năng cung cấp băng thông rất cao và không phụ thuộc vào tiếng ồn. Nó sử dụng ánh sáng để truyền tín hiệu thay thế cho tín hiệu điện tử, loại bỏ các vấn đề của nhiễu điện. Điều này làm cho nó lý tưởng cho các môi trường với sự ảnh hưởng của điện từ lớn và đây cũng là một tiêu chuẩn cho mạng kết nối giữa các tòa nhà, do nó không bị ảnh hưởng bởi những tác động của độ ẩm và sét.

Cáp quang có khả năng truyền tín hiệu với một khoảng cách xa hơn so với cáp đồng trực hoặc cable xoắn, đồng thời có khả năng mang theo thông tin ở tốc độ lớn. Năng lực này phù hợp với khả năng giao tiếp cho các dịch vụ như hội nghị video và các dịch vụ tương tác. Tuy nhiên, việc sử dụng cáp sợi quang đòi hỏi chi phí đáng kể về đầu tư ban đầu, kết nối, đầu nối, jumper cáp, các công cụ và card giao diện mạng. Đây là vấn đề chính để cài đặt và thay thế.

Có hai loại sợi cáp quang-đa chế độ (MMF) và đơn chế độ (SMF). Ánh sáng được truyền thông qua các lõi của sợi quang. Đa sợi, với đường kính lõi phổ biến là 62,5 micron hoặc 50 micron, được thiết kế cho khớp nối ánh sáng từ đèn LED có chi phí thấp dựa trên liên kết. Sợi đơn mode có đường kính lõi là 10 micron, chỉ thích hợp cho laser truyền dẫn. Nhiều cơ sở cài đặt sợi quang hỗ trợ mạng LAN như là phần xương sống đa phương thức, vì hầu hết các tốc độ hiện tại là thiết bị LAN -10 hoặc 100 Mb/s dựa trên đèn LED.

Gigabit Ethernet hoạt động ở mức 1,25 Gbps là quá nhanh cho LED và yêu cầu sử dụng tia laser. Theo truyền thống, laser dựa trên truyền dữ liệu được sử dụng với chất sợi đơn Mode. Các tiêu chuẩn 1000Base-X đã giới thiệu laser dựa trên truyền dẫn quang trên sợi đa mode và với lớp vật lý khác biệt so với trước.

2.6.3.4. Sự phát triển của các loại cable UTP

Năm 1991 với việc công bố tiêu chuẩn TIA/EIA-568, thuật ngữ "CAT" được sử dụng như biệt ngữ chỉ việc cài đặt cáp và quản lý mạng LAN để mô tả các đặc tính hiệu suất của hệ thống cáp UTP. Ban đầu, cáp CAT 3 sử dụng rộng rãi nhất trong các hệ thống cáp có cấu trúc có khả năng mang lưu lượng thoại và truyền dẫn 10Base-T LAN. CAT 4 được giới thiệu ngay sau đó khi nó cung cấp khả năng cao hơn ở tốc độ 16 Mb/s mạng Token Ring. Với dòng Base-TX, CAT 4 nhanh chóng được thay thế bởi CAT 5, được sử dụng rộng rãi cho tới ngày nay. Gần đây, nó dần được thay thế bởi Gigabit Ethernet (1000Base-T). Cụ thể, 1000Base-T sẽ yêu cầu đặc tả kỹ hơn về hiệu suất so với cáp Cat 5 UTP trong quá khứ. Ngoài ra, do sự ảnh hưởng bởi tiếng ồn, một loại cáp mới (5E) đã được xác định để hỗ trợ tốt hơn 1000Base T mới.

Danh mục Cable	Thiết kế hỗ trợ cho ứng dụng mạng cụ thể	Năm ban hành chuẩn cable
CAT 3	Thoại, 10Base-T	1991
CAT 4	Token Ring 16Mb/s	1993
CAT 5	100 Base-TX (Fast Ethernet)	1994
CAT 5E	1000 Base-T (Giga Ethernet)	1998
CAT 6,7	Chưa đề xuất	Chưa xác định

Gigabit Ethernet: tác nhân cho những đột xuất yêu cầu chuẩn cable mới.

Các khách hàng tiềm năng của Gigabit Ethernet đã có những ý tưởng và thảo luận trong ngành công nghiệp mạng. Dự thảo IEEE 802.3 xác định tiêu chuẩn Gigabit Ethernet được phát triển trong hai năm. Các đặc điểm kỹ thuật cho 802.3z Gigabit Ethernet qua cáp quang và cáp Twinax (1000Base-SX, LX và CX) đã được phê chuẩn vào tháng 6 năm 1998.

Hệ tiêu chuẩn IEEE 802.3z (1000Base-SX & 1000Base-LX) xác định các yêu cầu cho hoạt động Gigabit Ethernet qua sợi cáp quang đa và đơn mode. Tiêu chuẩn này được phê chuẩn vào tháng 6 năm 1998. Ban đầu, người dùng cuối sẽ triển khai Gigabit Ethernet trong mạng xương sống của họ, nơi phương tiện được lựa chọn. Tiêu chuẩn IEEE 802.3ab

(1000Base-T) sẽ được phê chuẩn vào năm 1999, mở đường cho việc triển khai Gigabit Ethernet cho máy tính để bàn trong quá trình cài đặt CAT 5 hoặc cáp Cat 5E xoắn đôi.

Đối với truyền hình hội nghị và Tele-medicine, Gigabit Ethernet là công nghệ thích hợp cho các ứng dụng ưu tiên và quan trọng. Các phần cứng cần thiết để được cài đặt cho Gigabit Ethernet là Gigabit hub/switch, UTP Cat E5 trở lên. Workgroup IEEE 802.3 hình thành trong tháng 7 năm 1996, mục tiêu ban đầu là phê duyệt và công bố tiêu chuẩn IEEE 802.3z tới tháng 01 năm 1998. Trên thực tế là tháng 6 năm 1998. Lý do cho sự chậm trễ nằm ở sự phức tạp của dữ liệu khi chạy tốc độ Gigabit trên sợi đa mode. Mục tiêu ban đầu là hỗ trợ ổ quang đa mode với khoảng cách tối đa là 500 mét, nhằm hỗ trợ xương sống kiến trúc trong một khuôn viên trường. Mặc dù khoảng cách đạt được cho một số loại sợi đa mode, nhưng trên thực tế khoảng cách tối đa được giới hạn xuống.

Chuẩn Gigabit Ethernet	Loại phương tiện hỗ trợ	Thời gian công bố
1000Base-SX (802.3z)	Sợi đa mode	Tháng 6 - 1998
1000Base-LX (802.3z)	Sợi đơn và đa mode	Tháng 6 - 1998
1000Base-CX (802.3z)	Thiết bị nội vi	Tháng 6 - 1998
1000Base-T (802.3ab)	CAT 5,5E UTP	Năm 1999

2.6.3.5. Cable CAT5E

Một loại cáp mới 5E (Nâng cao) đang được quy định rõ ràng để xử lý các thách thức về lưu lượng truy cập gigabit. Các chi tiết kỹ thuật cho loại cáp 5E và thủ tục kiểm nghiệm đề xuất theo tài liệu SP4194 TIA và SP4195. Yêu cầu cho việc trả về Return Loss và ELFEXT sẽ được thêm vào SP4195 dự kiến sẽ được công bố như phụ lục 4 cho TIA/EIA-568-A. SP4194 dự kiến sẽ được công bố như là một hệ thống kỹ thuật (TSB-95) được gắn chặt giới hạn cho cài đặt cáp CAT 5 với các tham số như NEXT, FEXT, và Return Loss để cung cấp cho cải thiện tiếng ồn trong thiết bị 1000Base-T. Hiện nay TIA hoàn thành SP4194 và SP4195, trong một nỗ lực để xác định các thông số cáp mới (ELFEXT, Return Loss, và skew) trước khi chuẩn 1000Base-T được công bố.

2.6.3.6. Cable CAT 6 & 7

Gần đây, đã từng có nhiều suy đoán về tương lai có thể có tiêu chuẩn cáp CAT 6 & 7. Vậy thực sự là cần tiêu chuẩn CAT 6 & 7 vào thời điểm này? Không có ứng dụng mạng LAN có hiệu suất cáp vượt CAT 5E. Thảo luận ban đầu về khái niệm của CAT 6 & 7 được đề ra tại TIA, nhưng chưa xác định được một đặc tả cụ thể nào. Vào thời gian này, mức giới hạn tần số và các thông số kỹ thuật cáp vẫn còn đang được thảo luận. Phê duyệt cuối cùng của bất cứ tiêu chuẩn tiềm năng CAT 6 & 7 có lẽ là ít nhất 1-2 năm tới. Vì không có định nghĩa cho CAT 6 & 7 được xuất bản, chưa thể kiểm tra cho hệ thống cáp “CAT 6 & 7”.

2.6.3.7. So sánh các loại cáp

Loại Cable	Chi phí	Cài đặt	Công suất	Độ dài	EMI
Thinnet Đồng	Ít hơn STP	Rẻ, dễ dàng	10Mbit/s	185m	Dễ hỏng hóc hơn UTP
Thicknet Đồng	Cao hơn STP, ít hơn cable sợi	Dễ dàng	10Mbit/s	500m	Dễ hỏng hóc hơn UTP
Xoắn đôi bọc vỏ (STP)	Cao hơn UTP, ít hơn thicknet	Dễ dàng	16-500Mbit/s	100m	Dễ hỏng hóc hơn UTP
Xoắn đôi không bọc vỏ (UTP)	Thấp nhất	Rẻ/dễ dàng	10-100Mbit/s	100m	Khó hư hỏng
Sợi quang	Tốn kém nhất	Đắt/Khó khăn	100-200.000 Mbit/s	10s/km	Không hởng hóc

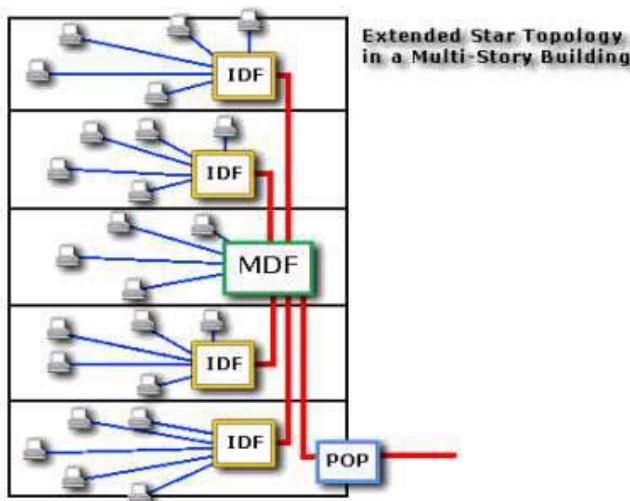
Khi so sánh các loại cáp, nhớ rằng các đặc tính mà ta quan sát phụ thuộc nhiều vào việc triển khai, chẳng hạn như card mạng, hub, và các thiết bị sử dụng. Có thể chúng ta đã từng nghĩ rằng cáp UTP sẽ không bao giờ hỗ trợ tốc độ dữ liệu trên 4Mbit/s đáng tin cậy, nhưng tốc độ dữ liệu 100Mbit/s đang phổ biến. Một số so sánh giữa các loại cáp là đáng tham khảo. Ví dụ, mặc dù sợi cáp quang tốn kém về cơ sở cho một lần triển khai, nhưng ta có được chi phí hiệu quả nhất khi bạn cần thay thế cáp cho nhiều km. Để xây dựng một dây cáp đồng chiều dài nhiều km,

bạn cần phải cài đặt lặp tại một số điểm dọc theo dây cáp để khuếch đại tín hiệu. Điều này có thể vượt qua chi phí ban đầu cho việc chạy một sợi cáp quang.

2.6.3.8. Chi tiết danh mục các loại CAT

Chỉ dẫn danh mục EIA/TIA cung cấp tốc độ truyền dẫn cho các loại CAT sau đây:

- CAT 1 : Không có tiêu chí hiệu suất
- CAT 2 : đạt tới 1MHz (sử dụng cho dây thoại)
- CAT 3 : đạt tới 16MHz (sử dụng cho Ethernet 10Base-T)
- CAT 4 : đạt tới 20MHz (sử dụng cho Token Ring, 10Base-T)
- CAT 5 : đạt tới 100MHz (sử dụng cho 100Base-T, 10Base-T)



Hình 2.20. Mở rộng mạng Star trong đa cơ sở

2.7. KẾT NỐI LAN

2.7.1 Vị trí nút mạng

Có nhiều lựa chọn cho việc kết nối máy tính, máy in và thiết bị đầu cuối ban đầu hoặc trong tương lai, tất cả các mạng như vậy thì vị trí "nút" phải được xác định như một phần quan trọng trong kế hoạch của việc xây dựng mạng, tùy thuộc vào quy mô.

2.7.2 Vị trí đặt Hub

Việc đặt hub/switch trong phòng hoặc closets nhằm bảo đảm an toàn từ truy cập trái phép. Đó cũng là mong muốn có switch/hub ít nhất là 1 m đi từ bất kỳ bảng chuyển mạch trung tâm. Nhìn vào bản đồ nút miền, lựa chọn vị trí tiềm năng ban đầu cho hub/switch, chẳng hạn như văn phòng, phòng lưu trữ, tốt hơn là gần trung tâm máy tính. Ở những công trình đa tầng, các vị trí trung tâm nói chung sẽ được đặt gần lối.

Vẽ một vòng tròn bán kính 50 m từ mỗi vị trí hub và đảm bảo tất cả các nút nằm trong vòng tròn. Một số outlet có thể nằm bên ngoài bán kính này, nhưng không quá 15m.

Xem xét các vị trí trung tâm nhằm loại trừ các vị trí chồng lên nhau. Nhiều máy có thể phục vụ nhiều hơn một tầng, cung cấp một đường cáp dẫn dọc giữa chúng.

Chọn một hub là hub trung tâm. Nên đặt tại vị trí dễ sử dụng cho người có khả năng chịu trách nhiệm quản trị mạng, nhưng cũng phải dễ dàng tiếp cận cho việc bổ sung cáp xương sống trong tương lai, và tốt nhất là hướng vào vị trí trung tâm. Trên các miền lớn, người ta thường đặt trong phòng máy tính.

Hub có thể phục vụ nhiều hơn một cơ sở, vì vậy cần cung cấp đường cáp khả thi giữa các tòa nhà, công trình chia sẻ và phân phối chung từ nguồn. Khả năng này bao gồm:

- Cài đặt dưới đất với đường dẫn đã tồn tại hay lắp đặt mới. Đường dẫn mới thường được yêu cầu phô biến (dễ dàng nhất được cài đặt nếu tuyến đường là cổ hay qua vườn). Đặc biệt cáp CAT 5 ngầm phải được sử dụng để bảo vệ chống lại thiệt hại do độ ẩm gây ra.
- Chạy cable trong đường dẫn hay ghim chặt trên bìa ống dân hình chữ nhật theo đường đi an toàn được định sẵn trước.
- Các móc xích nên đặt lên trên bên giữa tòa nhà (có thể là phương pháp chỉ thực hiện với những công trình có thể di động).

2.7.3 Chọn tuyến đường xương sống

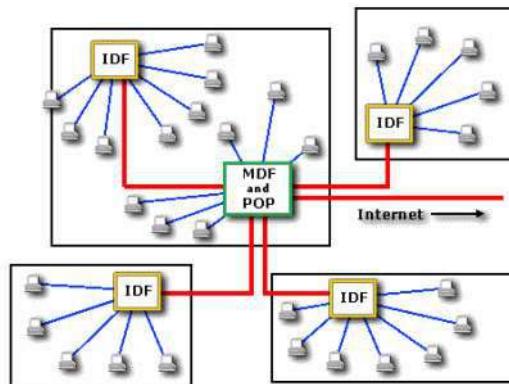
Việc chọn vị trí các hub định sẵn, đồng nghĩa với việc kết nối các workgroup hub với hub trung tâm. Trước đây, điều này được thực hiện

bằng các chạy 1 đường cable đồng Thin hoặc Thick Ethernet tại vị trí móc nối thuận loại nhất giữa toàn bộ các hub. Tuy nhiên điều này đã bộc lộ những giới hạn băng thông của toàn bộ mạng khi toàn bộ lưu lượng chỉ đi qua một dây duy nhất, và tại bất cứ vị trí nào cũng đều ẩn chứa khả năng làm gián đoạn mạng.

Cable đồng trực cũng có thể gây ra hiện tượng tạo ra liên kết năng lượng một cách vô ý trong tòa nhà, đây là nguyên nhân gây ra điện áp tăng trên mạng LAN, nếu một lỗi điện xảy ra thì sẽ làm đứt toàn bộ cầu chì trong tòa nhà. Phương pháp được sử dụng trong hệ thống cáp có cấu trúc là sử dụng riêng cặp cáp sợi quang (một cho truyền và một cho nhận) tản ra từ hub trung tâm đến mỗi workgroup. Ở những vị trí lưu thông tín hiệu thoại (điện thoại, ISDN,...) tương tự như mặt lưới được điều phối, nhiều cặp cáp cũng được cung cấp cho mục đích này từ một khung PABX / bảng nối hoặc MDF tới bảng điều khiển hoặc khung quản lý cáp tại mỗi vị trí đặt hub. Thông thường một hoặc nhiều cặp sợi bỗ sung sẽ được dự phòng ở vị trí trung tâm trong các phân khúc mạng nhằm dự trù cho tương lai, hoặc làm cho kết nối trực tiếp với máy chủ tập tin từ xa.

Nếu các hub nằm trong cùng tòa nhà, có thể liên kết chúng bằng cách sử dụng cáp Cat 5 nhằm cung cấp tới thiết bị đầu cuối, hay thiết bị phù hợp tương ứng và ở đây không tồn tại thiết bị chống sét, tăng điện áp, hoặc nối đất khiến có thể gây ra hỏng hóc (thường áp dụng thêm đối với cao ốc nhiều tầng). Cách đặt cáp sợi quang tùy thuộc vào mô hình trung tâm, và dàn nâng đỡ mạng. Bao gồm các khả năng sau đây:

- Khuôn cách cụm trung tâm, cáp riêng tản ra từ hub trung tâm như tăm trên một bánh xe.
- Khuôn cách vòng trung tâm - Cáp được tản quanh vòng, có thể đặt tất cả trong cùng một đường hoặc ống dẫn cho đến khi nó tới một trạm kết nối. Một cáp đa sợi có thể được chạy trong cùng tuyến đường này tới một bảng dây nối với workgroup, sau đó đem nối tới cable riêng để tiếp tục cho hub khác.
- Loại đường thẳng trung tâm - tương tự như với vòng, ngoại trừ cáp được đặt trong một đường thẳng đọc theo tường.



Hình 2.21. Mở rộng mạng Star trong thiết kế đa cơ sở trung tâm

2.7.4 Kết nối các workgroup tại Hub trung tâm

Mặc cho ấn tượng vẫn về rằng sợi quang sẽ xử lý dữ liệu tốc độ rất cao, trong thực tế, tốc độ của dữ liệu trên một sợi được quản lý bởi dữ liệu sẵn có giao tiếp với nó. Các giao diện tiêu chuẩn là 10 Mbit/s giống như dây xoắn đôi hoặc đồng. Tốc độ cao chỉ có thể đạt được bằng cách trả cho thiết bị mạng Fast Ethernet (100BaseFx, 100Mbit/s), FDDI (100 Mbit/giây) hoặc máy ATM (155 Mbit/giây), điều này chỉ kinh tế nếu mạng có hàng trăm máy trạm.

Việc cài đặt tối thiểu cho bất kỳ một miền với hơn hai hub là một repeater đa cổng. Hai hub có thể được liên kết bởi 1 hub tầng trung nhằm giảm một cổng repeater trên hub khác.

2.7.5 Kiểm tra phương pháp dự kiến

Sau khi tạo bản thảo kế hoạch hành động, cần phải xác minh rằng kiến trúc mạng được đề xuất là thực tế, nhằm xác nhận các vấn đề quan trọng không bị bỏ qua.

Tùy chọn cho đề nghị kiểm tra bao gồm:

- Tuyển kỹ sư tư vấn độc lập nhằm tạo ra một bản đánh giá
- Sử dụng phần mềm tư vấn để xem xét phương pháp đánh giá lại phần mềm.
- Thảo luận với các nhà cung cấp thiết bị tiềm năng và các nhà thầu cáp

- Thảo luận với các nhà cung cấp phần mềm
- Thảo luận với chi nhánh công nghệ thông tin của tổ chức
- Thảo luận với các doanh nghiệp tương đương ở một giai đoạn thực hiện nâng cao hơn

2.7.6 Liên kết các cơ sở

Nếu yêu cầu liên kết giữa cơ sở được đặt ra như là một phần của dự án, một số quyết định lựa chọn cần phải được thông qua và chỉ định tới loại cáp thích hợp. Chúng bao gồm:

- Liên kết sẽ được đặt lên hàng đâu? Nếu có, ước lượng cable kèm theo trong đường ống, hoặc nó sẽ được ra ngoài trời?
- Liên kết nào sẽ được chạy ngầm dưới lòng đất? Nếu có, cần phải đảm bảo độ ẩm của cable, thường xây dựng trong ống lồng.
- Có tồn tại tuyến đường ngầm sẵn có? Nếu không, lập kế hoạch cho phép các dịch vụ tương thích khác sử dụng cùng tuyến đường, chẳng hạn như bảo mật, giọng nói, điều khiển.
- Tuyến đường sẽ bị những mối nguy hại nào tấn công? Nếu có, yêu cầu nên bọc cáp hoặc sử dụng đường ống bao bọc cáp.
- Yêu cầu truyền thông băng thông rộng trong tương lai? Nếu có, cần dự trù một vài cặp sợi đơn chế độ.

Một số nhà thầu sẽ cung cấp bảo hành 5-20 năm trên bất cứ công việc đã hoàn thành, điều này nhằm đảm bảo sự tin tưởng, mặc dù bất kỳ việc thực hiện theo các tiêu chuẩn và đúng thiết kế, giám sát và thử nghiệm đều đáp ứng yêu cầu này.

Theo dõi trong quá trình cài đặt để bảo đảm rằng các cơ sở đang được cung cấp đúng như dự định, và rằng tất cả đường outlet được kiểm tra để đảm bảo các thông số kỹ thuật CAT 5 trước khi tuyên bố hoàn thành.

2.7.7 Chọn thiết bị

Trong quá trình cáp được cài đặt, có thể mua thiết bị hub. Thiết bị này sẽ cung cấp giao tiếp tới tất cả cáp, và chuyển lưu lượng dữ liệu giữa máy trạm, máy chủ tập tin, và các liên kết Internet.

Vẽ một giản đồ mạng đề xuất cho workgroup, máy chủ tập tin, máy in, hub và các đường xương sống, theo cách có thể minh họa các mối quan hệ chức năng và vật lý của các workgroup.

Tạo một danh sách những ứng dụng mạng yêu cầu, những lựa chọn ưa thích sẽ có, và các mục tiêu kết nối của mạng là gì?

Có thể sử dụng thiết bị của nhiều nhà cung cấp để tận dụng cơ sở hạ tầng cáp cung cấp, và đáp ứng các mục tiêu đặt ra. Bao gồm việc lắp đặt, nhiệm vụ nếu cần thiết. Thiết bị trung tâm được yêu cầu như sau:

- Hub mặt sau hoặc khung gầm: Yêu cầu ở vị trí đặt hub khuôn cách phích cắm được sử dụng. Cung cấp nguồn điện bình thường và kết nối trung gian.
- Các workgroup tập trung: Thay thế cho khung hub. Thường được dùng với hệ thống hub chồng, bao gồm repeater, giao tiếp đường trực sợi quang, nguồn cung năng lượng, và giao diện quản lý mạng đặt trong một hộp.
- Các repeater UTP (10BaseT): Thường sử dụng loại 8, 12, 16, 24 hoặc 32 cổng. Một cổng dành cho một máy trạm kết nối, máy chủ tập tin hoặc máy in. Phải có kết nối xếp chồng để làm việc với hub xếp chồng.
- Các repeater nội bộ thu nhỏ (8 hoặc 16 cổng): Được sử dụng để kết nối một cụm các PC trong một phòng đến hub đơn đặt tại buồng riêng, hoặc nơi có 15 máy tính hay ít hơn có khả năng kết nối đến vị trí hub. Sử dụng băng ngoài sợi quang 10BaseT hoặc chuyển đổi AUI nhằm kết nối tới sợi xương sống, nếu cần thiết.
- Các phương tiện giao tiếp sợi quang: Yêu cầu kết nối hub với sợi quang. Về cơ bản là một repeater đơn cổng hoặc phích cắm vòng quanh tích hợp cho hub.
- Repeater hoặc switch sợi quang đa cổng: Được sử dụng ở hub trung tâm để kết nối sợi quang.
- Switch: Sử dụng để cài đặt các workgroup xương sống và máy chủ nhằm cho phép các phiên đồng thời bên trong và giữa các phân đoạn

Số lượng các loại thiết bị khác nhau được sử dụng cũng cần được giảm thiểu, để các thiết bị dễ dàng trao đổi xung quanh trung tâm, và trang thiết bị thay thế trong một khu vực có thể được dùng để ở nơi khác. Nếu phụ tùng được thiết lập trên miền, hợp lý hóa thiết bị sẽ giảm thiểu hàng tồn kho.

2.8. HỒ SƠ THIẾT KẾ MẠNG LAN

2.8.1 Tài liệu lưu trữ

Tài liệu cần được lưu giữ vì nhiều lý do khác nhau. Một tài liệu đạt yêu cầu sẽ:

- Cho phép người không chuyên nhanh chóng nắm bắt các mô hình mạng. Điều này quan trọng nhất trong một môi trường mà nhân sự thay đổi thường xuyên.
- Giúp phát triển mạng theo kế hoạch được định sẵn và cách thức có cấu trúc, cho phép sử dụng ngân sách hiện một cách tốt nhất.
- Hỗ trợ người khác tham gia vào mạng của bạn như cài đặt cáp, giải quyết sự cố mạng và tư vấn. Bằng cách cho phép họ xem xét chính xác những gì được đặt ra, tiết kiệm thời gian và hiểu chính xác những gì được yêu cầu, mang lại kết quả là tiết kiệm chi phí.
- Cung cấp một công cụ có giá trị cho vị trí bị lỗi khi thực hiện sai.
- Hỗ trợ bảo hiểm phục hồi trong trường hợp hỏa hoạn hoặc trộm cắp.

2.8.2 Chi tiết các bản ghi

Các tài liệu không cần phải tồn thời gian hoặc quá mức trang trọng, nhưng ở một mức tối thiểu nên giữ lại các chi tiết sau đây.

- Bản vẽ trình bày vị trí chạy cáp, (tốt nhất với độ dài cáp đánh dấu riêng cho bất kỳ việc chạy cable Thin Ethernet).
- Kích thước và khoảng chiếm dụng của bất kỳ ống cáp hiện tại hoặc ống dẫn, có sẵn cho việc sử dụng khi mở rộng mạng.
- Các chi tiết về năng lực của các loại cáp và đầu kết nối sử dụng.
- Các chi tiết về loại kết nối hoặc ổ cắm ở hai đầu dây cáp (trạng thái bao phủ đầy đủ).

- Bản ghi tên và vị trí outlet.
- Bắt cứ chứng nhận thực hiện (ví dụ như kết quả kiểm tra cáp Cat5).
- Sơ đồ hiển thị mối quan hệ của các máy trạm làm việc, các máy chủ file, máy in và các thiết bị khác trong mạng với nhau.
- Sơ đồ hiển thị làm cách nào mà mỗi hub, bridge, switch, router bắt kỳ kết nối mạng (có thể được hiển thị trên hệ thống quản lý mạng).
- Bản ghi giấy phép phần mềm và các phiên bản của phần mềm được cài đặt.
- Cấu hình của card mạng máy trạm.
- Trả tiền cho bản sao của tiêu chuẩn được đề nghị cho quản trị hệ thống.

2.8.3 Các bản ghi dây nối và đầu cắm

Bản ghi dây nối nên được giữ lại ở mỗi bảng vá lỗi hoặc kết nối ngang. Nhiệm vụ của chúng là xác định các mối quan hệ giữa hub và các cổng của switch, cổng nối dây, và các thiết bị đầu cuối. Có thể dùng bảng tính để tự động hóa quá trình này. Cơ sở dữ liệu và hệ thống quản lý cáp được sử dụng để cung cấp sự tinh tế nhất, nhưng có thể mang lại sự rườm rà để nhập và duy trì dữ liệu.

2.8.4 Quản trị hệ thống

Nhu cầu của mạng máy tính không chỉ đơn giản là để kết nối một nhóm các máy tính với nhau tại một thiết bị kết nối trung tâm. Mạng đòi hỏi phần mềm đặc biệt gọi là hệ điều hành mạng (NOS), cho phép liên lạc giữa các thiết bị khác nhau. Các phần mềm NOS không đơn giản là tự nó có thể chạy. Nó đòi hỏi một người gọi là quản trị hệ thống để thực hiện chức năng quản trị bằng cách sử dụng phần mềm NOS để thực hiện các tác vụ như sao lưu tập tin, giữ cho lưu lượng mạng ổn định, và đảm bảo nhiều người sử dụng có quyền truy cập, giao tiếp với máy in, Internet, và với các máy tính khác. Khi hệ thống máy tính bị treo, quản trị hệ thống sẽ khôi phục nó trở lại trạng làm việc như trước. Khoảng thời gian và kỹ năng cần thiết của quản trị hệ thống phụ thuộc vào kích cỡ của mạng. Đối với một mạng lưới gồm 10 máy tính trung bình chỉ yêu cầu một giờ/tuần. Đối với

một mạng 100 máy vi tính, nó sẽ là 10 giờ/tuần. Mạng càng phức tạp liên quan đến bridge, router hoặc các máy chủ Internet thì đòi hỏi nhiều thời gian và kỹ năng hơn so với các mạng đơn giản.

2.8.5. Bảo trì và sửa chữa

Không thể tránh khỏi một số thiết bị sẽ hư hỏng hoặc cần nâng cấp. Một mạng rộng lớn với hơn 100 máy tính cần yêu cầu một kỹ thuật viên dành 20 giờ mỗi tuần. Đối với một mạng nhỏ, 10 máy vi tính có thể trả thêm chi phí cho một nhân viên có thẩm quyền thực hiện những nâng cấp cần thiết, hoặc đưa trang thiết bị tới một đại lý sửa chữa. Cho nên vấn đề này cần được xem xét khi thực hiện hợp đồng với một nhà cung cấp hoặc đại lý.

2.9. MỘT SỐ NGUYÊN TẮC HƯỚNG DẪN

2.9.1. Hướng dẫn ngăn cách cáp UTP khỏi nguồn có độ nhiễu từ cao

Điều kiện	<2kVA	2-5kVA	>5kVA
Đường dây điện không được bọc vỏ hoặc thiết bị điện ở gần nhau để mở hoặc đường dẫn phi kim loại	5 inch hoặc 12.7cm	12 inch hoặc 30.5 cm	24 inch hoặc 61 cm
Đường dây điện không bọc vỏ hoặc thiết bị điện ở gần đường ống kim loại	2.5 inch hoặc 6.4 cm	6 inch hoặc 15.2 cm	12 inch hoặc 30.5 cm
Đường dây điện kèm theo một đường ống kim loại (che chắn tương đương) ở gần vị trí đặt đường ống kim loại	-	6 inch hoặc 15.2 cm	12 inch hoặc 30.5 cm
Đèn huỳnh quang	12 inch hoặc 30.5 cm		
Máy biến áp và động cơ điện	40 inch hoặc 1.02 m		

2.9.2 Bán kính uốn cong tối thiểu cho dây cáp

Theo EIA/TIA SP-2840A bán kính uốn cong tối thiểu cho UTP là 4x đường kính cáp, đường kính khoảng 1 inch. Đối với cáp đa cặp bán kính tối thiểu uốn cong là 10x đường kính bên ngoài.

Đối với cáp quang không có độ căng, bán kính uốn cong tối thiểu là 10 x đường kính; cáp tải trọng với độ căng không được nhỏ hơn 20x

đường kính. Phát biểu SP-2840A nói rằng không có cáp sợi quang có bán kính nhỏ hơn 3,0 cm (1,18 inch).

Tối thiểu cho việc kéo trong khi cài đặt là 8x đường kính cáp, bán kính tối thiểu là 6x đường kính cáp nguyên gốc, 4x đường kính cáp cho cáp ngang.

2.9.3. Khuyến cáo cáp trên thực tiễn

NÊN	KHÔNG NÊN
Sử dụng kết nối phần cứng thích hợp với cable được cài đặt	Không sử dụng kết nối phần cứng với chủng loại thấp hơn cáp đang sử dụng
Chấm dứt mỗi cáp ngang tại một outlet viễn thông chuyên dụng	Đừng ngắt một dòng mới từ giữa cáp khác (gọi là bridge tap), vì nó gây tiếng ồn nhiều hơn nữa. Không dùng cable cho thiết bị không phải đầu cuối
Xác định vị trí kết nối chéo chính gần trung tâm của tòa nhà để giới hạn khoảng cách cáp	Không đặt vị trí kết nối chéo vượt quá khoảng cách tối đa cho phép.
Duy trì vòng xoắn của cặp cáp ngang và xương sống cho tới điểm kết thúc	Đừng để bắt cứ cặp dây nào tháo xoắn (Giữ xoắn cho đến gần những điểm cuối).
Cột và bọc gọn gàng cáp ngang với bán kính uốn cong tối thiểu là 4 lần đường kính cáp	Không thắt chặt cable. Không bao giờ sử dụng ghim hoặc làm cho cable bị gấp khúc
Đặt cáp ở khoảng cách vừa đủ tới thiết bị	Không đặt cable gần thiết bị có sự nhiễu từ cao (dây nguồn, đèn huỳnh quang,...)

Khi chạy cáp, cách tốt nhất là làm theo một vài quy tắc sau:

- Luôn luôn dự trù cable sử dụng, đường dây nối nên để chùng.
- Kiểm tra tất cả các phần của một mạng khi cài đặt nó. Thậm chí nếu nó là thương hiệu mới, ở đây có thể tồn tại nhiều vấn đề khó khăn để cài đặt sau này
- Giữ ít nhất 3 feet từ hộp đèn huỳnh quang và các nguồn điện khác
- Nếu là cần thiết để chạy cáp trên sàn nhà, bảo vệ cable bằng việc bao bọc nó cẩn thận.
- Đánh nhãn cả hai đầu cáp.

- Sử dụng dây buộc cáp (không phải băng keo) để giữ dây cáp ở cùng một vị trí với nhau.
- Các đường ống hoặc vỏ không nên dính hoàn toàn với cáp. Nên có chỗ cho việc mở rộng trong tương lai.

2.9.4. Thực hành cài đặt cable UTP

- Để tránh kéo dài, kéo căng không được vượt quá 110N hoặc (25 lb f) cho 4 - cặp cáp.
- Cài đặt uốn cong bán kính không quá: - 4 lần đường kính cáp cho cáp ngang UTP - 10 lần đường kính cáp cho nhiều cặp cáp xương sống UTP.
- Tránh căng cáp, gây ra bởi: - cáp xoắn trong khi kéo hoặc cài đặt - căng trong khi chạy cáp treo – ghì hoặc ghim chặt cáp – dẫn đến bán kính bị uốn cong.
- Cáp ngang nên được sử dụng với kết nối phần cứng và bảng nối dây (hoặc đầu nối) cùng chung hiệu suất hoặc cao hơn.
- Lưu ý: Việc cài đặt cáp UTP sẽ được phân loại bởi các thành phần ít thực hiện nhất trong liên kết.

2.9.5. Lắp đặt kết nối phần cứng sợi quang

Các chi tiết kỹ thuật trên sợi cáp quang bao gồm nhận dạng loại cáp cho hệ thống con nằm ngang và hai loại cáp cho hệ thống phụ xương sống:

- a) Ngang 62.5/125 µm đa mode (hai sợi trên một outlet)
- b) Đường trục 62,5/125 µm đa hoặc đơn mode

Sau đây là một số nguyên tắc phải tuân theo trong khi cài đặt phần cứng kết nối sợi quang:

- Đầu kết nối phải được bảo vệ khỏi thiệt hại vật lý và độ ẩm
- Cần cung cấp sức chứa cho 12 sợi hoặc hơn/ không gian rack [44,5mm (1.75 inche)]

- Kết nối phần cứng sợi quang sẽ được cài đặt:
 - + Để cung cấp cách tổ chức lắp đặt tốt với việc quản lý cáp
 - + Theo đúng nguyên tắc nhà sản xuất hướng dẫn

2.9.6. Lắp đặt sợi cáp quang

- Tối thiểu 1m (3.28ft) cho hai sợi cáp (hoặc hai sợi đệm) được sử dụng với mục đích châm dứt
- Khuyến khích thử nghiệm để đảm bảo tính chính xác và hiệu suất liên kết chấp nhận được. Thông tin trong phụ lục H của 568-A cung cấp cho tiêu chí đề nghị thử nghiệm hiệu suất liên kết sợi quang học.

2.10. GIỚI THIỆU TIỀN 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 tiền 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 lai 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 cho sơ đồ mạng LAN và WAN.
- Làm tài liệu cài đặt mạng ở mức vật lý và mức logic.

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.
- **Được quản lý:** 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.

2.10.1. 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:

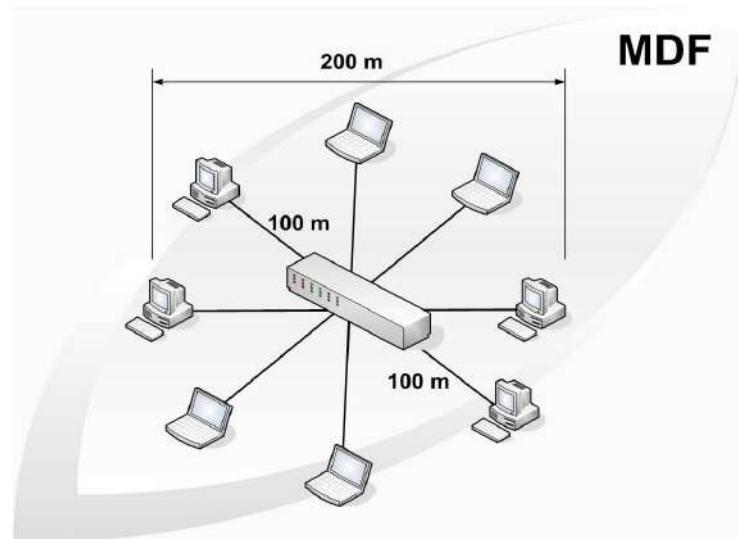
- Thiết kế sơ đồ mạng ở tầng vật lý
- Thiết kế sơ đồ mạng ở tầng liên kết dữ liệu
- Thiết kế sơ đồ mạng ở tầng mạng.

2.10.2. 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.

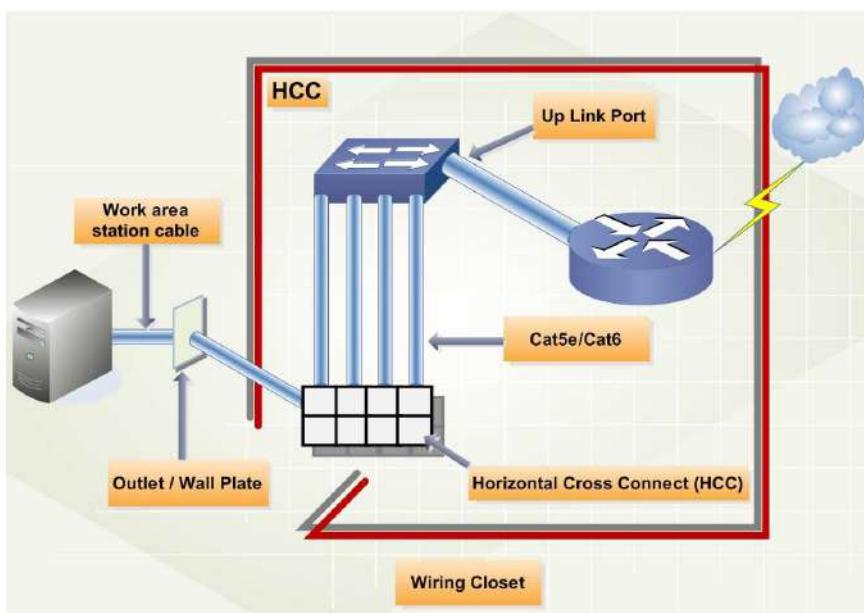
Sơ đồ mạng hình sao sử dụng cáp xoắn đôi CAT5 (Cat5e) thường được dùng hiện nay. Đôi với các mạng nhỏ, chỉ cần một điểm tập trung nối kết cho tất cả các máy tính với điều kiện rằng khoảng cách từ máy tính đến điểm tập trung nối kết là không quá 100 mét.

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 cắm dây (patch panels). Người ta gọi phòng này là “Nơi phân phối chính” - MDF (Main Distribution Facility).



Hình 2.22. Sử dụng MDF cho các mạng có đường kính nhỏ hơn 200 mét

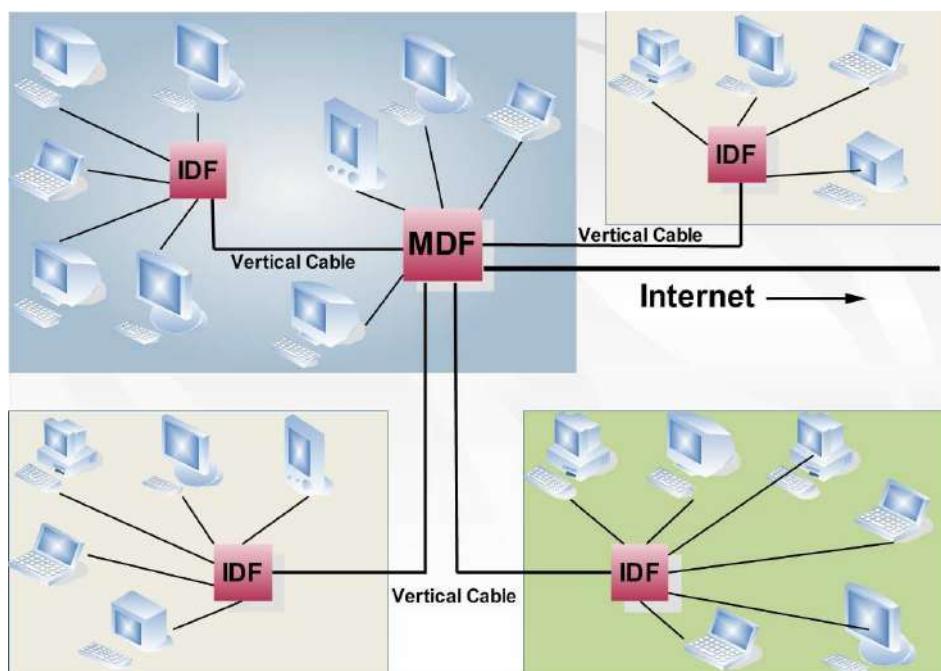
Đối với các mạng nhỏ với chỉ một điểm tập trung nối kết, MDF sẽ bao gồm một hay nhiều bảng cắm dây nối kết chéo nằm ngang (HCC – Horizontal Cross Connect patch panel).



Hình 2.23. Sử dụng HCC patch panel trong MDF

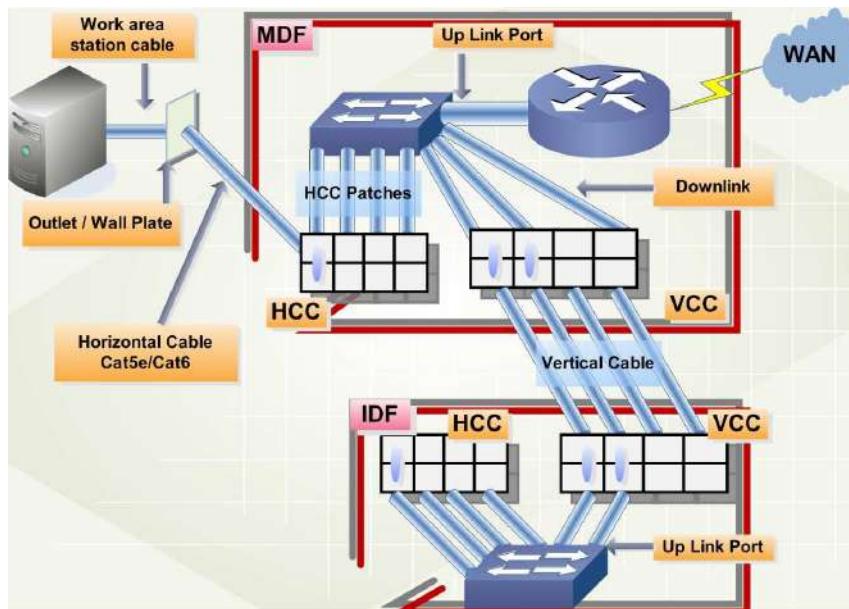
Số lượng cáp chiều ngang (Horizontal Cable) và kích thước của HCC patch panel (số lượng cổng) phụ thuộc vào số máy tính nối vào mạng.

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 2.24. Sử dụng thêm các IDF cho các mạng
có đường kính lớn hơn 200 mét*

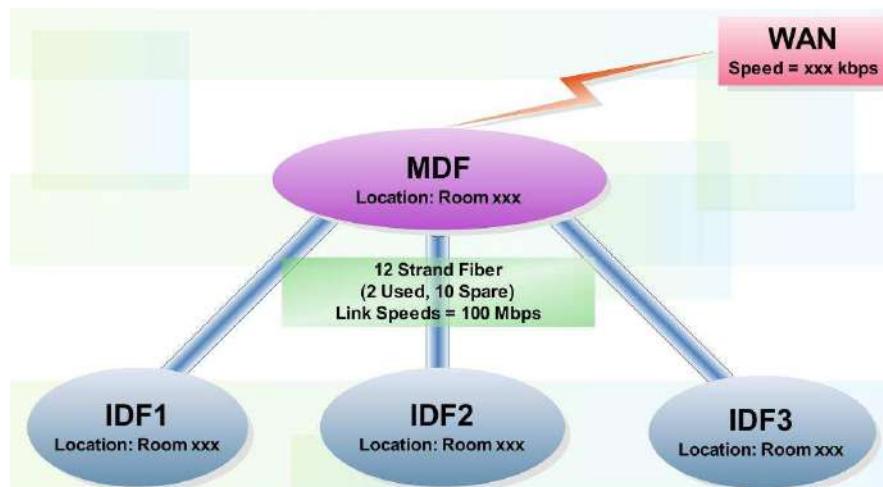
Để có thể nối các IDF về một MDF cần sử dụng thêm các patch panel nối kết chéo chiều đứng (VCC – Vertical Cross Connect Patch Panel). Dây cáp nối giữa hai VCC patch panel được gọi là cáp chiều đứng (Vertical Cabling). Chúng có thể là cáp xoắn đôi nếu khoảng cách giữa MDF và IDF không lớn hơn 100 mét.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



Hình 2.25. 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 MDF và IDFs.
- Kiểu và số lượng cáp được sử dụng để nối các IDF về MDF



Hình 2.26. 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.

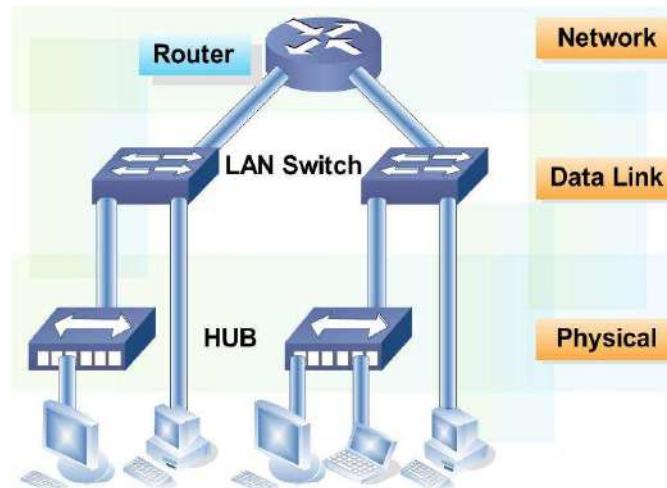
IDF1
Location-Rm XXX

Connection	Cable ID	Cross Connection Paired#/Port#	Type of Cable	Status
IDF1 to Rm 203	203-1	HCC1/Port 13	Category 5 UTP	Used
IDF1 to Rm 203	203-2	HCC1/Port 14	Category 5 UTP	Not used
IDF1 to Rm 203	203-3	HCC2/Port 3	Category 5 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 2.27. Thông tin dây nối tại một IDF

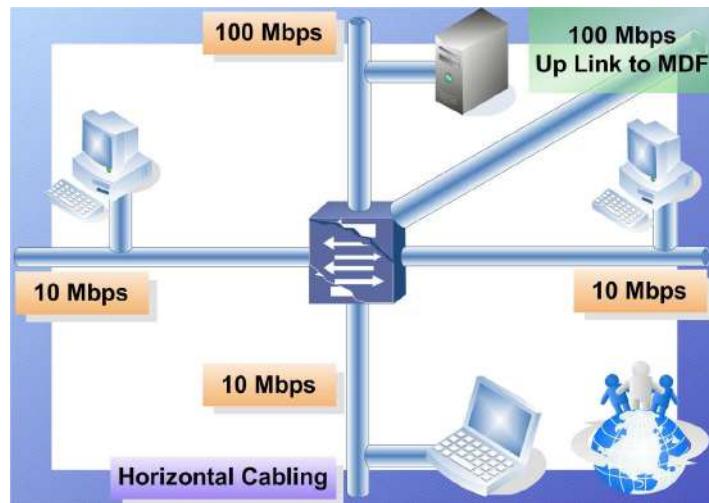
2.10.3. Nối kết tầng 2 bằng switch

Sự dụng độ và kích thước vùng dụng 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 tần suất đụng độ giữa các máy tính và giảm được kích thước của vùng dụng độ trong mạng.



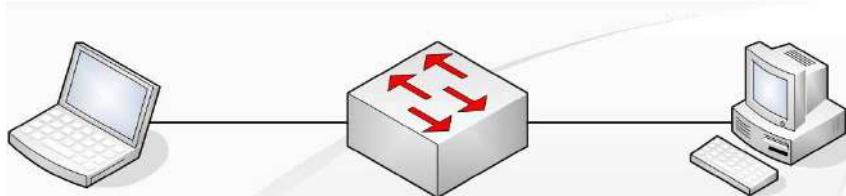
Hình 2.28. Sử dụng Switch để mở rộng băng thông mạng

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



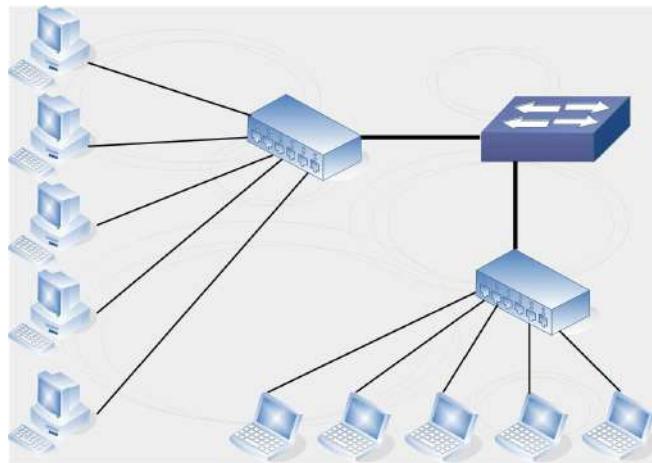
Hình 2.29. Sử dụng cổng tốc độ cao trong switch

Để xác định kích thước của vùng đụng độ bạn cần xác định bao nhiêu máy tính được 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 gửi và máy nhận tham gia vào mỗi cuộc giao tiếp.



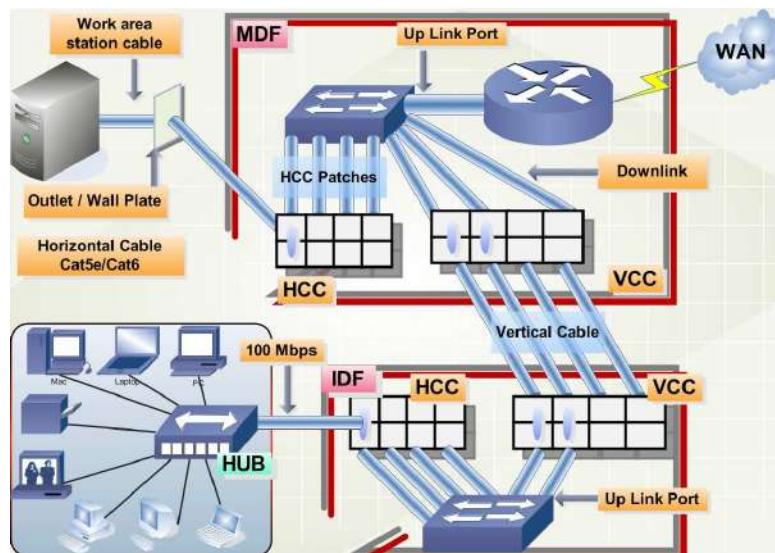
Hình 2.30. Nối trực tiếp các máy tính vào switch

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 sẻ nhau băng thông trên Hub.



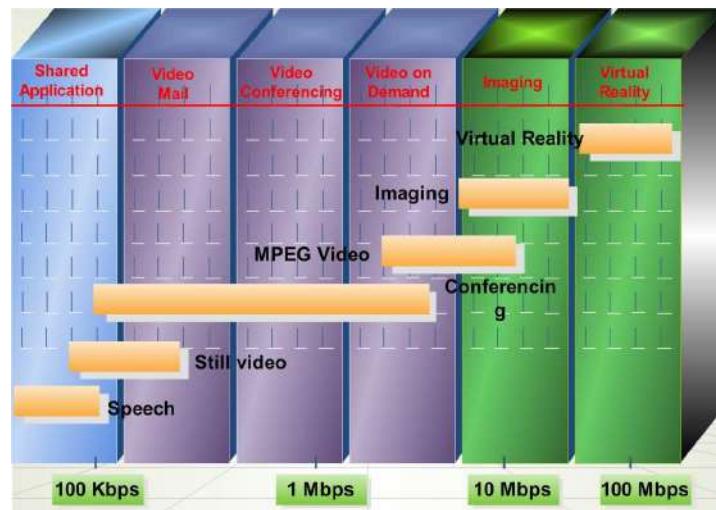
Hình 2.31. Nối HUB vào switch

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 dụng 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 2.32. Sử dụng cổng tốc độ cao của HUB để nối với Switch

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



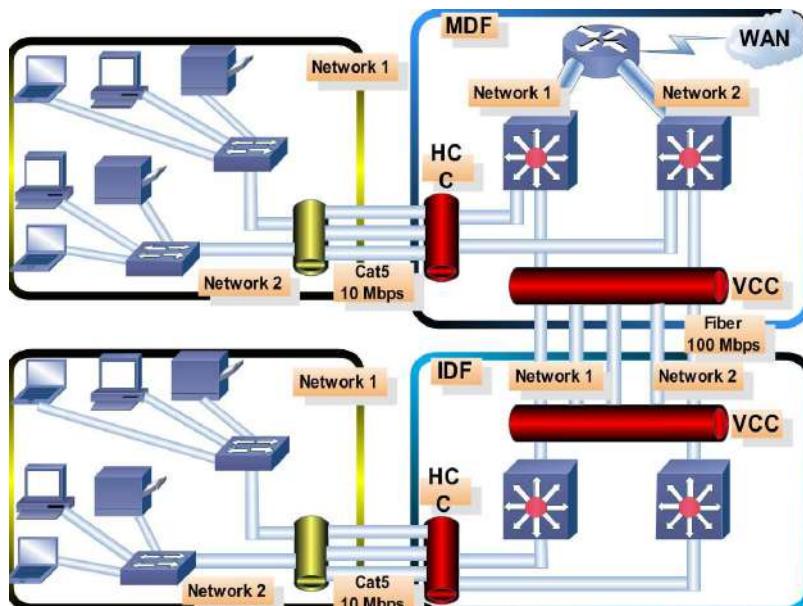
Hình 2.33. Nhu cầu băng thông của các ứng dụng

Sau khi đã thiết kế xong sơ đồ mạng ở tầng hai, cần thiết phải ghi nhận lại 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 Room 203	203-1	HCC1 / Port 13	CAT5 UTP	Used	10 Mbit/s
IDF1 to Room 203	203-2	HCC1 / Port 14	CAT5 UTP	Not Used	10 Mbit/s
IDF1 to Room 203	203-3	HCC2 / Port 3	CAT5 UTP	Not Used	10 Mbit/s
IDF1 to MDF	IDF1-1	VCC1 / Port 1	Multimode Fiber	Used	100 Mbit/s
IDF1 to MDF	IDF1-2	VCC1 / Port 2	Multimode Fiber	Used	100 Mbit/s

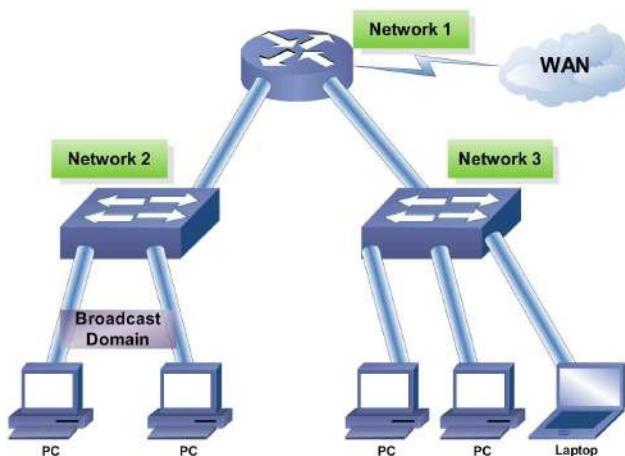
Hình 2.34. Tài liệu về tốc độ trên từng cổng



Hình 2.35. Băng thông sử dụng trong các kết nối

2.10.4. 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 modun tách rời nhau về mặt vật lý cũng như logic. Router cũng cho phép nối kết mạng với mạng diện rộng như mạng Internet chặng hạn.



Hình 2.36. Sử dụng router để phân chia vùng đệm độ trong mạng

Router cho phép hạn chế được các cuộc truyền quảng bá xuất phát từ một vùng dụng độ này lan truyền sang các vùng dụng độ khác. Nhờ đó tăng băng thông trên toàn mạng. Đối với switch, gói tin gửi 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 an 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.

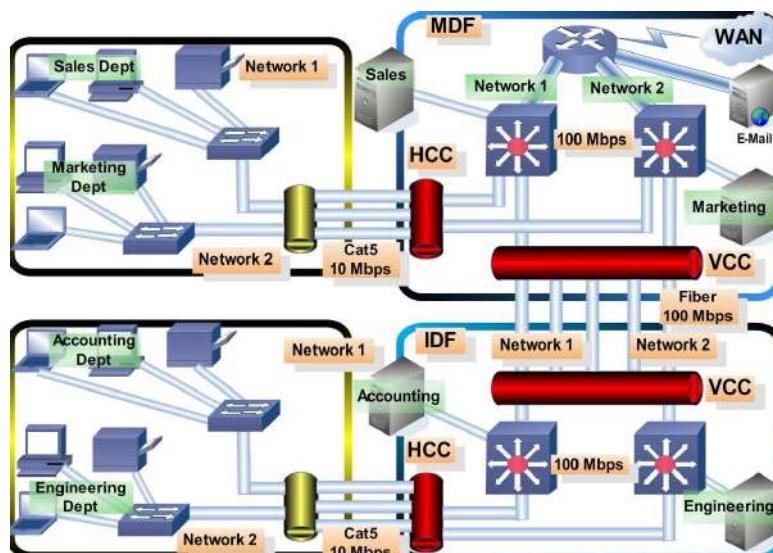
Trong ví dụ sau, mạng có nhiều nhánh mạng vật lý, tất cả các thông tin đi trao đổi giữa mạng Network 1 và mạng Network 2 đều phải đi qua router. Router đã chia mạng thành hai vùng dụng độ riêng rời. Mỗi vùng dụng độ có địa chỉ mạng và mặt nạ mạng riêng.

2.10.5. 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.

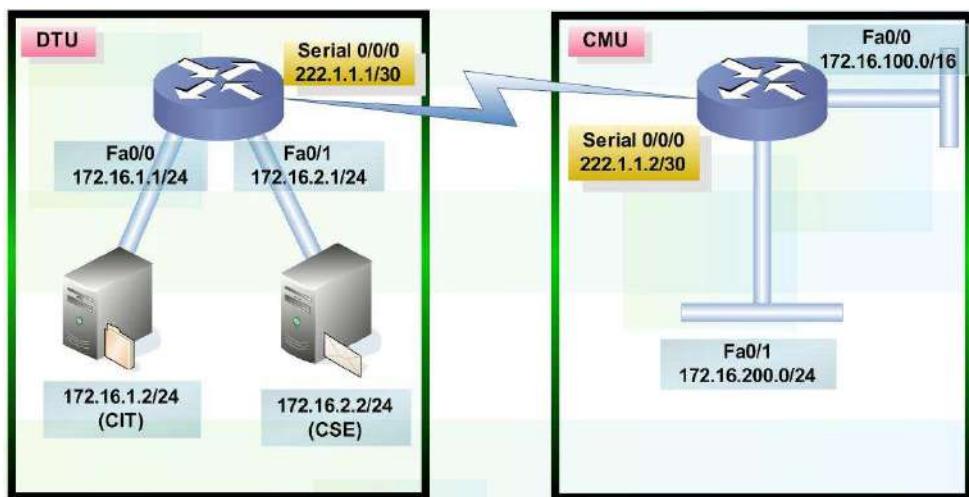


Hình 2.37. Tài liệu về vị trí đặt các server

2.10.5. 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 lập ra bao gồm:

- Bản đồ phân bổ địa chỉ IP



Hình 2.38. Bản đồ phân bổ địa chỉ IP

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

IP Network: 172.16.0.0 Subnet mask: 255.255.0.0	
DTU	CMU
172.16.1.0 ==> 172.16.99.0 Subnet Mask: 255.255.255.0	172.16.100.0 ==> 172.16.200.0 Subnet Mask: 255.255.255.0
Router name: DTU_Router Serial 0/0/0: 222.1.1.1/30	Router name: DTU_Router
Fa0/0: 172.16.1.1/24 Fa0/1: 172.16.2.1/24	Fa0/0: 172.16.100.1/24 Fa0/1: 172.16.200.1/24

Hình 2.39. Bảng tóm tắt về địa chỉ đã phân bổ

2.11. BÀI TẬP ỦNG DỤNG THIẾT KẾ LAN

Bài 1.

I. Giới thiệu:

VTMobile là công ty chuyên cung cấp các dịch vụ viễn thông. Gần đây công ty mở rộng hoạt động sang một thành phố mới và có mua một tòa nhà ở đây.

Tòa nhà này có 2 tầng, hệ thống cable chưa có. Tình trạng hiện tại của 2 tầng:

- Tầng 1: Được cấp cho bộ phận kế toán, tài chính, nhà kho, bảo vệ,... gồm 9 phòng riêng biệt.
- Tầng 2: Gồm 4 phòng (Phòng họp, P.Giám đốc, P.Trực ban, Phòng IT)

Nhu cầu hiện tại:

- Vì tầm quan trọng của dữ liệu của công ty nên vấn đề bảo mật được đặt lên hàng đầu. Phải có chính sách kiểm soát truy nhập hợp lý.
- Phòng tài chính phải được tách biệt với các phòng ban khác.
- Phải luôn đảm bảo kết nối giữa chi nhánh và TCT là 24/7.
- Phải đảm bảo rằng Ban UD CNTT (Năm ở TCT) có thể quản trị được các thiết bị mạng và máy chủ phòng tài chính.
- Không cho nhân viên gửi email ra ngoài, chỉ dùng mail của công ty.
- Không được phép sử dụng các phần mềm chat, như Y!M.
- Trong vòng 5 → 10 năm nữa thì chi nhánh này sẽ được xây dựng lại.

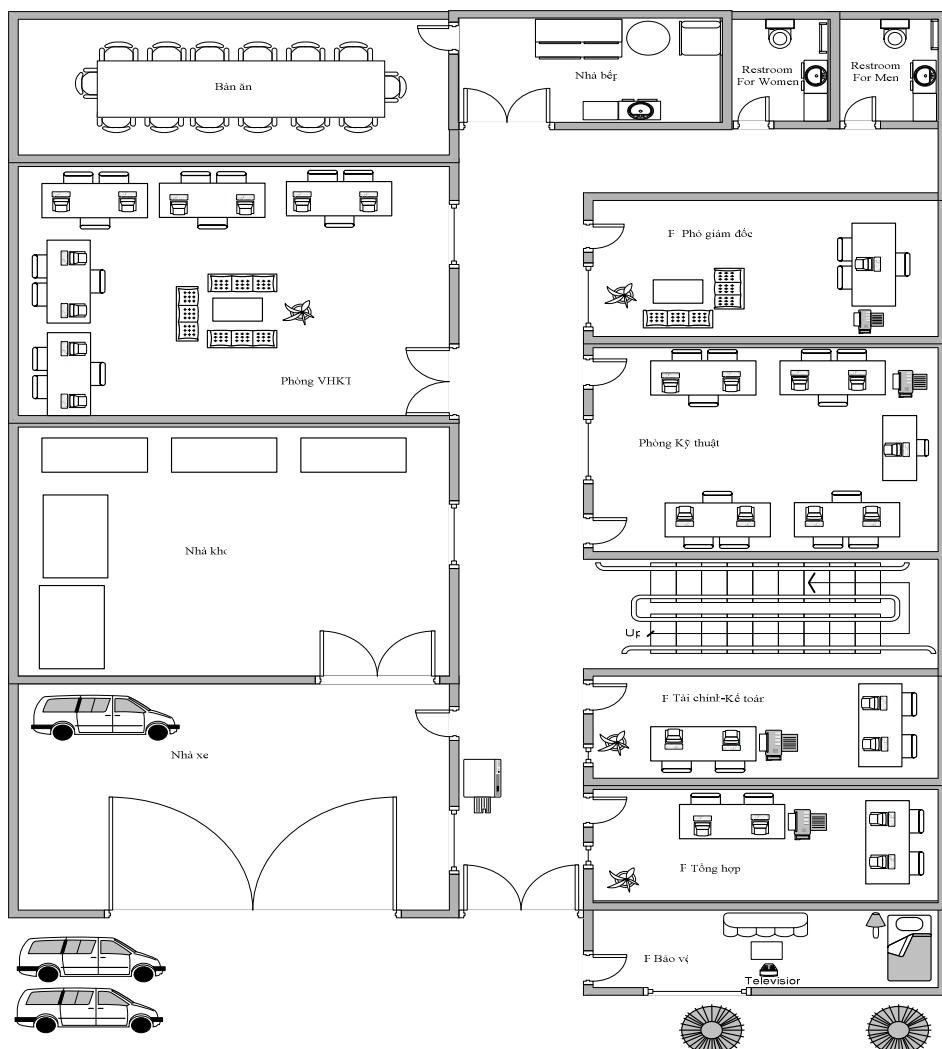
II. Thu thập và phân tích yêu cầu

Hiện nay mạng LAN tại các chi nhánh kinh doanh và chi nhánh kỹ thuật, đại diện vùng kết nối khá phức tạp, hầu hết mô hình mạng là tự đơn vị phát triển, theo hướng cần đến đâu kết nối đến đó, không theo mô hình chuẩn. Việc kết nối giữa các phòng ban được thực hiện tùy tiện, việc này dẫn đến tình trạng khó khăn trong việc quản lý, mở rộng mạng. Hệ thống mạng chỉ bao gồm các thiết bị Modem, Switch và Hub đơn giản, không có thiết bị chuyên dụng để tăng cường an ninh bảo mật và kiểm soát truy nhập. Nhằm mục đích đảm bảo hệ thống mạng hoạt động ổn định, tăng cường an ninh bảo mật, kiểm soát việc trao đổi thông tin giữa các vùng trong mạng và với mạng bên ngoài, đảm bảo hệ thống dễ dàng trong việc mở rộng và khắc phục sự cố.

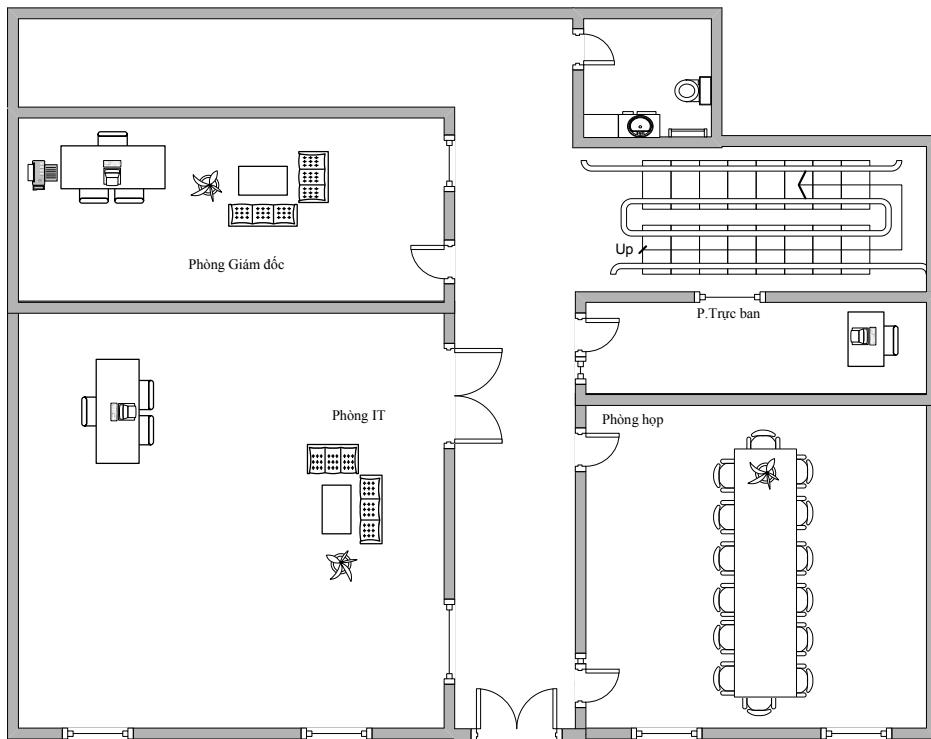
Nhân viên IT tại đơn vị thực hiện các công việc:

- Là đầu mối tiếp nhận, triển khai hệ thống mạng LAN.
- Quản lý hệ thống cáp mạng kết nối các phòng ban.
- Quản lý và duy trì hoạt động ổn định của các thiết bị mạng.
- Xây dựng, quản lý hồ sơ mạng: File cấu hình, Sơ đồ vật lý, sơ đồ logic.

Sơ đồ mặt chiếu bằng toàn nhà:



Hình 2.40. Sơ đồ mặt chiếu bằng tầng 1



Hình 2.41. Sơ đồ mặt chiếu bằng tầng 2

III. Thiết kế giải pháp

Hệ thống cable được thiết kế với yêu cầu: Phải có thêm 1 line dự phòng từ các phòng ban kết nối về phòng IT.

Hệ thống mạng LAN được chia thành 6 vùng (zone), được phân chia bởi thiết bị trung tâm của mạng là Firewall.

- Vùng kết nối máy trạm của các phòng ban (Trust).
- Vùng kết nối máy trạm của phòng tài chính (TaiChinh).
- Vùng kết nối máy chủ tài chính (DMZ).
- Vùng kết nối WAN ERP (ERP).
- Vùng kết nối mạng Internet (UnTrust).
- Vùng kết nối WIFI(WIFI)

Lưu ý: Vùng kết nối Wifi được sử dụng để kết nối với các thiết bị Access Point, kết hợp với các chính sách phù hợp được thiết lập. Việc sử dụng các thiết bị Wifi phải tuân thủ các quy định hiện hành của TCT.

Thiết bị Switch Layer 2

- Thiết bị Switch layer 2 có chức năng chính là phân tách các vùng va chạm trong mạng nội bộ của chi nhánh; gom lưu lượng của toàn bộ các máy tính nội bộ và đưa ra thiết bị firewall.
- Thiết bị Switch Layer 2 cung cấp 24 cổng kết nối 10/100 FE cho các thiết bị.
- Trên Switch Layer 2 chia thành 3 VLAN: VLAN 101 dùng cho các máy trạm, của các phòng ban, không kể phòng tài chính, kết nối với vùng phía trong của Firewall (Zone Trust); VLAN 103 dùng cho các máy trạm phòng tài chính, kết nối với vùng TaiChinh của Firewall (Zone TaiChinh); VLAN 102 dùng cho các kết nối với Modem ADSL, kết nối vùng ERP của Firewall.

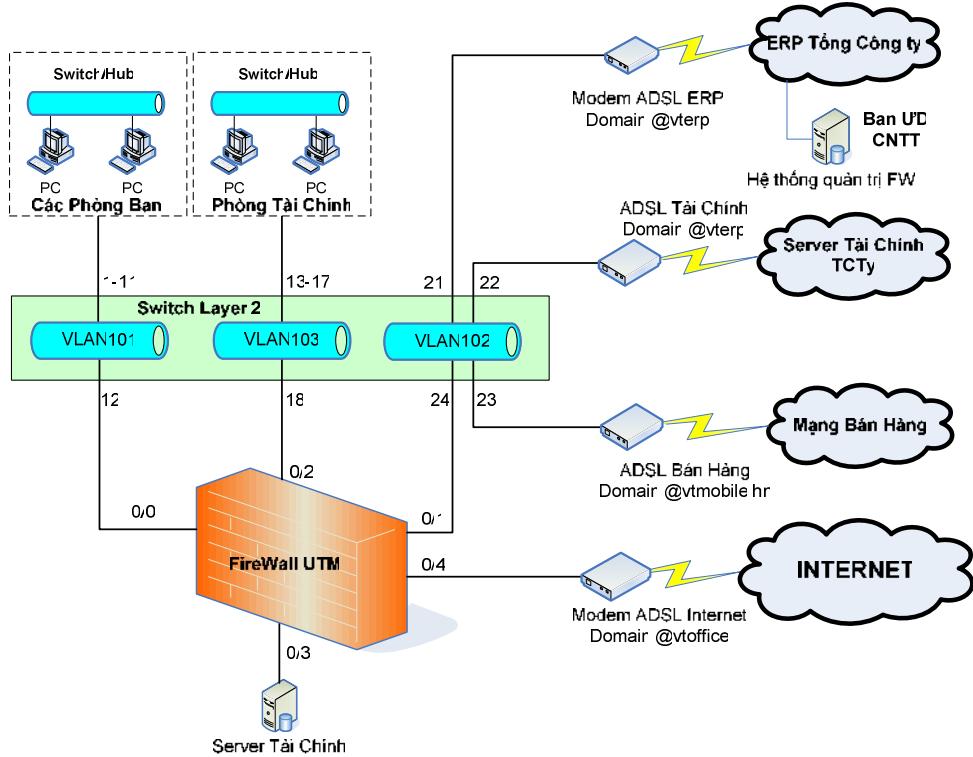
Thiết bị FW UTM

- Thiết bị FW UTM có 7 cổng kết nối 10/100 FE, được chia thành 6 vùng (zone), một port dự phòng, mỗi zone được sử dụng cho một vùng mạng bao gồm mạng nội bộ của các phòng ban (Trust), mạng nội bộ của phòng tài chính (TaiChinh), mạng máy chủ tài chính (DMZ), kết nối mạng ngoài Modem ADSL Internet (Untrust), vùng kết nối mạng ERP (ERP), vùng WiFi (WiFi).
- FW UTM sẽ thực hiện cách ly lưu lượng giữa các vùng, thực thi các chính sách định tuyến lọc gói tin và hạn chế truy nhập giữa các vùng khác nhau.

Modem ADSL

- Modem ADSL Internet: Kết nối mạng LAN của các Chi nhánh Kinh doanh, Chi nhánh kỹ thuật, Đại diện vùng với mạng Internet thông qua domain VTOffice.
- Modem ADSL ERP: Kết nối mạng LAN của các Chi nhánh Kinh doanh, Chi nhánh kỹ thuật, Đại diện vùng với hạ tầng mạng ERP của TCT, phục vụ việc trao đổi thông tin nội bộ, sử dụng các ứng dụng và thực thi chính sách bảo mật tập trung.
- Modem ADSL Tài Chính: Kết nối phục vụ cho việc trao đổi thông tin liên quan đến máy chủ Tài chính giữa các chi nhánh và TCT.
- Modem ADSL Bán Hàng: Kết nối mạng Bán hàng tại các Chi nhánh với mạng bán hàng và ứng dụng nội bộ của TCT.

3.1. Thiết kế sơ đồ mạng ở mức logic



Hình 2.42. Sơ đồ mạng ở mức logic

3.2. Thiết kế sơ đồ mạng ở mức vật lý

3.2.1. Quy hoạch giao diện kết nối

Quy hoạch các giao diện kết nối đảm bảo tính thống nhất trong cấu hình thiết bị, thuận tiện trong vận hành, khai thác, quản lý và xử lý sự cố mạng.

- Giao diện kết nối của Switch Layer 2



Hình 2.43. Quy hoạch cổng Switch layer 2

Thiết bị	Cổng	VLAN	Mục đích
Switch Layer 2	1 -> 11	101	Kết nối máy tính các phòng ban
	12	101	Kết nối cổng 0/0 của Firewall
	13->17	103	Kết nối các máy tính phòng Tài chính
	18	103	Kết nối cổng 0/2 của Firewall
	19 -> 20	102	Dự phòng
	21	102	Modem ADSL ERP
	22	102	Modem ADSL Tài Chính
	23	102	Modem ADSL Bán Hàng
	24	102	Kết nối cổng FW UTM Port 0/1

- Giao diện kết nối của FW UTM



Hình 2.44. Quy hoạch cổng thiết bị Firewall

Thiết bị	Port	Zone	Port Switch	VLAN	Mục đích
FW UTM	0/0	Trust	12	101	Kết nối các phòng ban
	0/1	ERP	24	102	Kết nối các modem ERP, Tài chính, Bán hàng
	0/2	TaiChinh	18	103	Kết nối phòng tài chính
	0/3	DMZ		104	Kết nối máy chủ Tai chinh
	0/4	UnTrust		105	Kết nối Modem ADSL Internet
	0/5	WiFi		106	Kết nối WiFi (Hiện nay chưa sử dụng)
	0/6			N/A	Dự phòng

3.2.2. Quy hoạch địa chỉ IP

Địa chỉ IP WAN sử dụng cho domain VToffice và domain VTBeer là địa chỉ IP private, được sử dụng thống nhất và theo quy hoạch mạng Intranet ADSL của Tổng công ty.

Địa chỉ IP WAN sử dụng cho domain VTmobile cũng là địa chỉ IP private, được sử dụng thống nhất và theo quy hoạch mạng của VTTelcom.

- Địa chỉ trong mạng LAN

Bảng 3.3. Quy hoạch địa chỉ IP và VLAN

STT	VLAN	Địa chỉ	Mục đích
1	101	192.168.1.0/24	Các phòng ban
2	102	192.168.2.0/24	Kết nối ERP
3	103	192.168.3.0/24	Phòng Tài chính
4	104	192.168.4.0/24	Máy chủ tài chính
5	105	192.168.5.0/24	Kết nối Modem Internet
6	106	192.168.6.0/24	WiFi

- Địa chỉ VLAN 101

Bảng 3.4. Quy hoạch địa chỉ VLAN 101

STT	Từ địa chỉ - đến địa chỉ	Subnetmask	Mục đích
1	192.168.1.10 → 192.168.1.60	255.255.255.0	Máy trạm
2	192.168.1.1	255.255.255.0	Gateway, trên FW UTM
2	192.168.1.2	255.255.255.0	Địa chỉ quản lý của Switch

Các thông tin về địa chỉ, subnetmask, gateway, DNS server của các máy trạm sẽ do FW UTM cấp động thông qua giao thức DHCP.

Ghi chú: Nhân viên IT tại chi nhánh sẽ thực hiện việc quản lý, theo dõi hoạt động của thiết bị Firewall và Switch từ một máy trạm trong VLAN 101.

- Địa chỉ VLAN 102

Các địa chỉ IP trong VLAN 102 được sử dụng cho giao diện LAN của Modem, UTM, không sử dụng cho máy trạm.

Bảng 3.5. Quy hoạch địa chỉ VLAN 102

STT	Địa chỉ IP	Subnetmask	Mục đích
1	192.168.2.1	255.255.255.0	Gateway, trên UTM/Quản lý
2	192.168.2.2	255.255.255.0	Dự phòng (cho quản lý Switch)
3	192.168.2.3	255.255.255.0	Modem ADSL ERP
4	192.168.2.4	255.255.255.0	Modem ADSL Tài Chính
5	192.168.2.5	255.255.255.0	Modem ADSL Bán Hàng
6	192.168.2.10	255.255.255.0	Địa chỉ Server Ảo

- Địa chỉ VLAN 103

Bảng 3.6. Quy hoạch địa chỉ VLAN 103

STT	Từ địa chỉ - đến địa chỉ	Subnetmask	Mục đích
1	192.168.3.10→192.168.3.60	255.255.255.0	Máy trạm
2	192.168.3.1	255.255.255.0	Gateway trên UTM

Các thông tin về địa chỉ, subnetmask, gateway, DNS server của các máy trạm sẽ do FW UTM cấp động thông qua giao thức DHCP.

Lưu ý: Đối với các máy tính kết nối máy in dùng chung, sẽ được gán IP tĩnh trên card mạng. Địa chỉ này là các địa chỉ đầu tiên sau địa chỉ FW UTM trong dải địa chỉ của mỗi Vlan. Nhận giá trị từ 192.168.x.2 đến 192.168.x.9

- Địa chỉ zone DMZ: Địa chỉ IP sử dụng cho kết nối máy chủ Tài Chính thuộc chi nhánh.

Bảng 3.7. Quy hoạch địa chỉ Zone DMZ

STT	Địa chỉ IP	Subnetmask	Mục đích
1	192.168.4.1	255.255.255.0	Gateway trên UTM
2	192.168.4.2	255.255.255.0	Máy chủ Tài Chính

- Địa chỉ zone Untrust: Địa chỉ IP sử dụng cho kết nối LAN của modem ADSL VTOffice chi nhánh.

Bảng 3.8. Quy hoạch địa chỉ Zone Untrust

STT	Địa chỉ IP	Subnetmask	Mục đích
1	192.168.5.1	255.255.255.0	Gateway trên UTM
2	192.168.5.2	255.255.255.0	Modem ADSL VTOffice

- Địa chỉ zone WiFi: Địa chỉ IP sử dụng cho kết nối thiết bị WiFi tại chi nhánh.

Bảng 3.9. Quy hoạch địa chỉ Zone WiFi

STT	Địa chỉ IP	Subnetmask	Mục đích
1	192.168.6.1	255.255.255.0	Gateway trên UTM
2	192.168.6.10→192.168.6.60	255.255.255.0	Thiết bị WiFi, máy trạm

Ghi chú: Thiết bị WiFi phải được áp dụng các cơ chế đảm bảo an ninh bảo mật.

3.2.3. Chính sách định tuyến và kiểm soát truy cập

Định tuyến và kiểm soát truy nhập trên Modem ADSL

- Trên Modem sử dụng cơ chế NAT các địa chỉ trong mạng LAN ra địa chỉ WAN để trao đổi thông tin với trung tâm.
- Trên Modem ADSL khởi tạo kết nối PPPoE, mặc định có default route trả về BRAS, nên không cần cấu hình định tuyến.
- Enable Firewall trên tất cả các Modem ADSL, không cho phép mở kết nối telnet, http từ giao diện WAN.
- Trên Modem ADSL ERP thực hiện dịch port (port forwarding) cho phép thực hiện quản lý FW UTM: Telnet, SSH, HTTPS.
- Trên Modem ADSL Tài chính thực hiện mở các cổng (forward port) cho phép thực hiện quản lý máy chủ tài chính (Remote Desktop) và truy vấn SQL.

Định tuyến và kiểm soát truy cập trên FW UTM

- Định tuyến

Định tuyến trên FW UTM được kết hợp với các policy nhằm thực thi các chính sách trao đổi thông tin, các cơ chế lọc gói tin và hạn chế truy cập giữa các vùng.

Định tuyến kết nối với trung tâm qua Modem ADSL

Bảng 3.10. Các lớp mạng định tuyến trên Firewall

STT	Lớp mạng/subnet	Next-hop/Thiết bị	Mục đích
1	0.0.0.0/0	192.168.5.2	Truy cập Internet
2	10.2.0.0/27	192.168.2.3	Truy cập ERP
3	10.2.0.1/32	192.168.2.4	Truy cập máy chủ TC
4	192.168.176.0/24 192.168.131.0/24	192.168.2.5	Truy cập mạng Bán hàng

- Chính sách kiểm soát truy nhập, trao đổi thông tin giữa các vùng (zone)
 - Chính sách chung: Các máy trạm, thiết bị trong nội bộ zone được phép trao đổi thông tin với nhau. Các máy trạm thiết bị trong zone được phép thực hiện ping (gửi

gói tin ICMP) tới gateway của zone đó và ra ngoài Internet. Trên UTM mặc định là chặn toàn bộ các lưu lượng giữa các zone, chỉ thực hiện mở các cổng, ứng dụng phù hợp.

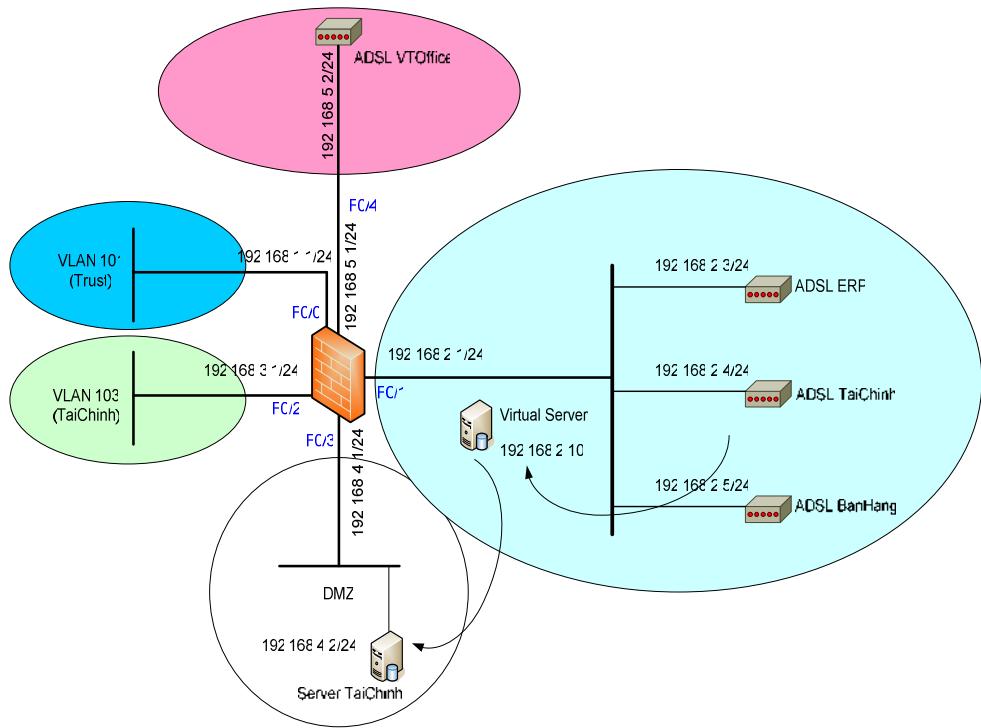
- Chính sách với từng zone:

Bảng 3.11. Các policy thiết lập trên Firewall

To From	Địa chỉ nguồn	Địa chỉ đích	Giao thức	Ghi chú
Trust	To UnTrust			
	192.168.1.0/24	0.0.0.0/0	- Chặn Email ngoài, chat - Permit Any	Truy nhập Internet, chặn Email ngoài, chat client
	To ERP			
	192.168.1.0/24	10.2.0.0/27	Any	Truy nhập Ứng dụng ERP
TaiChinh	192.168.2.0/24	Any		Quản lý Modem
	To UnTrust			
	192.168.3.0/24	0.0.0.0/0	- Chặn Email ngoài, chat - Permit Any	Truy nhập Internet, chặn email ngoài, chat client
	To ERP			
	192.168.3.0/24	10.2.0.0/27	Any	Truy nhập Ứng dụng ERP
DMZ	To DMZ			
	192.168.3.0/24	192.168.4.2/32	SQL(1433) Terminal Service (3389)	Trao đổi với máy chủ Tài chính chi nhánh
	To TaiChinh			
	192.168.4.2/32	192.168.3.0/24	SQL(1433)	Trao đổi với zone Tài chính
ERP	To ERP			
	192.168.4.2/32	10.2.0.1/32	SQL(1433) Terminal Service (3389)	Trao đổi với máy chủ Tài chính TCT
	10.2.0.1/32	192.168.4.2/24	SQL, Terminal Service	Trao đổi với máy chủ Tài chính TCT
Chú ý: Việc quản lý Firewall từ xa được thực hiện từ Zone ERP				

Cơ chế NAT địa chỉ IP

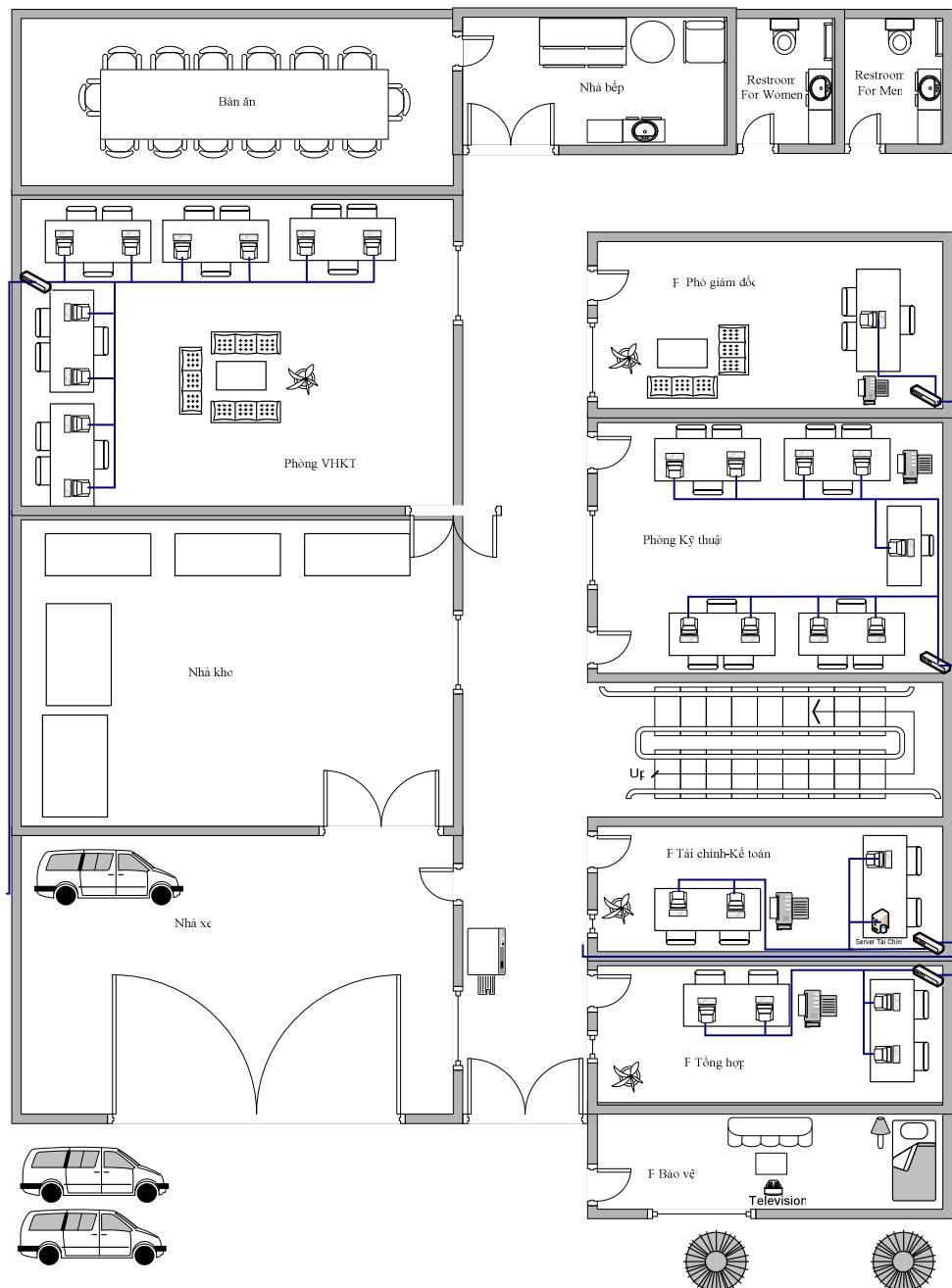
- Như chúng ta đã biết, trong quá trình trao đổi dữ liệu, khi gói tin đi từ trong mạng LAN ra bên ngoài thông qua Modem, địa chỉ IP nguồn của gói tin bị NAT sang địa chỉ WAN của modem.
- Để modem thực hiện việc NAT địa chỉ thì một yêu cầu đặt ra nữa là: Gói tin được NAT địa chỉ đó phải có địa chỉ nguồn thuộc cùng mạng với địa chỉ LAN của Modem.
- Trong khi đó, trong mạng LAN của chúng ta sử dụng rất nhiều lớp mạng khác nhau, được phân tách bởi thiết bị Firewall. Như vậy một vấn đề đặt ra là, Firewall phải thực hiện việc NAT các địa chỉ IP của gói tin nếu gói tin đó muốn gửi tới và đi qua modem.
- Đối với các máy tính trong mạng LAN:
 - Các gói tin khi đi từ máy tính trong VLAN 101 và VLAN 103 ra hướng VLAN 102 (hướng tới các modem ERP) sẽ được NAT địa chỉ IP nguồn thành địa chỉ IP của giao diện Firewall kết nối với VLAN 102.
 - Các gói tin khi đi từ máy tính trong VLAN 101 và VLAN 103 ra hướng VLAN 105 (hướng tới modem Internet) sẽ được NAT địa chỉ IP nguồn thành địa chỉ IP của giao diện Firewall kết nối với VLAN 105.
- Đối với Server Tài chính:
 - Server Tài chính đặt trong vùng DMZ, trên UTM SSG phải triển khai cơ chế NAT 1-1 từ địa chỉ Server TaiChinh (192.168.4.2) trong vùng DMZ ra địa chỉ ảo (VirtualIP) ngoài giao diện ERP, khi đó các máy tại trung tâm (TCT) mới kết nối được với Server trong DMZ nhờ cơ chế Virtual server trên Modem trỏ vào địa chỉ VirtualIP.



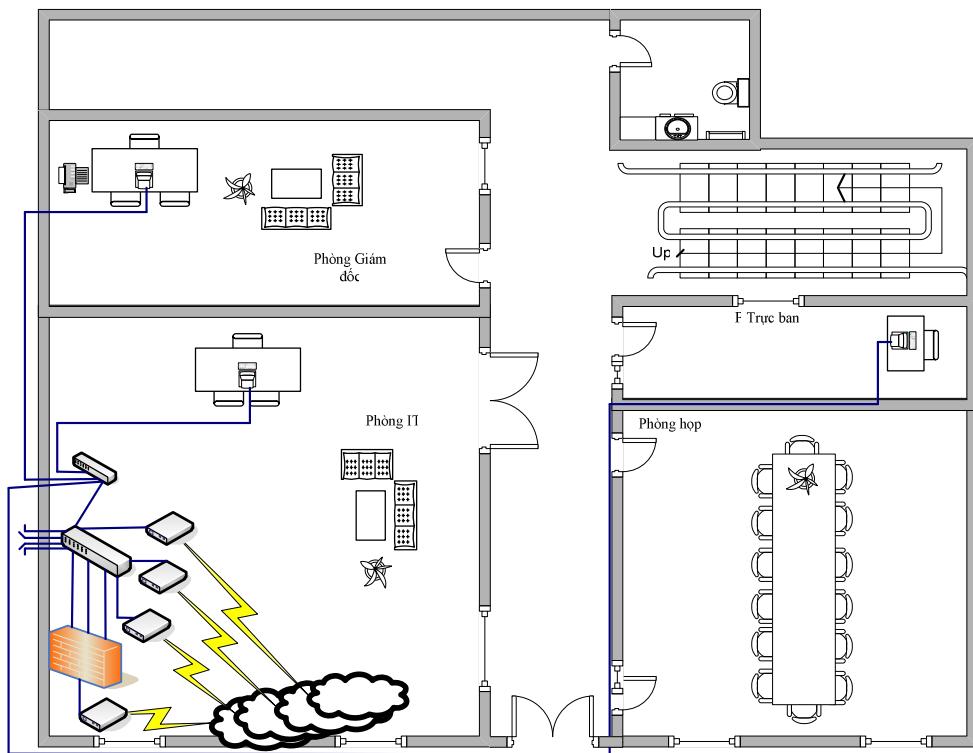
Hình 2.45. Tô chúc các Zone của Firewall và máy chủ tài chính

- Khai báo cơ chế MIP trên giao diện ERP, địa chỉ ảo là VirtualIP cùng subnet với ERP (192.168.2.10)
- Trong policy hướng từ DMZ ra ERP tiến hành NAT địa chỉ nguồn bình thường.
- Trong policy hướng từ zone ERP vào zone DMZ chọn địa chỉ đích là VirtualIP (192.168.2.10) trong MIP khai báo ở trên.

3.2.4. Sơ đồ mạng ở mức vật lý



Hình 2.46. Sơ đồ mạng ở mức vật lý - tầng 1



Hình 2.47. Sơ đồ mạng ở mức vật lý - tầng 2

IV. Cài đặt mạng

Bảng 4.1. Các bước triển khai

STT	Nội dung công việc	Đơn vị thực hiện	Ghi chú
1	Tổ chức đào tạo, các đơn vị nhận tài liệu, tổ chức học tập, nghiên cứu, thảo luận và kiểm tra	Ban UDCNTT, các chi nhánh	
2	Các đơn vị triển khai hệ thống mạng cáp	Các chi nhánh	
2.1	Rà soát các kết nối, thiết bị mạng Hub, Switch hiện tại.		
2.2	Bổ sung hệ thống mạng cáp, thiết bị kết nối Hub, switch kết nối các máy tính trong các phòng ban.		
2.3	Tập trung các kết nối từ phòng ban về điểm tập trung		
3	Cấu hình thiết bị Switch layer 2, Firewall tập trung, chuyển cho các đơn vị.	Ban UDCNTT	
4	Tiếp nhận, lắp đặt thiết bị Switch layer 2, Firewall	Các chi nhánh	
4.1	Cấu hình modem ADSL: Vietteloffice, ERP, Tài chính, bán hàng theo các thông số cấu hình trong tài liệu đã quy hoạch.		

4.2	Kết nối cáp từ các phòng ban vào đúng các cổng đã được quy định.		
4.3	Bật nguồn thiết bị Switch, Firewall.		
4.4	Kiểm tra kết nối giữa Firewall với hệ thống quản trị tập trung NSM tại TCT.		
4.5	Kiểm tra kết nối Internet, ERP, mạng tài chính, mạng bán hàng, kết nối giữa phòng tài chính với máy chủ tài chính, kiểm tra kết nối máy chủ tài chính tại đơn vị với máy chủ tài chính TCT.		
4.6	Đánh nhãn hệ thống cáp mạng.		
4.7	Lập hồ sơ mạng: Backup cấu hình thiết bị, vẽ sơ đồ vật lý, sơ đồ logic.		
4.8	Báo cáo kết quả thực hiện		
5	Xử lý các sự cố mạng.	Ban UDCNTT, Các chi nhánh	

V. 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.

Kiểm tra các kết nối từ chi nhánh về TCT.

Kiểm tra các Rule trên Firewall có đúng như thiết kế ban đầu không.

VI. Bảo trì mạng

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.

Cần theo dõi hệ thống và báo cáo kết quả về TCT.

Cần xây dựng một quy trình bảo trì mạng có tính định kỳ và thường xuyên.

Kiểm tra toàn bộ hệ thống phần cứng.

Kiểm tra các dịch vụ mạng được cài đặt và độ ổn định.

Kiểm tra và chữa trị các lỗi tiềm ẩn, các dịch vụ mạng cộng thêm.

Kiểm tra và đưa ra giải pháp nâng cấp hệ thống bảo mật thông tin khi cần thiết.

Phân quyền hệ thống theo yêu cầu và nhu cầu từ Tổng công ty.

Cấu hình lại Server và hệ thống mạng nếu cần.

Kiểm tra sự hoạt động ổn định của các trình ứng dụng.

Cấu hình máy con và chia sẻ tài nguyên trên hệ thống mạng.

Đề xuất giải pháp nâng cấp phần cứng và phần mềm.

Dọn dẹp "rác" và tối ưu hoá chương trình.

Kiểm tra và tiêu diệt virus. Cập nhật phần mềm phòng chống virus.

Backup dữ liệu.

Diệt virus, cập nhật các chương trình phòng chống và diệt virus mới nhất.

Dọn rác ổ đĩa, sắp xếp dữ liệu.

Cài đặt các phần mềm văn phòng ứng dụng.

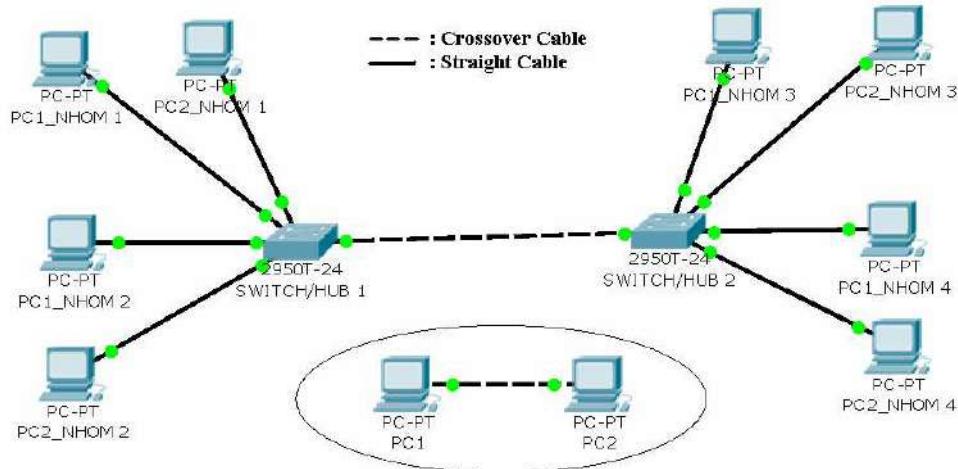
Vệ sinh công nghiệp máy tính

Bài 2. Thiết kế một Mạng LAN đơn giản

Mục tiêu:

Ôn lại một số kỹ năng thực hành cơ bản về mạng máy tính như lắp đặt và cấu hình card mạng, các loại chuẩn cáp mạng, cách bấm cáp cáp xoắn...

Cấu hình và kết nối một mạng LAN đơn giản theo mô hình cho sẵn.



Thiết bị yêu cầu:

- Kim mạng RJ-45
- Thiết bị test cáp mạng
- 20m dây cáp CAT5e, chia làm 4 đoạn, mỗi đoạn 5m
- 32 đầu nối RJ-45, mỗi nhóm 8 đầu nối
- 8 máy tính có card mạng, mỗi nhóm 2 máy tính để thực hành nối trực tiếp 2 máy
- 2 hub/switch

Khảo sát các loại Card mạng và các cổng giao tiếp mà nó hỗ trợ.

Lắp Card mạng và cài đặt driver.

Kiểm tra card mạng xem đã hoạt động được chưa, ghi nhận nhà sản xuất card mạng và tốc độ kết nối tối đa mà nó hỗ trợ.

Khảo sát cáp mạng CAT5, phân biệt màu sắc của các dây trong nó.
Khảo sát đầu cáp RJ-45 của cáp CAT5.

Dùng kìm mạng thực hiện một đoạn cáp **Crossover Cable** (cáp chéo) để đấu nối trực tiếp 2 PC.

Dùng đoạn cáp trên để nối trực tiếp 2 PC thông qua card mạng của chúng. Sau đó cấu hình địa chỉ IP tĩnh của 2 PC theo lớp C sao cho

chúng có thể trao đổi thông tin được cho nhau. (Dùng lệnh ipconfig, ping, net view... để kiểm tra, sau đó thử chia sẻ các tập tin hay thư mục để dùng chung trong Win).

Khảo sát hub/switch, nhận biết các port và tốc độ tối đa mà chúng hỗ trợ.

Dùng kìm mạng thực hiện một đoạn cáp **Straight Cable** (cáp thẳng) để đấu nối một PC đến hub/switch.

Nối 3-4 PC vào một hub/switch. Cấu hình địa chỉ IP tĩnh cho từng PC để chúng có thể liên lạc được với nhau.

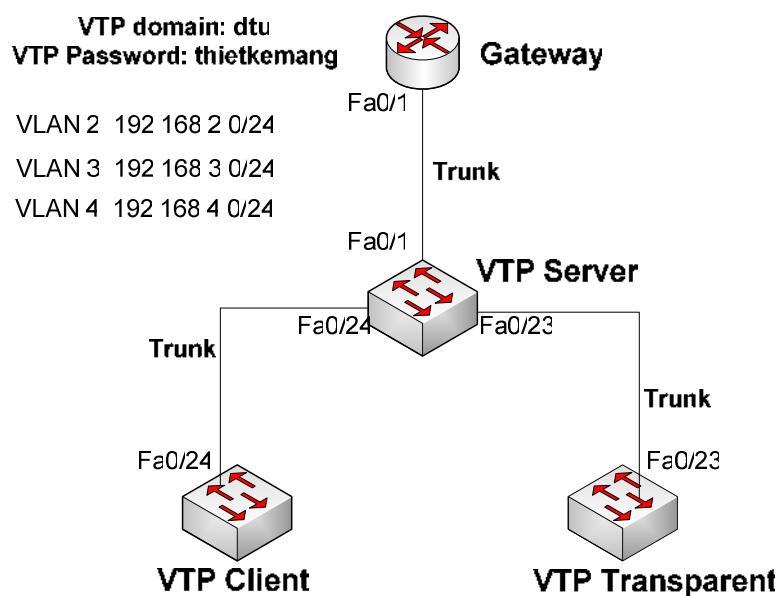
Bài 3.

Mục tiêu:

Rèn luyện kỹ năng thiết kế mô phỏng hệ thống mạng trên phần mềm Packet tracer.

Thiết kế các hệ thống LAN, VLAN cơ bản trên Packet tracer

Yêu cầu: Thiết kế mạng LAN theo mô hình bên dưới bằng Packet tracer



Bước 1: Xóa thông tin VLAN và VTP trên các Switch

```

Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#reload
Proceed with reload? [confirm]
System configuration has been modified. Save? [yes/no]: n

```

Bước 2: Cấu hình mật khẩu cho cổng Console, line vty , mode privilege

```

SW1>enable
SW1#config terminal
SW1(config)#enable secret thietkemang2
SW1(config)#line console 0
SW1(config-line)#password thietkemang3
SW1(config)#line vty 0 15
SW1(config-line)#password thietkemang4
SW1(config-line)#login

```

Lặp lại bước 2 cho các switch còn lại và router

Bước 3: Cấu hình VTP trên 3 Switch

Các Switch Cisco có cấu hình VTP mặc định là:

- VTP domain name: None
- VTP mode: Server mode
- VTP pruning: Enabled or disabled (model specific)
- VTP password: Null
- VTP version: Version 1

SW1:

```

Switch>enable
Switch#config terminal
Switch(config)#hostname SW1
Switch(config)#exit

```

Xem thông tin VTP trên SW1 trước khi cấu hình bằng lệnh show vtp status

```

SW1#show vtp status
VTP Version : 2
Configuration Revision : 0

```

```

Maximum VLANs supported locally : 250
Number of existing VLANs      : 5
VTP Operating Mode           : Server
VTP Domain Name               :
VTP Pruning Mode             : Disabled
VTP V2 Mode                   : Disabled
VTP Traps Generation         : Disabled
MD5 digest                  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
=====
```

```

SW1(config)#vtp version 2
SW1(config)#vtp domain dtu
Changing VTP domain name from NULL to dtu
SW1(config)#vtp password thietkemang
Setting device VLAN database password to thietkemang
SW1(config)#vtp mode server
Device mode already VTP SERVER.
=====
```

```

Thông tin VTP trên SW1 sau khi cấu hình
SW1#show vtp status
VTP Version
Configuration Revision       : 1
Maximum VLANs supported locally : 250
Number of existing VLANs      : 5
VTP Operating Mode           : Server
VTP Domain Name               : dtu
VTP Pruning Mode             : Disabled
VTP V2 Mode                   : Enabled
VTP Traps Generation         : Disabled
MD5 digest                  : 0x14 0x8E 0xDA 0xC9 0x0A 0x42 0xAF 0xE7
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:26
Local updater ID is 0.0.0.0 (no valid interface found)
SW1#show vtp password
VTP Password: thietkemang
SW2:
Switch>enable
Switch#config terminal
Switch(config)#hostname SW2
```

```
SW2(config)#vtp version 2
SW2(config)#vtp domain dtu
Changing VTP domain name from NULL to dtu
SW2(config)#vtp password thietkemang
Setting device VLAN database password to thietkemang
SW2(config)#vtp mode client
Setting device to VTP CLIENT mode.
Kiểm tra lại thông tin VTP trên SW2
SW2#show vtp status
VTP Version : 2
Configuration Revision : 1
Maximum VLANs supported locally : 250
Number of existing VLANs : 5
VTP Operating Mode : Client
VTP Domain Name : dtu
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0x14 0x8E 0xDA 0xC9 0x0A 0x42 0xAF 0xE7
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:26
SW2#show vtp password
VTP Password: thietkemang
SW3:
Switch>enable
Switch#config terminal
Switch(config)#hostname SW3
SW3(config)#vtp version 2
SW3(config)#vtp domain dtu
Changing VTP domain name from NULL to dtu
SW3(config)#vtp password thietkemang
Setting device VLAN database password to thietkemang
SW3(config)#vtp mode transparent
Device mode already VTP TRANSPARENT.
SW3#show vtp status
```

Bước 4: Cấu hình Trunking cho 3 switch SW1,SW2,SW3 và Router

Chú ý: Đối với Switch layer 3 do hỗ trợ cả 2 chuẩn 802.1Q và ISL nên trước khi cấu hình Trunking cần thêm lệnh switchport trunk encapsulation dot1q ở mode interface, Switch layer 2 thì chỉ hỗ trợ 802.1Q nên không cần nhập lệnh trên.

```
SW1:  
SW1(config)#interface fa0/1  
SW1(config-if)#switchport trunk encapsulation dot1q #chỉ dùng cho layer3 Switch#  
SW1(config-if)#switchport mode trunk  
SW1(config-if)#switchport nonegotiate #vô hiệu hóa chức năng DTP #  
SW1(config-if)#no shutdown  
SW1(config-if)#exit  
SW1(config)#interface fa0/24  
SW1(config-if)#switchport trunk encapsulation dot1q # chỉ dùng cho layer3 Switch#  
SW1(config-if)#switchport mode trunk  
SW1(config-if)#switchport nonegotiate  
SW1(config-if)#no shutdown  
SW1(config-if)#exit  
SW1(config)#interface fa0/23  
SW1(config-if)#switchport trunk encapsulation dot1q # chỉ dùng cho layer3 Switch#  
SW1(config-if)#switchport mode trunk  
SW1(config-if)#switchport nonegotiate  
SW1(config-if)#no shutdown  
SW2:  
SW2(config)#interface fa0/22  
SW2(config-if)# switchport trunk encapsulation dot1q #chi dung cho layer3 Switch#  
SW2(config-if)#switchport mode trunk  
SW2(config-if)#switchport nonegotiate  
SW2(config-if)#no shutdown  
SW3:  
SW3(config)#interface fa0/23  
SW3(config-if)# switchport trunk encapsulation dot1q #chi dung cho SW layer3 Switch#  
SW3(config-if)#switchport mode trunk  
SW3(config-if)#switchport nonegotiate  
SW3(config-if)#no shutdown  
Router:  
Router#config terminal  
Router(config)#interface fa0/1  
Router(config-if)#description Gateway cho VLAN1  
Router(config-if)#ip address 192.168.1.1 255.255.255.0  
Router(config-if)#no shutdown  
Router(config-if)#exit  
Router(config)#interface fa0/1.2  
Router(config-subif)#description Gateway cho VLAN2  
Router(config-subif)#encapsulation dot1Q 2
```

```
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface fa0/1.3
Router(config-subif)#description Gateway cho VLAN3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface fa0/1.4
Router(config-subif)#description Gateway cho VLAN4
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/1    192.168.1.1    YES  manual up       up
FastEthernet0/1.2   192.168.2.1    YES  manual up       up
FastEthernet0/1.3   192.168.3.1    YES  manual up       up
FastEthernet0/1.4   192.168.4.1    YES  manual up       up
FastEthernet0/1     unassigned     YES administratively down down
Serial0/1/0         unassigned     YES administratively down down
Serial0/1/1         unassigned     YES administratively down down
```

Bước 5: Tạo VLAN trên VTP server ở SW1

Kiểm tra thông tin VLAN hiện tại trên SW1

SW1#show vlan

Tiến hành tạo VLAN

```
SW1(config)#vlan 2
SW1(config-vlan)#name CNTT
SW1(config-vlan)#exit
SW1(config)#vlan 3
SW1(config-vlan)#name KeToan
SW1(config-vlan)#exit
SW1(config)#vlan 4
SW1(config-vlan)#name TaiChinh
SW1(config-vlan)#exit
```

Kiểm tra lại thông tin trên SW1,SW2,SW3 sau khi cấu hình để đảm bảo thông tin VLAN và VTP được đồng bộ

SW1#show vlan

SW1#show vtp status

SW2#show vlan

```
SW2#show vtp status
SW3#show vlan
SW3#show vtp status
```

Bước 6: Gán các port trên từng Switch vào VLAN tương ứng

SW1:

```
SW1(config)#interface range fa0/2 - 5
SW1(config-if-range)#switchport access vlan 2
SW1(config-if-range)#exit
SW1(config)#interface range fa0/6 - 10
SW1(config-if-range)#switchport access vlan 3
SW1(config-if-range)#exit
SW1(config)#interface range fa0/11 - 15
SW1(config-if-range)#switchport access vlan 4
SW1(config-if-range)#exit
```

Lặp lại bước 6 trên các Switch còn lại

Kiểm tra lại bằng lệnh show vlan trên cả 3 Switch

```
SW1#show vlan
```

Bước 7: Cấu hình địa chỉ IP cho các Switch để có thể quản lý từ xa

```
SW1(config)# interface VLAN 1
SW1(config-if)#ip address 192.168.1.11 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit
SW1(config)#ip default-gateway 192.168.1.1
SW1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
Vlan1              192.168.1.11   YES manual up           up

SW2(config)# interface VLAN1
SW2(config-if)#ip address 192.168.1.12 255.255.255.0
SW2(config-if)#no shutdown
SW2(config-if)#exit
SW2(config)#ip default-gateway 192.168.1.1
SW2#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
Vlan1              192.168.1.12   YES manual up           up

SW3(config)# interface VLAN1
SW3(config-if)#ip address 192.168.1.13 255.255.255.0
SW3(config-if)#no shutdown
SW3(config-if)#exit
```

```

SW3(config)#ip default-gateway 192.168.1.1
SW3#show ip interface brief
Interface          IP-Address   OK? Method Status      Protocol
Vlan1              192.168.1.13 YES manual up           up
Từ các Switch thử ping đến router
SW1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1000 ms
SW1#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1000 ms
SW1#
Sau đó từ router thử telnet đến các Switch
Router#telnet 192.168.1.11
Trying 192.168.1.11 ... Open
User Access Verification
Password:
SW1>enable
Password:
SW1#

```

Bước 8: Kiểm tra lại sự định tuyến giữa các VLAN

Kiểm tra thông mạng giữa các PC khác VLAN

Bài 4. Vẽ sơ đồ mạng

Mục tiêu:

Làm quen với một số phần mềm vẽ sơ đồ mạng.

Rèn luyện kỹ năng vẽ thiết kế các sơ đồ mạng mức logic và vật lý.

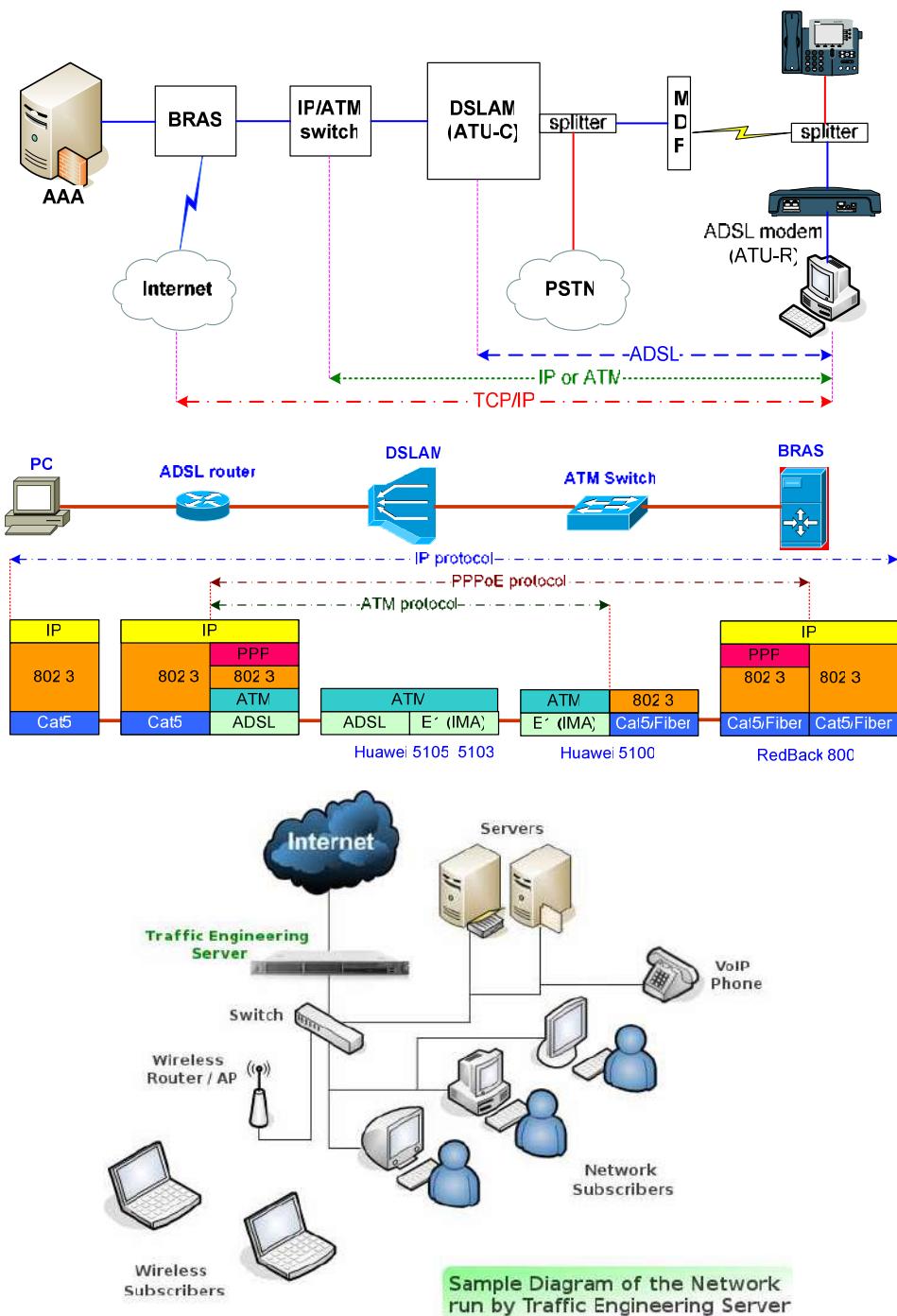
Làm quen với một số sơ đồ mạng.

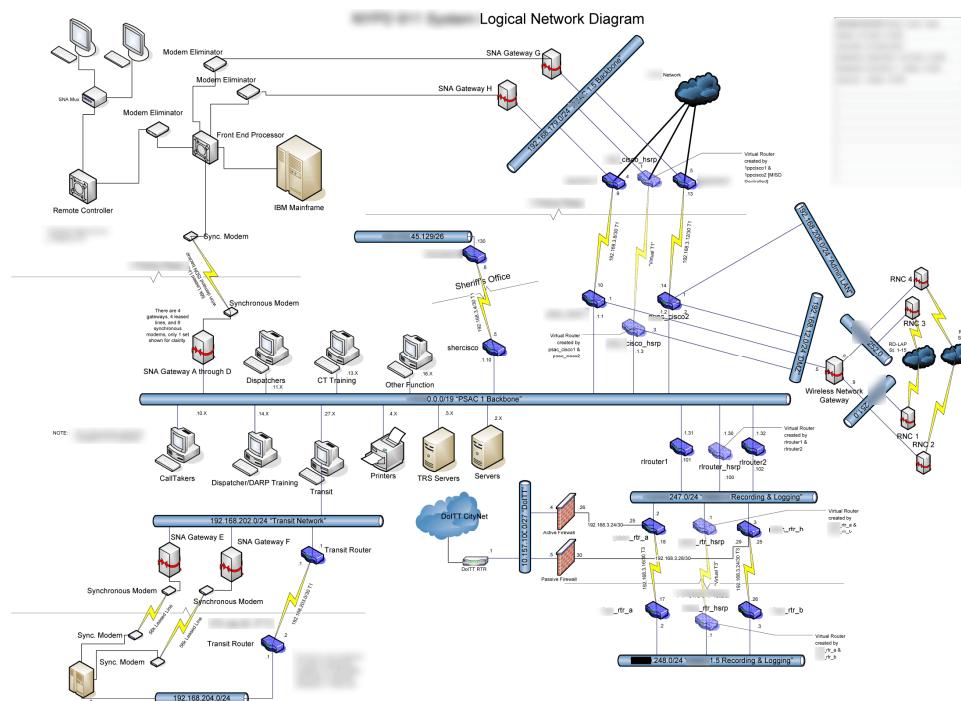
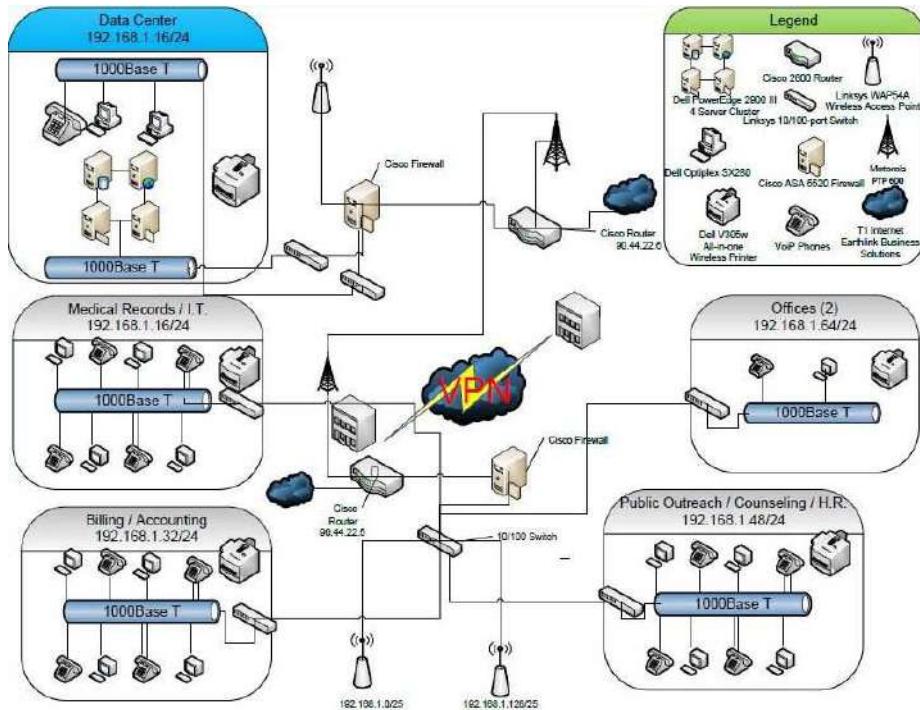
Yêu cầu: Sử dụng một trong các phần mềm sau để vẽ các sơ đồ mạng cho sau đây:

Microsoft Office Visio 2003/2007

EDraw Network Diagrammer 3

Edraw Max 4







2.12. CÂU HỎI ÔN TẬP

Câu 1: Tại sao lại phải tối ưu hệ thống mạng của chúng ta?

Câu 2: Tại sao việc kiểm tra hệ thống là quan trọng?

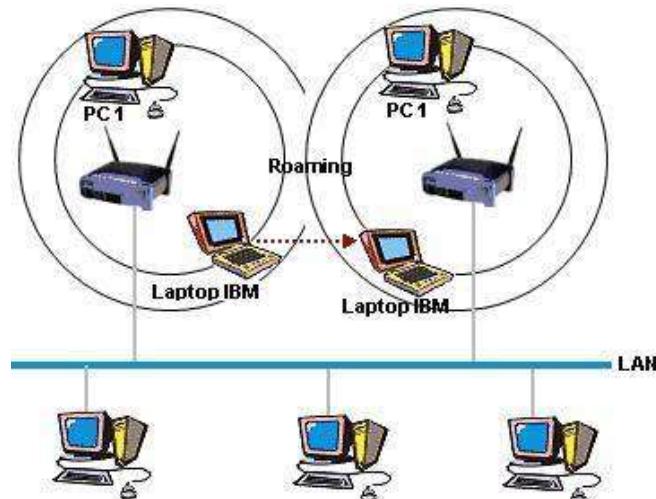
Câu 3: Tại sao nói việc lập tài liệu trong thiết kế mạng là quan trọng?

Câu 4: Các nội dung chính trong tài liệu thiết kế mạng là gì?

Câu 5: Vấn đề thiết kế địa chỉ IP trong mạng có quan trọng không? Tại sao?

Chương 3

MẠNG CỤC BỘ KHÔNG DÂY



Chương này giới thiệu các kiến thức cơ bản về công nghệ mạng cục bộ không dây, bao gồm các chuẩn mạng WLAN, các thiết bị mạng WLAN và mô hình mạng WLAN thông dụng. Đồng thời, giới thiệu phương pháp thiết kế và lắp đặt mạng WLAN. Cuối chương là bài tập ứng dụng thiết kế mạng WLAN trên thực tế và trên phần mềm mô phỏng.

3.1. TỔNG QUAN VỀ WLAN

3.1.1 Lịch sử hình thành và phát triển

Mạng LAN không dây viết tắt là WLAN (Wireless Local Area Network), là một mạng dùng để kết nối hai hay nhiều máy tính với nhau mà không sử dụng dây dẫn. WLAN dùng công nghệ trai phổ, sử dụng sóng vô tuyến cho phép truyền thông giữa các thiết bị trong một vùng nào đó còn được gọi là Basic Service Set. Nó giúp cho người sử dụng có thể di chuyển trong một vùng bao phủ rộng mà vẫn kết nối được với mạng.

Công nghệ WLAN lần đầu tiên xuất hiện vào cuối năm 1990, khi những nhà sản xuất giới thiệu những sản phẩm hoạt động trong băng tần 900MHz. Những giải pháp này (không được thống nhất giữa các nhà sản xuất) cung cấp tốc độ truyền dữ liệu 1Mbit/s, thấp hơn nhiều so với tốc độ 10Mbit/s của hầu hết các mạng sử dụng cáp hiện thời.

Năm 1992, những nhà sản xuất bắt đầu bán những sản phẩm WLAN sử dụng băng tần 2.4GHz. Mặc dù những sản phẩm này đã có tốc độ truyền dữ liệu cao hơn nhưng chúng vẫn là những giải pháp riêng của mỗi nhà sản xuất không được công bố rộng rãi. Sự cần thiết cho việc hoạt động thống nhất giữa các thiết bị ở những dãy tần số khác nhau dẫn đến một tổ chức bắt đầu phát triển ra những chuẩn mạng không dây chung.

Năm 1997, Institute of Electrical and Electronics Engineers (IEEE) đã phê chuẩn sự ra đời của chuẩn 802.11, và cũng được biết với tên gọi WI-FI (Wireless Fidelity) cho các mạng WLAN. Chuẩn 802.11 hỗ trợ ba phương pháp truyền tín hiệu, trong đó có bao gồm phương pháp truyền tín hiệu vô tuyến ở tần số 2.4GHz.

Năm 1999, IEEE thông qua hai sự bổ sung cho chuẩn 802.11 là các chuẩn 802.11a và 802.11b (định nghĩa ra những phương pháp truyền tín hiệu). Và những thiết bị WLAN dựa trên chuẩn 802.11b đã nhanh chóng trở thành công nghệ không dây vượt trội. Các thiết bị WLAN 802.11b truyền phát ở tần số 2.4GHz, cung cấp tốc độ truyền dữ liệu có thể lên tới 11Mbit/s. IEEE 802.11b được tạo ra nhằm cung cấp những đặc điểm về tính hiệu dụng, thông lượng (throughput) và bảo mật để so sánh với mạng có dây.

Năm 2003, IEEE công bố thêm một sự cải tiến là chuẩn 802.11g mà có thể truyền nhận thông tin ở cả hai dãy tần 2.4GHz và 5GHz và có thể nâng tốc độ truyền dữ liệu lên đến 54Mbit/s. Thêm vào đó, những sản phẩm áp dụng 802.11g cũng có thể tương thích ngược với các thiết bị chuẩn 802.11b. Hiện nay chuẩn 802.11g đã đạt đến tốc độ 108Mbit/s-300Mbit/s.

3.1.2. Dải tần số không dây

FCC (Federal Communication Commission) là một tổ chức phi chính phủ của Mỹ, trực tiếp chịu trách nhiệm trước Quốc hội. FCC được thành lập bởi đạo luật truyền thông (Communication Act) năm 1934 và

được sát nhập vào ban điều chỉnh liên bang và truyền thông quốc tế về vô tuyến, truyền hình, dây, vệ tinh và cable. Phạm vi quyền hạn của FCC không chỉ 50 bang và quận Columbia mà toàn bộ các thuộc địa của Mỹ như Puerto Rico, Guam và Virgin Islands.

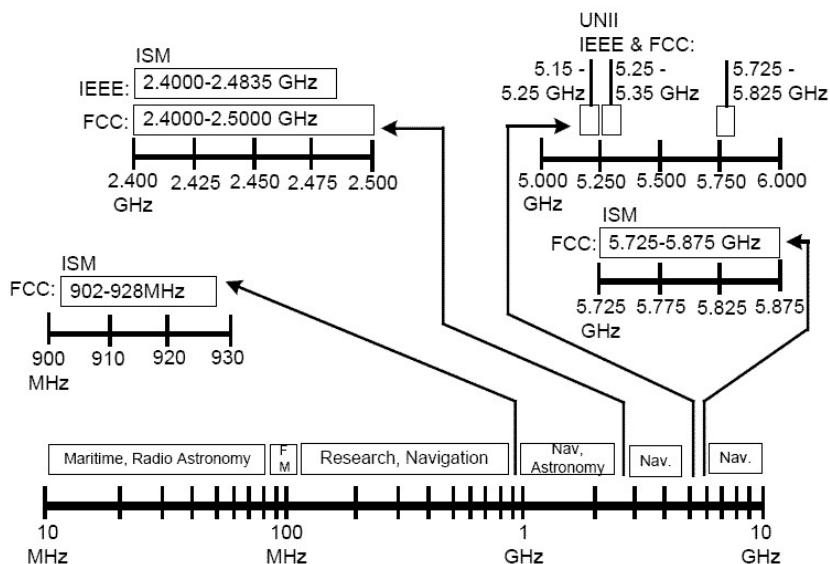
FCC tạo ra các văn bản pháp luật mà các thiết bị WLAN phải tuân thủ theo. FCC quy định phổ tần số vô tuyến mà mạng WLAN có thể hoạt động, mức công suất cho phép và các phần cứng WLAN khác nhau được sử dụng ở đâu, như thế nào.

3.1.2.1. Băng tần ISM và UNII

FCC đưa ra những quy tắc giới hạn về tần số sử dụng và công suất phát của các dãy tần số đó. FCC cũng chỉ định rằng WLAN có thể sử dụng băng tần công nghiệp, khoa học và y học (ISM = Industrial, Scientific, and Medical) chính là băng tần miễn phí. Băng tần ISM bao gồm 900 MHz, 2.4 GHz, 5.8 GHz và có độ rộng khác nhau từ 26 MHz đến 150 MHz.

Ngoài băng tần ISM, FCC cũng chỉ định 3 băng tần UNII (Unlicenced National Information Infrastructure), mỗi băng tần nằm trong vùng 5 GHz và rộng 100 MHz.

ISM and UNII Spectra



Hình 3.1. Băng tần ISM và UNII

Dưới đây là những thuận lợi và khó khăn của băng tần không cấp phép (miễn phí):

- Khi triển khai bất kỳ một hệ thống không dây nào trên băng tần miễn phí thì không cần phải xin phép FCC về băng thông và công suất cần dùng. Có giới hạn về công suất truyền, nhưng không có một thủ tục nào trong việc nhận được sự cho phép để truyền ở mức công suất đó. Hơn nữa, việc không cần giấy phép sử dụng nên không tốn thêm chi phí xin giấy phép. Đặc điểm tự nhiên của băng tần miễn phí như ISM và UNII là rất quan trọng bởi vì nó cho phép các doanh nghiệp nhỏ và hộ gia đình triển khai hệ thống không dây và làm cho thị trường WLAN ngày càng phát triển.
- Sự tự do như vậy làm cho nó có một bất lợi chính đối với người sử dụng băng tần miễn phí. Băng tần miễn phí mà bạn sử dụng cũng sẽ là băng tần miễn phí cho các người khác. Giả sử như bạn cài đặt một mạng không dây trong gia đình của bạn. Nếu như láng giềng của bạn cũng cài đặt một mạng không dây thì hệ thống của bạn và của họ có thể gây nhiễu lẫn nhau. Hơn nữa, nếu họ sử dụng một hệ thống có công suất cao thì sẽ làm cho mạng không dây của bạn không thể sử dụng được.

3.1.2.2. Băng tần Industry, Scientific and Medical (ISM)

Có 3 băng tần ISM miễn phí mà FCC chỉ định mạng WLAN có thể sử dụng gồm 900 MHz, 2.4 GHz và 5.8 GHz.

Băng tần 900 MHz ISM: được định nghĩa trong vùng tần số từ 902 MHz đến 928 MHz hay 915 MHz +- 13 MHz. Mặc dù băng tần này được phép sử dụng trong mạng WLAN nhưng mạng WLAN thường sử dụng các băng tần số cao hơn vì nó có băng thông (bandwidth) rộng hơn và throughput cao hơn. Một số các thiết bị không dây vẫn còn sử dụng băng tần 900 MHz như điện thoại gia đình không dây hay hệ thống camera không dây. Các tổ chức sử dụng mạng WLAN 900 MHz sẽ rất khó tìm ra thiết bị để thay thế vì chúng rất ít được sản xuất và giá cả rất cao.

Băng tần 2.4 GHz ISM: Băng tần này được sử dụng bởi tất cả các thiết bị tương thích chuẩn 802.11, 802.11b, 802.11g và đã trở nên rất

phổ biến. Băng tần này nằm trong khoảng từ 2.4000 GHz đến 2.5000 GHz (2.4500 GHz +- 50 MHz). Trong số 100 MHz từ 2.4000 GHz đến 2.5000 GHz thì chỉ có dãy tần số từ 2.4000 GHz đến 2.4835 GHz là thật sự được sử dụng bởi các thiết bị WLAN. Nguyên nhân chủ yếu cho sự giới hạn này là FCC về công suất phát chỉ cho vùng tần số này mà thôi.

Băng tần 5.8 GHz ISM: Băng tần này thường được gọi là 5 GHz ISM. Nó nằm trong khoảng 5.725 GHz đến 5.875 GHz (rộng 150 MHz). Băng tần này không được chỉ định để sử dụng trong mạng WLAN nên nó gây ra một số nhầm lẫn. Băng tần 5.8 GHz ISM trùng lặp với một phần của một băng tần miễn phí khác là băng tần UNII upper làm cho băng tần 5.8 Hz ISM thường bị nhầm lẫn với băng tần 5 GHz UNII upper (băng tần này được sử dụng trong WLAN).

3.1.2.3. Băng tần cơ sở hạ tầng thông tin quốc gia không được cấp phép (UNII)

Băng tần 5 GHz UNII (Unlicenced National Information Infrastructure) bao gồm 3 băng tần rộng 100 MHz riêng biệt được sử dụng trong các thiết bị tương thích chuẩn 802.11a. Ba băng tần này là lower (thấp), middle (trung) và upper (cao). Trong mỗi băng tần này có 4 kênh DSST không trùng lặp, mỗi kênh cách nhau 5 MHz. FCC quy định rằng băng tần lower được sử dụng indoor (trong nhà), băng tần middle được sử dụng indoor và outdoor (ngoài trời) và băng tần upper được sử dụng cho outdoor. Thường thì AP được để trong nhà nên băng tần 5 GHz UNII sẽ cho phép 8 AP indoor được sử dụng đồng thời (mỗi AP hoạt động ở một kênh) băng cách sử dụng cả băng tần lower và middle.

Băng tần Lower: Băng tần lower nằm trong khoảng 5.15GHz đến 5.25GHz và FCC chỉ định công suất phát lớn nhất cho băng tần này là 50 mW. Khi triển khai các thiết bị tương thích chuẩn 802.11a thì IEEE đã chỉ định rằng chỉ 40 mW (80%) của công suất phát tối đa là được sử dụng cho các thiết bị tương thích chuẩn 802.11a.

Tất nhiên bạn vẫn có thể truyền với công suất 50 mW, điều này vẫn tuân theo luật của FCC nhưng lại không tương thích với chuẩn 802.11a.

Băng tần Middle: Băng tần middle nằm trong khoảng 5.25GHz đến 5.35GHz và FCC quy định công suất phát tối đa là 250 mW. Công suất phát được quy định bởi IEEE là 200 mW. Giới hạn công suất này cho

phép thiết bị có thể hoạt động indoor hay outdoor và thường được sử dụng cho outdoor với khoảng cách ngắn giữa 2 tòa nhà gần nhau. Do có công suất phát vừa phải và sự linh hoạt trong việc sử dụng indoor/outdoor nên các sản phẩm trong băng tần middle này sẽ được chấp nhận rộng rãi trong tương lai.

Băng tần Upper: Băng tần upper được dành cho các kết nối outdoor và FCC giới hạn công suất phát là 1 W (1000 mW). Băng tần này chiếm vùng tần số giữa 5.725 GHz đến 5.825 GHz và thường bị nhầm lẫn với băng tần 5.8 GHz ISM. IEEE quy định công suất phát tối đa cho băng tần này là 800 mW, đây là mức công suất khá lớn cho hầu hết các kết nối outdoor.

3.1.3. Ưu điểm của WLAN

Sự tiện lợi: Mạng không dây cũng như hệ thống mạng thông thường. Nó cho phép người dùng truy xuất tài nguyên mạng ở bất kỳ nơi đâu trong khu vực được triển khai (nhà hay văn phòng). Với sự gia tăng số người sử dụng máy tính xách tay (laptop), đó là một điều rất thuận lợi.

Khả năng di động: Với sự phát triển của các mạng không dây công cộng, người dùng có thể truy nhập Internet ở bất cứ đâu. Chẳng hạn ở các quán Cafe, người dùng có thể truy nhập Internet không dây miễn phí.

Hiệu quả: Người dùng có thể duy trì kết nối mạng khi họ đi từ nơi này đến nơi khác.

Triển khai: Việc thiết lập hệ thống mạng không dây ban đầu chỉ cần ít nhất 1 điểm truy nhập (AP: Access Point). VỚI MẠNG DÙNG CÁP, PHẢI TỐN THÊM CHI PHÍ VÀ CÓ THỂ GẶP KHÓ KHĂN TRONG VIỆC TRIỂN KHAI HỆ THỐNG CÁP Ở NHIỀU NƠI TRONG TÒA NHÀ.

Khả năng mở rộng: Mạng không dây có thể đáp ứng tức thì khi gia tăng số lượng người dùng. VỚI HỆ THỐNG MẠNG DÙNG CÁP CẦN PHẢI GẮN THÊM CÁP.

3.1.4. Nhược điểm của WLAN

Công nghệ mạng LAN không dây, ngoài rất nhiều sự tiện lợi và những ưu điểm được đề cập ở trên thì cũng có các nhược điểm. Trong một số trường hợp mạng LAN không dây có thể không như mong muốn vì một số lý do. Hầu hết chúng phải làm việc với những giới hạn vốn có của công nghệ.

Bảo mật: Môi trường kết nối không dây là không khí nên khả năng bị tấn công của người dùng là rất cao.

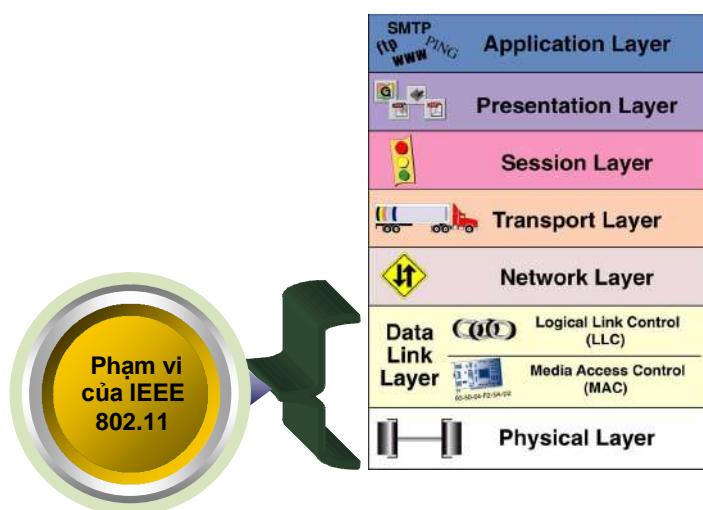
Phạm vi: Một mạng chuẩn 802.11g với các thiết bị chuẩn chỉ có thể hoạt động tốt trong phạm vi vài chục mét. Nó phù hợp trong 1 căn nhà, nhưng với một tòa nhà lớn thì không đáp ứng được nhu cầu. Để đáp ứng cần phải mua thêm Repeater hay access point, dẫn đến chi phí gia tăng.

Độ tin cậy: Vì sử dụng sóng vô tuyến để truyền thông nên việc bị nhiễu, tín hiệu bị giảm do tác động của các thiết bị khác (lò vi sóng,...) là không tránh khỏi. Làm giảm đáng kể hiệu quả hoạt động của mạng.

Tốc độ: Tốc độ của mạng không dây (1- 125 Mbit/s) rất chậm so với mạng sử dụng cáp (100 Mbit/s đến hàng Gbps).

3.2. CÁC CHUẨN THÔNG DỤNG CỦA WLAN

Hiện nay tiêu chuẩn chính cho mạng LAN không dây (WLAN: Wireless LAN) là một họ giao thức truyền tin qua mạng không dây IEEE 802.11. Do việc nghiên cứu và đưa ra ứng dụng rất gần nhau nên có một số giao thức đã thành chuẩn của thế giới, một số khác vẫn còn đang tranh cãi và một số còn đang dự thảo. Một số chuẩn thông dụng như: 802.11b (cải tiến từ 802.11), 802.11a, 802.11g, 802.11n.



Hình 3.2. Phạm vi của WLAN trong mô hình OSI

3.2.1. Chuẩn IEEE 802.11b

Chuẩn này được đưa ra vào năm 1999, nó cải tiến từ chuẩn 802.11. Cũng hoạt động ở dải tần 2,4 GHz nhưng chỉ sử dụng trai phổ trực tiếp DSSS.

Tốc độ tại Access Point có thể lên tới 11Mbit/s (802.11b), 22Mbit/s (802.11b+).

Các sản phẩm theo chuẩn 802.11b được kiểm tra và thử nghiệm bởi hiệp hội các công ty Ethernet không dây (WECA) và được biết đến như là hiệp hội Wi-Fi, những sản phẩm Wireless được WiFi kiểm tra nếu đạt thì sẽ mang nhãn hiệu này.

Hiện nay IEEE 802.11b là một chuẩn được sử dụng rộng rãi nhất cho Wireless LAN. Vì dải tần số 2,4GHz là dải tần số ISM (Industrial, Scientific and Medical: dải tần vô tuyến dành cho công nghiệp, khoa học và y học, không cần xin phép) cũng được sử dụng cho các chuẩn mạng không dây khác như là: Bluetooth và HomeRF, hai chuẩn này không được phổ biến như là 801.11. Bluetooth được thiết kế sử dụng cho thiết bị không dây mà không phải là Wireless LAN, nó được dùng cho mạng cá nhân PAN(Personal Area Network). Như vậy Wireless LAN sử dụng chuẩn 802.11b và các thiết bị Bluetooth hoạt động trong cùng một dải băng tần.

Bảng 3.1. Một số thông số kỹ thuật của chuẩn IEEE 802.11b

Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
October 1999	2.4 GHz	4.5 Mbit/s	11 Mbit/s	~35 m

3.2.2. Chuẩn IEEE 802.11a

Đây là một chuẩn được cấp phép ở dải băng tần mới. Nó hoạt động ở dải tần số 5 GHz sử dụng phương thức điều chế ghép kênh theo vùng tần số trực giao (OFDM). Phương thức điều chế này làm tăng tốc độ trên mỗi kênh (từ 11Mbit/s/1kênh lên 54 Mbit/s/1 kênh).

Có thể sử dụng đến 8 Access Point (AP) (truyền trên 8 kênh Non-overlapping; kênh không chồng lấn phổ), đặc điểm này ở dải tần 2,4GHz chỉ có thể sử dụng 3 AP (truyền trên 3 kênh non-overlapping).

Hỗ trợ đồng thời nhiều người sử dụng với tốc độ cao mà ít bị xung đột.

Các sản phẩm của theo chuẩn IEEE 802.11a không tương thích với các sản phẩm theo chuẩn IEEE 802.11 và 802.11b vì chúng hoạt động ở các dải tần số khác nhau. Tuy nhiên các nhà sản xuất chipset đang cố gắng đưa loại chipset hoạt động ở cả 2 chế độ theo hai chuẩn 802.11a và 802.11b. Sự phối hợp này được biết đến với tên WiFi5 (WiFi cho tốc độ 5Gbps).

Bảng 3.2. Một số thông số kỹ thuật của chuẩn IEEE 802.11a

Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
October 1999	5 GHz	23 Mbit/s	54 Mbit/s	~35 m

2.2.3. IEEE 802.11g

Bản dự thảo của tiêu chuẩn này được đưa ra vào tháng 10 – 2002.

Sử dụng dải tần 2,4GHz, tốc độ truyền lên đến 54Mbit/s.

Phương thức điều chế: Có thể dùng một trong 2 phương thức

- Dùng OFDM (giống với 802.11a) tốc độ truyền lên tới 54Mbit/s.
- Dùng trai phổ trực tiếp DSSS tốc độ bị giới hạn ở 11Mbit/s.

Tương thích ngược với chuẩn 802.11b.

Bị hạn chế về số kênh truyền.

Bảng 3.3. Một số thông số kỹ thuật của chuẩn IEEE 802.11g

Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
June 2003	2.4 GHz	23 Mbit/s	54 Mbit/s	~35 m

3.2.4. Chuẩn IEEE 802.11n



Hình 3.3. Logo Wi-fi

Chuẩn 802.11n đang được xúc tiến để đạt tốc độ 100 Mbit/s nhanh gấp 5 lần chuẩn 802.11g và cho phép thiết bị kết nối hoạt động với khoảng cách xa hơn các mạng Wi-Fi hiện hành.

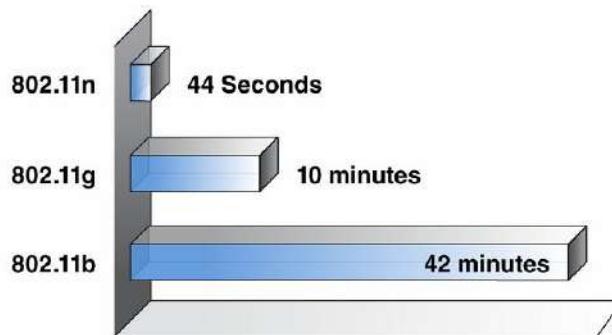
Winston Sun, giám đốc công nghệ của công ty không dây Atheros Communications, nhận xét, một thiết bị tương thích 802.11n có thể truy nhập các điểm hotspot với tốc độ 150Mbit/s với khoảng cách lý tưởng dưới 6m, khả năng liên kết càng giảm khi người dùng ở cách xa điểm truy nhập đó.

802.11n chưa thể sớm trở thành chuẩn Wi-Fi thế hệ mới vì một số mạng Wi-Fi không thuộc thông số 802.11n cũng được giới thiệu. Theo Sun, các chuẩn Wi-Fi mới được ra mắt có thể tự động dò tần sóng thích hợp để kết nối Internet. Chính vì thế, thiết bị hỗ trợ 802.11n không thể “độc chiếm” phổ Wi-Fi và phải “nhường” sóng cho các mạng kết nối khác.

Ông Sun cho biết, tốc độ truy nhập Wi-Fi giảm tỷ lệ nghịch với khoảng cách từ thiết bị tới hotspot vẫn cho phép các máy cầm tay, như iTV của Apple stream được các đoạn video clip nhưng không thể stream video nén có độ nét cao.

Bảng 3.4. Một số thông số kỹ thuật của chuẩn IEEE 802.11n

Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
June 2009 (est.)	5 GHz and/or 2.4 GHz	74 Mbit/s	300 Mbit/s (2 streams)	~70 m



Hình 3.4. Tốc độ truyền tải so với các chuẩn khác

3.2.5. So sánh các chuẩn IEEE 802.11x

Wi-Fi còn có tên gọi khác là IEEE 802.11 (hay ngắn gọn là 802.11) cũng chính là nhóm các tiêu chuẩn kỹ thuật của công nghệ kết nối này do liên minh Wi-Fi (Wi-Fi Alliance: www.wi-fi.org) quy định. Hiện tồn tại các xác thực sau được đưa ra bởi Wi-Fi Alliance:

Bảng 3.5. So sánh các chuẩn IEEE 802.11x

Chuẩn	Phân loại	Tính năng chính Định nghĩa	Chú thích
IEEE 802.11	Kết nối	Tần số: 2,4 GHz Tốc độ tối đa: 2 Mbit/s Tầm hoạt động: không xác định	Chuẩn lý thuyết
IEEE 802.11a	Kết nối	Tần số: 5 GHz Tốc độ tối đa: 54 Mbit/s Tầm hoạt động: 25-75 m	Xem thêm 802.11d và 802.11h
IEEE 802.11b	Kết nối	Tần số: 2,4 GHz Tốc độ tối đa: 11 Mbit/s Tầm hoạt động: 35-100 m	Tương thích với 802.11g
IEEE 802.11g	Kết nối	Tần số: 2,4 GHz Tốc độ tối đa: 54 Mbit/s Tầm hoạt động: 25-75 m	Tương thích ngược với 802.11b, xem thêm 802.11d và 802.11h
IEEE 802.11n	Kết nối	Tần số: 2,4 GHz Tốc độ tối đa: 540 Mbit/s Tầm hoạt động: 50-125 m	Tương thích ngược với 802.11b/g Dự kiến sẽ được thông qua vào tháng 11/2008
IEEE 802.11d	Tính năng bổ sung	Bật tính năng thay đổi tầng MAC để phù hợp với các yêu cầu ở những quốc gia khác nhau	Hỗ trợ bởi một số thiết bị 802.11a và 802.11a/g
IEEE 802.11h	Tính năng bổ sung	Chọn tần số động (dynamic frequency selection: DFS) và điều khiển truyền năng lượng (transmit power control: TPC) để hạn chế việc xung đột với các thiết bị dùng tần số 5 GHz khác	Hỗ trợ bởi một số thiết bị 802.11a và 802.11a/g

WPA Enterprise	Bảo mật	Sử dụng xác thực 802.1x với chế độ mã hóa TKIP và một máy chủ xác thực	Xem thêm WPA2 Enterprise
WPA Personal	Bảo mật	Sử dụng khóa chia sẻ với mã hóa TKIP	Xem thêm WPA2 Personal
WPA2 Enterprise	Bảo mật	Nâng cấp của WPA Enterprise với việc dùng mã hóa AES	Dựa trên 802.11i
WPA2 Personal	Bảo mật	Nâng cấp của WPA Personal với việc dùng mã hóa AES	Dựa trên 802.11i
EAP-TLS	Bảo mật	Extensible Authentication Protocol Transport Layer Security	Sử dụng cho WPA Enterprise
EAP-TTLS/MSCHA Pv2	Bảo mật	EAP-Tunneled TLS/Microsoft Challenge Authentication Handshake Protocol	Sử dụng cho WPA/WPA2 Enterprise
EAP-SIM	Bảo mật	Một phiên bản của EAP cho các dịch vụ điện thoại di động nền GSM	Sử dụng cho WPA/WPA2 Enterprise
WMM	Multimedia	Xác thực cho VoIP để quy định cách thức ưu tiên băng thông cho giọng nói hoặc video	Một thành phần của bǎn thǎo 802.11e WLAN Quality of Service

IEEE 802.11 chưa từng được ứng dụng thực tế và chỉ được xem là bước đệm để hình thành nền kỹ nguyên Wi-Fi. Trên thực tế, cả 24 kí tự theo sau 802.11 đều được lên kế hoạch sử dụng bởi Wi-Fi Alliance. Như ở bảng trên, các IEEE 802.11 được phân loại thành nhiều nhóm, trong đó hầu như người dùng chỉ biết và quan tâm đến tiêu chuẩn phân loại theo tính chất kết nối (IEEE 802.11a/b/g/n...).

Một số IEEE 802.11 ít phổ biến khác:

- IEEE 802.11c: các thủ tục quy định cách thức bắt cầu giữa các mạng Wi-Fi. Tiêu chuẩn này thường đi kèm với 802.11d.
- IEEE 802.11e: đưa QoS (Quality of Service) vào Wi-Fi, qua đó sắp đặt thứ tự ưu tiên cho các gói tin, đặc biệt quan trọng trong trường hợp băng thông bị giới hạn hoặc quá tải.

- IEEE 802.11F: giao thức truy nhập nội ở Access Point, là một mở rộng cho IEEE 802.11. Tiêu chuẩn này cho phép các Access Point có thể “nói chuyện” với nhau, từ đó đưa vào các tính năng hữu ích như cân bằng tải, mở rộng vùng phủ sóng Wi-Fi...
- IEEE 802.11h: những bổ sung cho 802.11a để quản lý dải tần 5 GHz nhằm tương thích với các yêu cầu kỹ thuật ở châu Âu.
- IEEE 802.11i: những bổ sung về bảo mật. Chỉ những thiết bị IEEE 802.11g mới nhất mới bổ sung khả năng bảo mật này. Chuẩn này trên thực tế được tách ra từ IEEE 802.11e. WPA là một trong những thành phần được mô tả trong 802.11i ở dạng bản thảo, và khi 802.11i được thông qua thì chuyển thành WPA2 (với các tính chất được mô tả ở bảng trên).
- IEEE 802.11j: những bổ sung để tương thích điều kiện kỹ thuật ở Nhật Bản.
- IEEE 802.11k: những tiêu chuẩn trong việc quản lí tài nguyên sóng radio. Chuẩn này dự kiến sẽ hoàn tất và được đệ trình thành chuẩn chính thức trong năm nay.
- IEEE 802.11p: hình thức kết nối mở rộng sử dụng trên các phương tiện giao thông (Ví dụ: sử dụng Wi-Fi trên xe buýt, xe cứu thương...). Dự kiến sẽ được phổ biến vào năm 2009.
- IEEE 802.11r: mở rộng của IEEE 802.11d, cho phép nâng cấp khả năng chuyển vùng.
- IEEE 802.11T: đây chính là tiêu chuẩn WMM như mô tả ở bảng trên.
- IEEE 802.11u: quy định cách thức tương tác với các thiết bị không tương thích 802 (chẳng hạn các mạng điện thoại di động).
- IEEE 802.11w: là nâng cấp của các tiêu chuẩn bảo mật được mô tả ở IEEE 802.11i, hiện chỉ trong giải đoạn khởi đầu.

Các chuẩn IEEE 802.11F và 802.11T được viết hoa chữ cái cuối cùng để phân biệt đây là hai chuẩn dựa trên các tài liệu độc lập, thay vì là

sự mở rộng / nâng cấp của 802.11, và do đó chúng có thể được ứng dụng vào các môi trường khác 802.11 (chẳng hạn WiMAX – 802.16).

Trong khi đó 802.11x sẽ không được dùng như một tiêu chuẩn độc lập mà sẽ bỏ trống để trở đến các chuẩn kết nối IEEE 802.11 bất kì. Nói cách khác, 802.11 có ý nghĩa là “mạng cục bộ không dây”, và 802.11x mang ý nghĩa “mạng cục bộ không dây theo hình thức kết nối nào đấy (a/b/g/n)”.

Hình thức bảo mật cơ bản nhất ở mạng Wi-Fi là WEP là một phần của bản IEEE 802.11 “gốc”.

Chúng ta có thể dễ dàng tạo một mạng Wi-Fi với lỗ lòn các thiết bị theo chuẩn IEEE 802.11b với IEEE 802.11g. Tất nhiên là tốc độ và khoảng cách hiệu dụng sẽ là của IEEE 802.11b. Một trở ngại với các mạng IEEE 802.11b/g và có lẽ là cả n là việc sử dụng tần số 2,4 GHz, vốn đã quá “chật chội” khi đó cũng là tần số hoạt động của máy bộ đàm, tai nghe và loa không dây... Tệ hơn nữa, các lò vi ba cũng sử dụng tần số này, và công suất quá lớn của chúng có thể gây ra các vấn đề về nhiễu loạn và giao thoa.

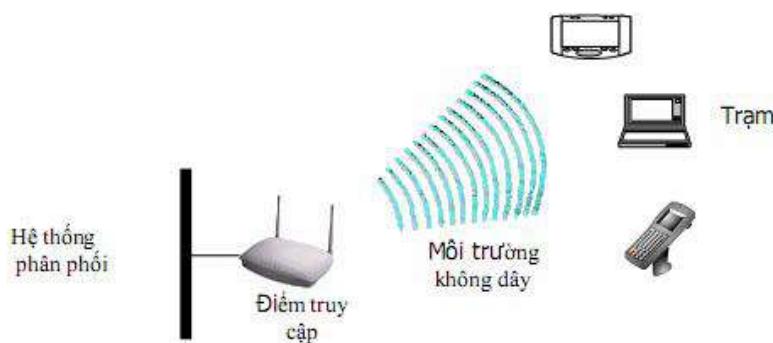
Tuy chuẩn IEEE 802.11n chưa được thông qua nhưng khá nhiều nhà sản xuất thiết bị đã dựa trên bản thảo của chuẩn này để tạo ra những cái gọi là chuẩn G+ hoặc SuperG với tốc độ thông thường là gấp đôi giới hạn của IEEE 802.11g. Các thiết bị này tương thích ngược với IEEE 802.11b/g rất tốt nhưng tất nhiên là ở mức tốc độ giới hạn. Bên cạnh đó, bạn phải dùng các thiết bị (card mạng, router, access point...) từ cùng nhà sản xuất.

Khi chuẩn IEEE 802.11n được thông qua, các nút kết nối theo chuẩn b/g vẫn được hưởng lợi khá nhiều từ khoảng cách kết nối nếu Access Point là chuẩn n.

Cần lưu ý, bất kể tốc độ kết nối Wi-Fi là bao nhiêu thì tốc độ “ra net” của bạn cũng chỉ giới hạn ở mức khoảng 2 Mbit/s (tốc độ kết nối Internet). Với môi trường Internet công cộng (quán cafe Wi-Fi, thư viện...), át hẳn lợi thế tốc độ truyền file trong mạng cục bộ xem như không tồn tại.

3.3. CẤU TRÚC VÀ CÁC MÔ HÌNH WLAN

3.3.1. Cấu trúc cơ bản của WLAN



Hình 3.5. Cấu trúc WLAN

Có 4 thành phần chính trong các loại mạng sử dụng chuẩn 802.11:

- Hệ thống phân phối (DS: Distribution System)
- Điểm truy nhập (Access Point)
- Tần liên lạc vô tuyến (Wireless Medium)
- Trạm (Station)

Hệ thống phân phối (DS):

- Thiết bị logic của 802.11 được dùng để nối các khung tới đích của chúng: Bao gồm kết nối giữa động cơ và môi trường DS (ví dụ như mạng xương sống).
- 802.11 không xác định bất kỳ công nghệ nhất định nào đối với DS.
- Hầu hết trong các ứng dụng quảng cáo, Ethernet được dùng như là môi trường DS - Trong ngôn ngữ của 802.11, xương sống Ethernet là môi trường hệ thống phân phối. Tuy nhiên, không có nghĩa nó hoàn toàn là DS.

Điểm truy nhập (Aps: Access Points)

- Chức năng chính của AP là mở rộng mạng. Nó có khả năng chuyển đổi các frame dữ liệu trong 802.11 thành các frame thông dụng để có thể sử dụng trong các mạng khác.

- APs có chức năng cầu nối giữa không dây thành có dây.

Tần liên lạc vô tuyến (Wireless Medium): Chuẩn 802.11 sử dụng tầng liên lạc vô tuyến để chuyển các frame dữ liệu giữa các máy trạm với nhau.

Trạm (Stations): Các máy trạm là các thiết bị vi tính có hỗ trợ kết nối vô tuyến như: Máy tính xách tay, PDA, Palm, Desktop ...

3.3.2. Các thiết bị hạ tầng mạng không dây

Điểm truy cập: AP (Access Point): Cung cấp cho các máy khách(client) một điểm truy nhập vào mạng "Nơi mà các máy tính dùng wireless có thể vào mạng nội bộ của công ty". AP là một thiết bị song công (Full duplex) có mức độ thông minh tương đương với một chuyển mạch Ethernet phức tạp (Switch).

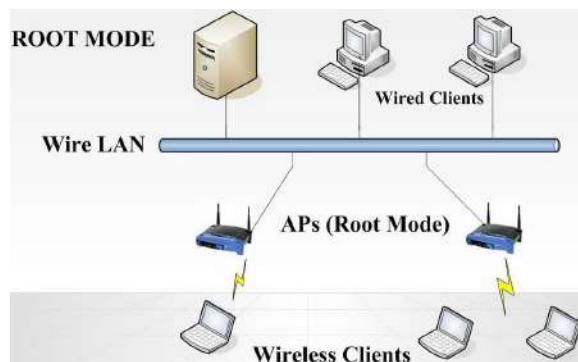


Hình 3.6. Access Points

Các chế độ hoạt động của AP: AP có thể giao tiếp với các máy không dây, với mạng có dây truyền thống và với các AP khác. Có 3 Mode hoạt động chính của AP:

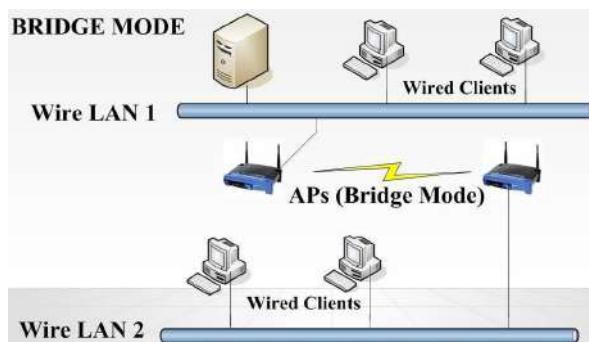
Chế độ gốc (Root mode): Root mode được sử dụng khi AP được kết nối với mạng backbone có dây thông qua giao diện có dây (thường là Ethernet) của nó. Hầu hết các AP sẽ hỗ trợ các mode khác ngoài root mode, tuy nhiên root mode là cấu hình mặc định. Khi một AP được kết nối với phân đoạn có dây thông qua cổng Ethernet của nó, nó sẽ được cấu hình để hoạt động trong root mode. Khi ở trong root mode, các AP được kết nối với cùng một hệ thống phân phối có dây có thể nói chuyện

được với nhau thông qua phân đoạn có dây. Các client không dây có thể giao tiếp với các client không dây khác nằm trong những cell (ô tế bào, hay vùng phủ sóng của AP) khác nhau thông qua AP tương ứng mà chúng kết nối vào, sau đó các AP này sẽ giao tiếp với nhau thông qua phân đoạn có dây, như ví dụ trong hình 3.7



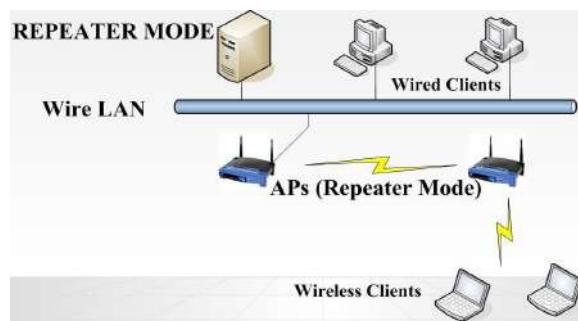
Hình 3.7. ROOT MODE

Chế độ cầu nối (bridge Mode): Trong Bridge mode, AP hoạt động hoàn toàn giống với một cầu nối không dây. AP sẽ trở thành một cầu nối không dây khi được cấu hình theo cách này. Chỉ một số ít các AP trên thị trường có hỗ trợ chức năng Bridge, điều này sẽ làm cho thiết bị có giá cao hơn đáng kể. Chúng ta sẽ giải thích một cách ngắn gọn cầu nối không dây hoạt động như thế nào, từ hình 3.7 Client không kết nối với cầu nối, nhưng thay vào đó, cầu nối được sử dụng để kết nối 2 hoặc nhiều đoạn mạng có dây lại với nhau bằng kết nối không dây.



Hình 3.8. BRIDGE MODE

Chế độ lặp(repeater mode): AP có khả năng cung cấp một đường kết nối không dây upstream vào mạng có dây thay vì một kết nối có dây bình thường. Một AP hoạt động như là một root AP và AP còn lại hoạt động như là một Repeater không dây. AP trong repeater mode kết nối với các client như là một AP và kết nối với upstream AP như là một client.



Hình 3.9. REPEATER MODE

Các thiết bị máy khách trong WLAN: Là những thiết bị WLAN được các máy khách sử dụng để kết nối vào WLAN.

3.3.2.1. Card PCI Wireless

Là thành phần phổ biến nhất trong WLAN. Dùng để kết nối các máy khách vào hệ thống mạng không dây. Được cắm vào khe PCI trên máy tính. Loại này được sử dụng phổ biến cho các máy tính để bàn (desktop) kết nối vào mạng không dây.



Hình 3.10. Card PCI Wireless

3.3.2.2. Card PCMCIA Wireless

Trước đây được sử dụng trong các máy tính xách tay (laptop) và các thiết bị hỗ trợ cá nhân số PDA (Personal Digital Association). Hiện nay

nhờ sự phát triển của công nghệ nên PCMCIA wireless ít được sử dụng vì máy tính xách tay và PDA,... đều được tích hợp sẵn Card Wireless bên trong thiết bị.



Hình 3.11. Card PCMCIA Wireless

3.3.2.3. Card USB Wireless

Loại rất được ưu chuộng hiện nay dành cho các thiết bị kết nối vào mạng không dây vì tính năng di động và nhỏ gọn. Có chức năng tương tự như Card PCI Wireless, nhưng hỗ trợ chuẩn cắm là USB (Universal Serial Bus). Có thể tháo lắp nhanh chóng (không cần phải cắm cố định như Card PCI Wireless) và hỗ trợ cắm khi máy tính đang hoạt động.



Hình 3.12. Card USB Wireless

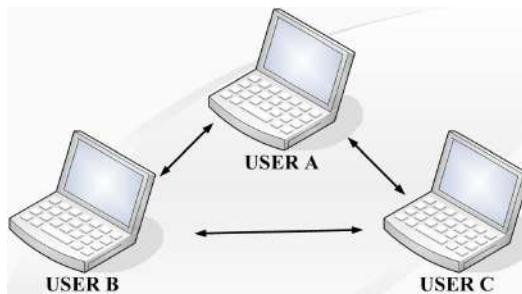
3.3.3. Các mô hình WLAN

Mạng 802.11 linh hoạt về thiết kế, gồm 3 mô hình mạng sau:

- Mô hình mạng độc lập (IBSSs) hay còn gọi là mạng Ad hoc.
- Mô hình mạng cơ sở (BSSs).
- Mô hình mạng mở rộng (ESSs).

3.3.3.1. Mô hình mạng AD HOC (Independent Basic Service Sets (IBSSs))

Các nút di động (máy tính có hỗ trợ card mạng không dây) tập trung lại trong một không gian nhỏ để hình thành nên kết nối ngang cáp (peer-to-peer) giữa chúng. Các nút di động có card mạng wireless là chúng có thể trao đổi thông tin trực tiếp với nhau, không cần phải quản trị mạng. Vì các mạng ad-hoc này có thể thực hiện nhanh và dễ dàng nên chúng thường được thiết lập mà không cần một công cụ hay kỹ năng đặc biệt nào vì vậy nó rất thích hợp để sử dụng trong các hội nghị thương mại hoặc trong các nhóm làm việc tạm thời. Tuy nhiên chúng có thể có những nhược điểm về vùng phủ sóng bị giới hạn, mọi người sử dụng đều phải nghe được lẫn nhau.

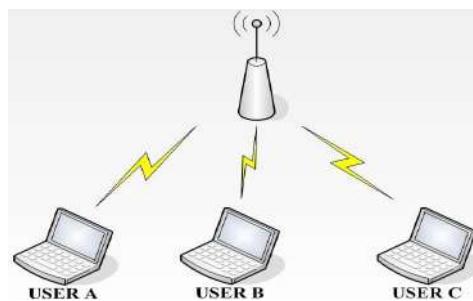


Hình 3.13. Mô hình mạng AD-HOC

3.3.3.2. Mô hình mạng cơ sở (Basic service sets (BSSs))

Bao gồm các điểm truy nhập AP (Access Point) gắn với mạng đường trục hữu tuyến và giao tiếp với các thiết bị di động trong vùng phủ sóng của một cell. AP đóng vai trò điều khiển cell và điều khiển lưu lượng tới mạng. Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các AP. Các cell có thể chồng lấn lên nhau khoảng 10-15% cho phép các trạm di động có thể di chuyển mà không bị mất kết nối vô tuyến và cung cấp vùng phủ sóng với chi phí thấp nhất. Các trạm di động sẽ chọn AP tốt nhất để kết nối. Một điểm truy nhập nằm ở trung tâm có thể điều khiển và phân phối truy nhập cho các nút tranh chấp, cung cấp truy nhập phù hợp với mạng đường trục, xác định các địa chỉ và các mức ưu tiên, giám sát lưu lượng mạng, quản lý chuyển đổi các gói và duy trì theo dõi cấu hình mạng. Tuy nhiên giao thức đa truy nhập tập trung không cho phép các nút di động truyền trực tiếp tới nút khác nằm

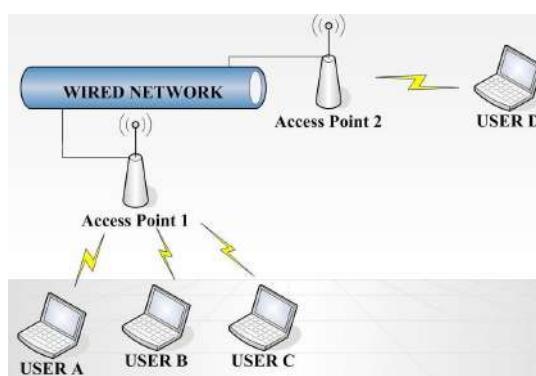
trong cùng vùng với điểm truy nhập như trong cấu hình mạng WLAN độc lập. Trong trường hợp này, mỗi gói sẽ phải được phát đi hai lần (từ nút phát gốc và sau đó là điểm truy nhập) trước khi nó tới nút đích, quá trình này sẽ làm giảm hiệu quả truyền dẫn và tăng trễ truyền dẫn.



Hình 3.14. Mô hình mạng cơ sở

3.3.3.3. Mô hình mạng mở rộng (Extended Service Set (ESSs))

Mạng 802.11 mở rộng phạm vi di động tới một phạm vi bất kì thông qua ESS. Một ESSs là một tập hợp các BSSs nơi mà các Access Point giao tiếp với nhau để chuyển lưu lượng từ một BSS này đến một BSS khác để làm cho việc di chuyển dễ dàng của các trạm giữa các BSS. Access Point thực hiện việc giao tiếp thông qua hệ thống phân phối. Hệ thống phân phối là một lớp mỏng trong mỗi Access Point mà nó xác định đích đến cho một lưu lượng được nhận từ một BSS. Hệ thống phân phối được tiếp sóng trở lại một đích trong cùng một BSS, chuyển tiếp trên hệ thống phân phối tới một Access Point khác, hoặc gửi tới một mạng có dây tới đích không nằm trong ESS. Các thông tin nhận bởi Access Point từ hệ thống phân phối được truyền tới BSS sẽ được nhận bởi trạm đích.



Hình III.15. Mô hình mạng mở rộng

3.4. PHƯƠNG PHÁP THIẾT KẾ VÀ LẮP ĐẶT WLAN

Trong quá trình khai mạng không dây, việc xác định vị trí và lắp đặt Wireless Access Point là một trong những yếu tố quan trọng quyết định đến tốc độ và sự ổn định của mạng. Nó không giống như chúng ta triển khai một mạng LAN thông thường vì công nghệ không dây truyền tín hiệu dựa trên sự truyền phát tín hiệu radio. Một khía cạnh khác của tín hiệu radio là loại tín hiệu có thể bị cản trở, phản hồi, bị chặn hoặc bị nhiễu bởi các vật cản như tường, trần nhà, lò vi sóng ..., việc này làm cho quá trình kết nối bị gián đoạn khi người sử dụng di chuyển trong phạm vi phủ sóng của mạng. Qua phần này, chúng ta có thể nắm bắt sơ qua các yếu tố ảnh hưởng đến quá trình truyền thông trong mạng không dây và từ đó tìm ra phương thức triển khai lắp đặt WLAN một cách tốt nhất.

3.4.1. Xem xét trước khi thiết kế

3.4.1.1. Các yêu cầu về Access Point

Xác định các yêu cầu cần thiết cho các Access Point trước khi chúng ta quyết định mua và lắp đặt nó vào hệ thống.

IEEE 802.1X và RADIUS (Remote Authentication Dial-In User Service)

- Để an toàn cho truyền thông không dây cho các tổ chức và các nhà cung cấp dịch vụ không dây công cộng thì Access Point cần phải hỗ trợ chuẩn IEEE 802.1X cho chứng thực kết nối không sử dụng các RADIUS server.
- Đối với các Access Point sử dụng trong văn phòng nhỏ hoặc gia đình thì có thể không cần hỗ trợ 802.1X và RADIUS.

WPA (Wi-Fi Protect Access)

- Để cung cấp mức bảo mật cao trong việc mã hóa và toàn vẹn dữ liệu và thay thế cho mã hóa WEP (Wired Equivalent Privacy) đã trở lên yếu kém, các Access Point cần phải hỗ trợ chuẩn WPA mới.
- Đối với các văn phòng nhỏ và gia đình, WPA cũng cung cấp một phương pháp chứng thực an toàn hơn mà không yêu cầu một RADIUS server.

802.11a, b, g, n: Tùy thuộc vào ngân sách cung cấp cho việc lắp đặt mạng mà chúng ta có thể sử dụng các Access Point có tốc độ khác, có thể cần Access Point hỗ trợ 802.11b (tối đa 11 Mbit/s) có giá thấp hay các Access Point hỗ trợ chuẩn 802.11a (tối đa 54) có giá cao hơn, 802.11g (tối đa 54 Mbit/s), 802.11n (tối đa 300 Mbit/s) hoặc sử dụng kết hợp các chuẩn trên.

Cấu hình trước và cấu hình từ xa các cho các Access Point

- Việc cấu Access Point trước khi lắp đặt chúng giúp tăng tốc độ của quá trình triển khai và tiết kiệm sức lao động. Chúng ta có thể cấu hình trước các Access Point bằng cách sử dụng cổng giao tiếp, Telnet hoặc Web server được tích hợp trong Access Point.
- Nếu chúng ta không thực hiện cấu hình trước các Access Point thì chí ít chúng ta cũng phải chắc chắn rằng chúng có thể cấu hình từ xa bằng công cụ của nhà cung cấp, vì nếu khi lắp đặt xong mà chúng ta không để truy nhập từ xa để cấu hình chúng thì điều đó thực sự là một thảm họa.

Các kiểu ăng-ten

- Chúng ta cần phải tìm hiểu xem Access Point đó có hỗ trợ nhiều loại antena khác nhau hay không? Ví dụ, trong một tòa nhà nhiều tầng, một Access Point với ăng-ten đǎng hướng truyền phát tín hiệu như nhau theo tất cả các phương hướng trừ phương thẳng đứng có thể làm việc tốt nhất.
- Để biết được Access Point có hỗ trợ những loại antena nào thì cần xem hướng dẫn đi kèm Access Point.

3.4.1.2. Tách kênh

Nếu chúng ta cấu hình hoạt động Access Point ở một kênh cụ thể thì card mạng không dây sẽ tự động cấu hình chính nó theo kênh của Access Point với tín hiệu mạnh nhất. Do vậy, để giảm bớt giao thoa giữa các Access Point chuẩn, chúng ta phải cấu hình cho mỗi Access Point có vùng phủ sóng chồng lên nhau ở một kênh riêng biệt. Trong Access Point đã cung cấp sẵn cho chúng ta khoảng 15 kênh.

Để ngăn tín hiệu từ các Access Point liền kề xen vào với nhau, phải đặt số kênh của chúng cách nhau ít nhất là 5 kênh. Chúng ta có thể sử dụng một trong ba kênh là 1, 6 hoặc 11. Nếu không dùng đến 3 kênh trên thì chúng ta phải đảm bảo sao cho khoảng cách giữa các kênh là 5 kênh.

Ví dụ: 1, 6, 1, 6, 11, 6 là các số hiệu kênh

3.4.1.3. Xác định các vật cản xung quanh

Việc lựa chọn vị trí đặt Access Point phụ thuộc vào cấu trúc của tòa nhà, các vật cản... Việc thay đổi truyền phát tín hiệu làm biến dạng vùng phủ sóng vi lý tưởng qua việc ngăn chặn, phản hồi và suy giảm tần số radio (giảm cường độ tín hiệu) có thể ảnh hưởng đến cách chúng ta triển khai Access Point. Các vật kim loại trong 1 tòa nhà hoặc được dùng trong xây dựng của một tòa nhà có thể ảnh hưởng đến tín hiệu không dây.

- Xà nhà.
- Cáp thang máy.
- Thép trong bê tông.
- Các ống thông gió, điều hòa nhiệt độ và điều hòa không khí.
- Dây lưới đỡ thạch cao hoặc vữa trên tường.
- Tường chứa kim loại, các khối xi than, bê tông.
- Bàn kim loại, bể cá, hoặc các loại thiết bị kim loại lớn khác.

3.4.1.4. Xác định các nguồn giao thoa

Bất cứ thiết bị nào hoạt động trên các tần số giống như các thiết bị mạng không dây của chúng ta (trong băng S dải tần ISM hoạt động trong dải tần số từ 2.4GHz đến 2.5GHz, hoặc băng C hoạt động trong dải tần số từ 5.725GHz đến 5.875GHz) đều có thể bị nhiễu tín hiệu. Các nguồn giao thoa cũng làm biến dạng một vùng phủ sóng vi lý tưởng của Access Point. Vì vậy ta cần lựa chọn vị trí đặt Access Point cách xa các nguồn giao thoa này.

Các thiết bị hoạt động trong băng C dải tần ISM bao gồm:

- Các thiết bị cho phép dùng bluetooth
- Lò vi sóng

- Phone 2.4GHz
- Camera không dây
- Các thiết bị y học
- Động cơ thang máy

3.4.1.5. Xác định số lượng Access Point

Để xác định số Access Point để triển khai, hãy theo các nguyên tắc chỉ dẫn sau:

Phải có đủ Access Point để đảm bảo những người dùng không dây có đủ cường độ tín hiệu từ bất cứ đâu trong vùng thể tích phạm vi. Các Access Point điển hình sử dụng ăng-ten đăng hướng phát ra 1 vùng tín hiệu hình tròn phẳng thẳng đứng lan truyền giữa các tầng của tòa nhà. Điểm hình, Access Point có phạm vi trong nhà trong vòng bán kính 200 foot (đổi ra đơn vị mét). Phải có đủ Access Point để đảm bảo rằng tín hiệu chồng lên nhau giữa các Access Point.

Xác định số lượng lớn nhất những người dùng không dây cùng lúc trên một vùng phạm vi.

Đánh giá lưu lượng dữ liệu mà trung bình người dùng không dây thường yêu cầu. Nếu cần thì tăng thêm số Access Point, điều đó sẽ:

- Cải thiện khả năng băng thông mạng máy khách không dây.
- Tăng số lượng người dùng không dây được hỗ trợ trong vùng phạm vi.

Dựa trên toàn bộ lưu lượng dữ liệu của tất cả người dùng, xác định số người dùng mà chúng ta có thể kết nối họ tới một Access Point. Hãy hiểu biết rõ về lưu lượng trước khi triển khai hoặc thay đổi mạng. Vài nhà cung cấp không dây cung cấp một công cụ mô phỏng chuẩn 802.11 mà chúng ta có thể sử dụng để làm mẫu sự lưu chuyển trong mạng và xem mức lưu lượng dưới nhiều điều kiện.

Hãy đảm bảo sự dư thừa trong trường hợp một Access Point bị lỗi.

3.4.2. Triển khai Access Point

Điều quan trọng trong việc triển khai lắp đặt Access Point là lắp đặt các Access Point sao cho phải đủ gần nhau để cung cấp phạm vi rộng

nhưng phải đủ xa để các Access Point không gây nhiễu lẫn nhau. Khoảng cách thực tế giữa hai Access Point bất kỳ phụ thuộc vào sự kết hợp của kiểu Access Point (kiểu ăng-ten của Access Point và cấu trúc xây dựng của tòa nhà) cũng như các nguồn làm giảm, chặn và phản hồi tín hiệu.

Chúng ta nên cố gắng giữ tỉ lệ trung bình tốt nhất giữa các máy trạm tới Access Point, tức là không để một Access Point phục vụ quá nhiều máy trạm còn một Access Point lại phục vụ một vài máy trạm vì lượng trung bình người dùng kết nối tới một Access Point càng lớn thì hiệu quả truyền dữ liệu càng thấp. Quá nhiều máy khách sử dụng cùng một Access Point sẽ làm giảm lưu lượng mạng, hiệu quả và băng thông cho mỗi máy khách.

Bằng cách tăng thêm số Access Point giúp tăng thêm lưu lượng và giảm tải cho mạng. Để tăng thêm số Access Point tỉ lệ với số máy khách thì cần phải tăng số Access Point trong một vùng thể tích phạm vi đã cho.

Để triển khai Access Point của chúng ta, hãy làm theo các bước sau:

- Phân tích vị trí các Access Point dựa trên sơ đồ tòa nhà.
- Lắp đặt tạm thời các Access Point.
- Phân tích cường độ tín hiệu trên tất cả các vùng.
- Tái định vị các Access Point.
- Xác định vùng thể tích phạm vi.
- Cập nhật các bản vẽ kiến trúc của mạng để đổi chiều số lượng và vị trí cuối cùng của các Access Point.

3.4.2.1. Phân tích các vị trí đặt Access Point

Vẽ phác thảo kiến trúc cho mỗi tầng của tòa nhà. Trên bản vẽ cho mỗi tầng, xác định các văn phòng, các phòng hội nghị, hành lang hoặc các nơi khác mà chúng ta muốn cung cấp truy nhập không dây.

Trên bản kế hoạch hãy ghi rõ các thiết bị gây nhiễu và đánh dấu các vật liệu xây dựng tòa nhà hoặc các vật có thể làm giảm, phản hồi hoặc chặn các tín hiệu không dây. Sau đó chỉ rõ vị trí các Access Point mà mỗi Access Point cách Access Point liền kề không quá 60m.

Sau khi xác định các vị trí của các Access Point, chúng ta phải xác định các kênh của chúng sau đó gán số hiệu kênh cho mỗi Access Point.

- Xác định xem có mạng không dây nào ở gần không để xác định số hiệu kênh và nơi đặt Access Point của họ. Điều đó giúp ta triển khai các Access Point của mình mà không sợ bị nhiễu do trùng kênh.
- Các Access Point đặt gần nhau trên các tầng khác nhau phải được gán các sao cho các kênh của chúng không bị chồng lên nhau.
- Sau khi xác định vùng thể tích không gian chồng lên nhau trong và ngoài mạng, hãy gán các số hiệu kênh cho các Access Point.

3.4.2.2. Lắp đặt tạm thời các Access Point

Lắp đặt dựa vào các vị trí, các cấu hình kênh đã được ghi trong bản kế hoạch và các phân tích cơ bản về vị trí của các Access Point.

3.4.2.3. Khảo sát vị trí

Ta có thể thực hiện khảo sát vị trí bằng cách đi quanh tòa nhà và các tầng của nó với một chiếc laptop hỗ trợ 802.11 và phần mềm khảo sát vị trí. Xác định cường độ tín hiệu và tốc độ truyền của vùng thể tích phạm vi cho mỗi Access Point được cài đặt.

3.4.2.4. Tái định vị các Access Point

Tại những vị trí có cường độ tín hiệu yếu, chúng ta có thể thực hiện những điều chỉnh sau đây để cải thiện tín hiệu.

- Đặt cố định các Access Point đã được cài đặt tạm để làm tăng cường độ tín hiệu cho vùng thể tích phạm vi đó.
- Đặt lại hoặc loại bỏ các thiết bị gây nhiễu (bluetooth, lò vi sóng, ...).
- Đặt lại hoặc loại bỏ các vật kim loại gây nhiễu (tủ hồ sơ, các thiết bị hoặc dụng cụ,...).
- Thêm nhiều Access Point hơn để bù cho cường độ tín hiệu yếu. (Nếu thêm Access Point, có thể chúng ta phải thay đổi số hiệu kênh của các Access Point liền kề nhau).
- Mua các ăng-ten phù hợp với yêu cầu cơ sở hạ tầng của tòa nhà. Ví dụ để loại bỏ giao thoa giữa các Access Point đặt trên các tầng gần nhau trong tòa nhà, chúng ta có thể mua các ăng-ten định hướng để tăng phạm vi nằm ngang và giảm phạm vi thẳng đứng.

3.4.2.5. Xác minh vùng thể tích phạm vi

Khảo sát các vị trí khác để giúp loại trừ các vị trí có cường độ tín hiệu yếu.

3.4.2.6. Cập nhật kế hoạch

Cập nhật các bản vẽ kiến trúc để đổi chiếu số lượng và vị trí cuối cùng của các Access Point. Chỉ rõ ranh giới vùng thể tích phạm vi cho mỗi Access Point nơi tốc độ truyền dữ liệu thay đổi.

Những nguy cơ bảo mật trong WLAN bao gồm:

- Các thiết bị có thể kết nối tới những Access Point đang broadcast SSID.
- Hacker sẽ cố gắng tìm kiếm các phương thức mã hoá đang được sử dụng trong quá trình truyền thông tin trên mạng, sau đó có phương thức giải mã riêng và lấy các thông tin nhạy cảm.
- Người dùng sử dụng Access Point tại gia đình sẽ không đảm bảo tính bảo mật như khi sử dụng tại doanh nghiệp.

Để bảo mật mạng WLAN, ta cần thực hiện qua các bước: Authentication → Encryption → IDS & IPS.

- Chỉ có những người dùng được xác thực mới có khả năng truy nhập vào mạng thông qua các Access Point.
- Các phương thức mã hoá được áp dụng trong quá trình truyền các thông tin quan trọng.
- Bảo mật các thông tin và cảnh báo nguy cơ bảo mật bằng hệ thống IDS (Intrusion Detection System) và IPS (Intrusion Prevention System). Xác thực và bảo mật dữ liệu bằng cách mã hoá thông tin truyền trên mạng. IDS như một thiết bị giám sát mạng Wireless và mạng Wired để tìm kiếm và cảnh báo khi có các dấu hiệu tấn công.

3.4.3. Các phần mềm hỗ trợ

Ekahau 2.1: Khảo sát mạng WLAN.

Sniffer Wireless: Phần mềm bắt gói tin giống Wireshark (Ethereal).

Network Stumbler: Là một công cụ rất phổ biến và hữu dụng cho chúng ta khi muốn dò tìm sóng Wireless và các thông tin cơ bản của một mạng Wireless (đây cũng là công cụ mà những kẻ tấn công dùng để bắt lấy những thông tin cơ bản của mạng trước khi tấn công). NetStumbler sẽ dò tìm các thông số như MAC, SSID, Channel, Type, Encryption.

SMAC 2.0: Là chương trình hỗ trợ cho chúng ta thay đổi địa chỉ MAC (địa chỉ vật lý do nhà sản xuất thiết lập sẵn trên card mạng). Thông thường về nguyên tắc là địa chỉ này là cố định và là duy nhất, nhưng chương trình sẽ cho phép bạn thay đổi giá trị địa chỉ này (thông thường các kẻ tấn công làm như vậy để có thể mạo danh truy nhập vào AP, mạo danh là User của mạng, ...).

ManageEngine Wifi Manager: Là phần mềm cung cấp các giải pháp quản lý và bảo mật. Phát hiện Access Point giả mạo, cho biết các thông tin cấu hình Access Point trong việc giám sát mạng.

Airsnot, Kismet ...

Kết luận: Trước khi triển khai Access Point, chúng ta hãy xem xét các yêu cầu về Access Point, việc tách kênh, các thay đổi truyền phát tín hiệu, các nguồn giao thoa (nguồn gây nhiễu), số lượng Access Point cần thiết tương ứng với phạm vi không dây, băng thông, và các yêu cầu dự trữ.

Để triển khai Access Point, hãy ước lượng các vị trí Access Point dựa trên sơ đồ tòa nhà và các kiến thức về sự thay đổi truyền phát tín hiệu và các nguồn giao thoa (nguồn nhiễu). Cài đặt các Access Point tại các vị trí tạm và thực hiện khảo sát vị trí (lưu ý các vùng bị thiểu phạm vi). Thay đổi vị trí các Access Point, các thay đổi truyền phát tín hiệu hoặc các nguồn giao thoa và xác minh phạm vi bằng cách thực hiện khảo sát vị trí bổ sung. Sau khi xác định các vị trí cuối cùng của các Access Point.

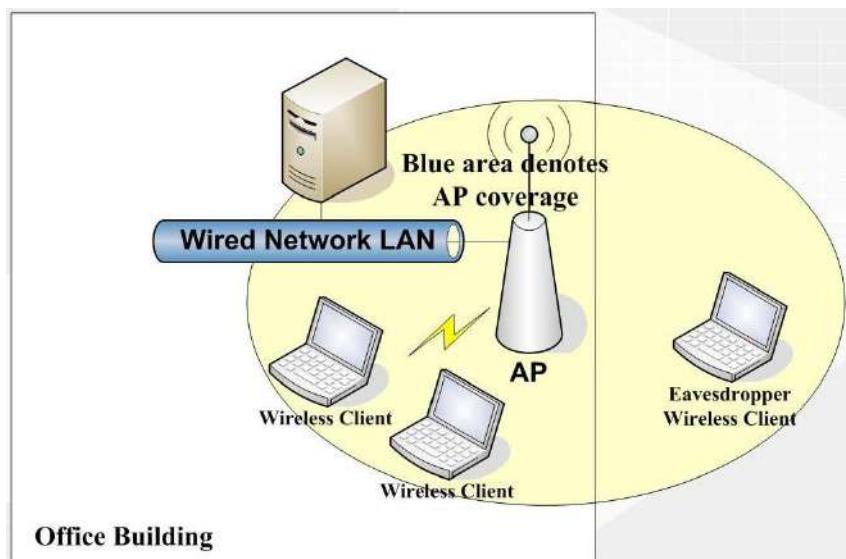
3.5. BẢO MẬT WLAN

3.5.1. Tại sao phải bảo mật WLAN?

Để kết nối tới một mạng LAN hữu tuyến ta cần phải truy nhập theo đường truyền bằng dây cáp, phải kết nối một PC vào một cổng mạng. Với mạng không dây ta chỉ cần có máy của ta trong vùng sóng bao phủ

của mạng không dây. Điều khiển cho mạng có dây là đơn giản: đường truyền bằng cáp thông thường được đi trong các tòa nhà cao tầng và các port không sử dụng có thể làm cho nó disable bằng các ứng dụng quản lý. Các mạng không dây (hay vô tuyến) sử dụng sóng vô tuyến xuyên qua vật liệu của các tòa nhà và như vậy sự bao phủ là không giới hạn ở bên trong một tòa nhà. Sóng vô tuyến có thể xuất hiện trên đường phố, từ các trạm phát từ các mạng LAN này, và như vậy ai đó có thể truy nhập nhờ thiết bị thích hợp. Do đó mạng không dây của một công ty cũng có thể bị truy nhập từ bên ngoài tòa nhà công ty của họ.

Với giá thành xây dựng một hệ thống mạng WLAN giảm, ngày càng có nhiều công ty sử dụng. Điều này sẽ không tránh khỏi việc Hacker chuyển sang tấn công và khai thác các điểm yếu trên nền tảng mạng sử dụng chuẩn 802.11. Những công cụ Sniffers cho phép tóm được các gói tin giao tiếp trên mạng, họ có thể phân tích và lấy đi những thông tin quan trọng của chúng ta.



Hình 3.16. Truy nhập trái phép mạng không dây

Những nguy cơ bảo mật trong WLAN bao gồm:

- Các thiết bị có thể kết nối tới những Access Point đang broadcast SSID.

- Hacker sẽ cố gắng tìm kiếm các phương thức mã hoá đang được sử dụng trong quá trình truyền thông tin trên mạng, sau đó có phương thức giải mã riêng và lấy các thông tin nhạy cảm.
- Người dùng sử dụng Access Point tại gia đình sẽ không đảm bảo tính bảo mật như khi sử dụng tại doanh nghiệp.

Để bảo mật mạng WLAN, ta cần thực hiện qua các bước: Authentication → Encryption → IDS & IPS.

- Chỉ có những người dùng được xác thực mới có khả năng truy nhập vào mạng thông qua các Access Point.
- Các phương thức mã hoá được áp dụng trong quá trình truyền các thông tin quan trọng.
- Bảo mật các thông tin và cảnh báo nguy cơ bảo mật bằng hệ thống IDS (Intrusion Detection System) và IPS (Intrusion Prevention System). Xác thực và bảo mật dữ liệu bằng cách mã hoá thông tin truyền trên mạng. IDS như một thiết bị giám sát mạng Wireless và mạng Wired để tìm kiếm và cảnh báo khi có các dấu hiệu tấn công.

3.5.2. WEP

WEP (Wired Equivalent Privacy) có nghĩa là bảo mật không dây tương đương với có dây. Thực ra, WEP đã đưa cả xác thực người dùng và đảm bảo an toàn dữ liệu vào cùng một phương thức không an toàn. WEP sử dụng một khoá mã hoá không thay đổi có độ dài 64 bit hoặc 128 bit, (nhưng trừ đi 24 bit sử dụng cho vector khởi tạo khoá mã hoá, nên độ dài khoá chỉ còn 40 bit hoặc 104 bit) được sử dụng để xác thực các thiết bị được phép truy nhập vào trong mạng và cũng được sử dụng để mã hoá truyền dữ liệu.

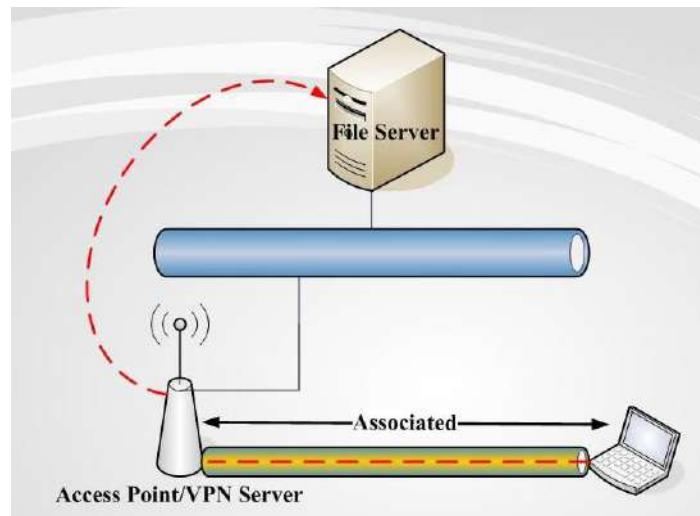
Rất đơn giản, các khoá mã hoá này dễ dàng bị "bẻ gãy" bởi thuật toán brute-force và kiểu tấn công thử lỗi (trial-and-error). Các phần mềm miễn phí như Airsnort hoặc WEPCrack sẽ cho phép hacker có thể phá vỡ khoá mã hoá nếu họ thu thập đủ từ 5 đến 10 triệu gói tin trên một mạng không dây. Với những khoá mã hoá 128 bit cũng không khá hơn: 24 bit cho khởi tạo mã hoá nên chỉ có 104 bit được sử dụng để mã hoá, và cách

thức cũng giống như mã hoá có độ dài 64 bit nên mã hoá 128 bit cũng dễ dàng bị bẻ khoá. Ngoài ra, những điểm yếu trong những vector khởi tạo khoá mã hoá giúp cho hacker có thể tìm ra mật khẩu nhanh hơn với ít gói thông tin hơn rất nhiều.

Không dự đoán được những lỗi trong khoá mã hoá, WEP có thể được tạo ra cách bảo mật mạnh mẽ hơn nếu sử dụng một giao thức xác thực mà cung cấp mỗi khoá mã hoá mới cho mỗi phiên làm việc. Khoá mã hoá sẽ thay đổi trên mỗi phiên làm việc. Điều này sẽ gây khó khăn hơn cho hacker thu thập đủ các gói dữ liệu cần thiết để có thể bẻ gãy khoá bảo mật.

3.5.3. WLAN VPN

Mạng riêng ảo VPN bảo vệ mạng WLAN bằng cách tạo ra một kênh che chắn dữ liệu khỏi các truy nhập trái phép. VPN tạo ra một tin cậy cao thông qua việc sử dụng một cơ chế bảo mật như IPSec (Internet Protocol Security). IPSec dùng các thuật toán mạnh như Data Encryption Standard (DES) và Triple DES (3DES) để mã hóa dữ liệu và dùng các thuật toán khác để xác thực gói dữ liệu. IPSec cũng sử dụng thẻ xác nhận số để xác nhận khóa mã (public key). Khi được sử dụng trên mạng WLAN, cổng kết nối của VPN đảm nhận việc xác thực, đóng gói và mã hóa.



Hình 3.17. Mô hình WLAN VPN

3.5.4. TKIP

TKIP (Temporal Key Integrity Protocol) là giải pháp của IEEE được phát triển năm 2004. Là một nâng cấp cho WEP nhằm vá những vấn đề bảo mật trong cài đặt mã dòng RC4 trong WEP. TKIP dùng hàm băm (hashing) IV để chống lại việc giả mạo gói tin, nó cũng cung cấp phương thức để kiểm tra tính toàn vẹn của thông điệp MIC (Message Integrity Check) để đảm bảo tính chính xác của gói tin. TKIP sử dụng khóa động bằng cách đặt cho mỗi frame một chuỗi số riêng để chống lại dạng tấn công giả mạo.

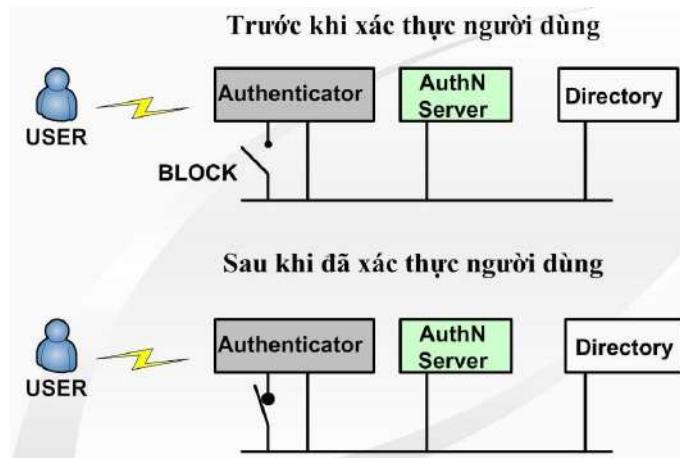
3.5.5. AES

Trong mật mã học, AES (Advanced Encryption Standard - Tiêu chuẩn mã hóa tiên tiến) là một thuật toán mã hóa khối được chính phủ Hoa Kỳ áp dụng làm tiêu chuẩn mã hóa. Giống như tiêu chuẩn tiền nhiệm DES, AES được kỳ vọng áp dụng trên phạm vi thế giới và đã được nghiên cứu rất kỹ lưỡng. AES được chấp thuận làm tiêu chuẩn liên bang bởi Viện tiêu chuẩn và công nghệ quốc gia Hoa Kỳ (NIST) sau một quá trình tiêu chuẩn hóa kéo dài 5 năm.

Thuật toán được thiết kế bởi hai nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen (lấy tên chung là "Rijndael" khi tham gia cuộc thi thiết kế AES). Rijndael được phát âm là "Rhine dahl" theo phiên âm quốc tế (IPA: [raindal]).

3.5.6. 802.1X và EAP

802.1x là chuẩn đặc tả cho việc truy nhập dựa trên cổng (port-based) được định nghĩa bởi IEEE. Hoạt động trên cả môi trường có dây truyền thống và không dây. Việc điều khiển truy nhập được thực hiện bằng cách: Khi một người dùng cố gắng kết nối vào hệ thống mạng, kết nối của người dùng sẽ được đặt ở trạng thái bị chặn (blocking) và chờ cho việc kiểm tra định danh người dùng hoàn tất.



Hình 3.18. Mô hình hoạt động xác thực 802.1x

EAP là phương thức xác thực bao gồm yêu cầu định danh người dùng (password, certificate,...), giao thức được sử dụng (MD5, TLS_Transport Layer Security, OTP_ One Time Password,...) hỗ trợ tự động sinh khóa và xác thực lẫn nhau.

Quá trình chứng thực 802.1x-EAP như sau: Wireless client muốn liên kết với một AP trong mạng.

1. AP sẽ chặn lại tất cả các thông tin của client cho tới khi client log on vào mạng, khi đó Client yêu cầu liên kết tới AP
2. AP đáp lại yêu cầu liên kết với một yêu cầu nhận dạng EAP
3. Client gửi đáp lại yêu cầu nhận dạng EAP cho AP
4. Thông tin đáp lại yêu cầu nhận dạng EAP của client được chuyển tới Server chứng thực
5. Server chứng thực gửi một yêu cầu cho phép tới AP
6. AP chuyển yêu cầu cho phép tới client
7. Client gửi trả lời sự cấp phép EAP tới AP
8. AP chuyển sự trả lời đó tới Server chứng thực
9. Server chứng thực gửi một thông báo thành công EAP tới AP
10. AP chuyển thông báo thành công tới client và đặt cổng của client trong chế độ forward.

3.5.7. WPA

WEP được xây dựng để bảo vệ một mạng không dây tránh bị nghe trộm. Nhưng nhanh chóng sau đó người ta phát hiện ra nhiều lỗ hổng ở công nghệ này. Do đó, công nghệ mới có tên gọi WPA (Wi-Fi Protected Access) ra đời, khắc phục được nhiều nhược điểm của WEP.

Trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khoá TKIP. WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit. Và một đặc điểm khác là WPA thay đổi khoá cho mỗi gói tin. Các công cụ thu thập các gói tin để phá khoá mã hoá đều không thể thực hiện được với WPA. Bởi WPA thay đổi khoá liên tục nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu.

Không những thế, WPA còn bao gồm kiểm tra tính toàn vẹn của thông tin (Message Integrity Check). Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền. WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn đều sử dụng giao thức TKIP, và sự khác biệt chỉ là khoá khởi tạo mã hóa lúc đầu. WPA Personal thích hợp cho gia đình và mạng văn phòng nhỏ, khoá khởi tạo sẽ được sử dụng tại các điểm truy nhập và thiết bị máy trạm. Trong khi đó, WPA cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khoá khởi tạo cho mỗi phiên làm việc.

Lưu ý: Có một lỗ hổng trong WPA và lỗi này chỉ xảy ra với *WPA Personal*. Khi mà sử dụng hàm thay đổi khoá TKIP được sử dụng để tạo ra các khoá mã hoá bị phát hiện, nếu hacker có thể đoán được khoá khởi tạo hoặc một phần của mật khẩu, họ có thể xác định được toàn bộ mật khẩu, do đó có thể giải mã được dữ liệu. Tuy nhiên, lỗ hổng này cũng sẽ bị loại bỏ bằng cách sử dụng những khoá khởi tạo không dễ đoán (đừng sử dụng những từ như "P@SSWORD" để làm mật khẩu).

Điều này cũng có nghĩa rằng kỹ thuật TKIP của WPA chỉ là giải pháp tạm thời, chưa cung cấp một phương thức bảo mật cao nhất. WPA chỉ thích hợp với những công ty mà không truyền dữ liệu "mật" về những thương mại, hay các thông tin nhạy cảm... WPA cũng thích hợp với những hoạt động hàng ngày và mang tính thử nghiệm công nghệ.

3.5.8. WPA2

Một giải pháp về lâu dài là sử dụng 802.11i tương đương với WPA2, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hoá mạnh mẽ và được gọi là Chuẩn mã hoá nâng cao **AES**. AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit. Để đánh giá chuẩn mã hoá này, Viện nghiên cứu quốc gia về Chuẩn và Công nghệ của Mỹ, NIST (National Institute of Standards and Technology), đã thông qua thuật toán mã hoá đối xứng này.

Lưu ý: Chuẩn mã hoá này được sử dụng cho các cơ quan chính phủ Mỹ để bảo vệ các thông tin nhạy cảm.

Trong khi AES được xem như là bảo mật tốt hơn rất nhiều so với WEP 128 bit hoặc 168 bit DES (Digital Encryption Standard). Để đảm bảo về mặt hiệu năng, quá trình mã hoá cần được thực hiện trong các thiết bị phần cứng như tích hợp vào chip. Tuy nhiên, rất ít người sử dụng mạng không dây quan tâm tới vấn đề này. Hơn nữa, hầu hết các thiết bị cầm tay Wi-Fi và máy quét mã vạch đều không tương thích với chuẩn 802.11i.

3.5.9. Lọc (Filtering)

Lọc là cơ chế bảo mật cơ bản có thể sử dụng cùng với WEP. Lọc hoạt động giống như **Access list** trên router, cấm những cái không mong muốn và cho phép những cái mong muốn. Có 3 kiểu lọc cơ bản có thể được sử dụng trong wireless lan:

- Lọc SSID
- Lọc địa chỉ MAC
- Lọc giao thức

3.5.9.1. Lọc SSID

Lọc SSID là một phương thức cơ bản của lọc và chỉ nên được sử dụng cho việc điều khiển truy nhập cơ bản.

SSID của client phải khớp với SSID của AP để có thể xác thực và kết nối với tập dịch vụ. SSID được quảng bá mà không được mã hóa

trong các Beacon nên rất dễ bị phát hiện bằng cách sử dụng các phần mềm. Một số sai lầm mà người sử dụng WLAN mắc phải trong việc quản lý SSID gồm:

- Sử dụng giá trị SSID mặc định tạo điều kiện cho hacker dò tìm địa chỉ MAC của AP.
- Sử dụng SSID có liên quan đến công ty.
- Sử dụng SSID như là phương thức bảo mật của công ty.
- Quảng bá SSID một cách không cần thiết.

3.5.9.2. Lọc địa chỉ MAC

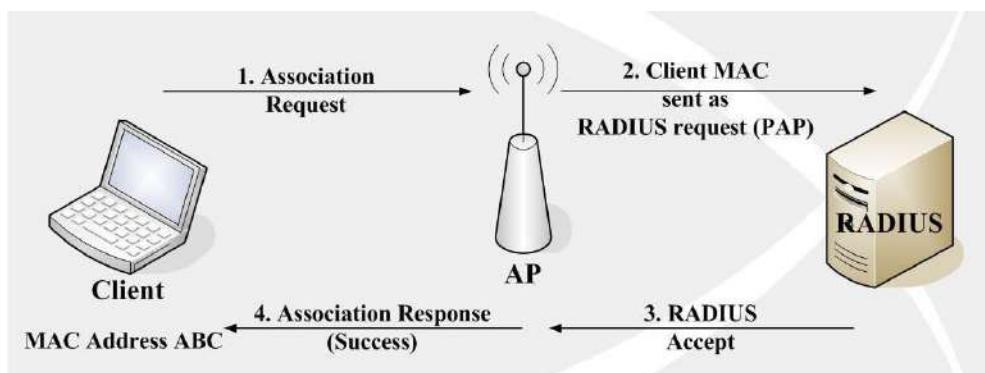
Hầu hết các AP đều có chức năng lọc địa chỉ MAC. Người quản trị có thể xây dựng danh sách các địa chỉ MAC được cho phép.

Nếu client có địa chỉ MAC không nằm trong danh sách lọc địa chỉ MAC của AP thì AP sẽ ngăn chặn không cho phép client đó kết nối vào mạng.

Nếu công ty có nhiều client thì có thể xây dựng máy chủ RADIUS có chức năng lọc địa chỉ MAC thay vì AP. Cấu hình lọc địa chỉ MAC là giải pháp bảo mật có tính mở rộng cao.

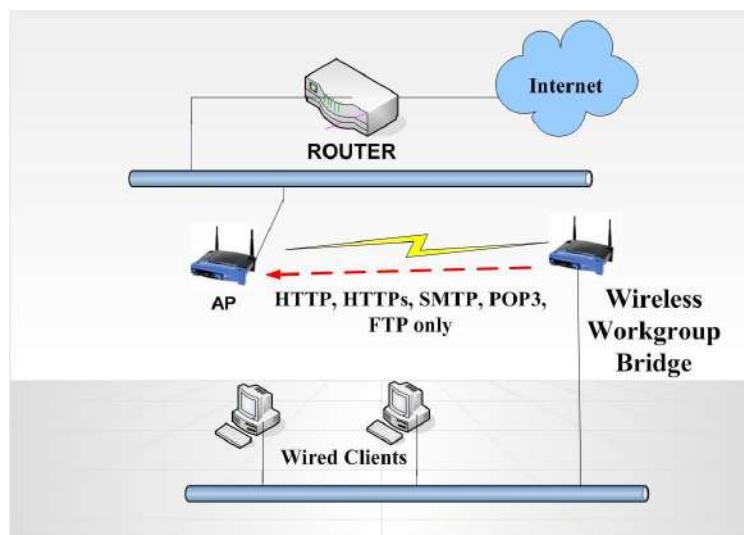
3.5.9.3. Lọc giao thức

Mạng Lan không dây có thể lọc các gói đi qua mạng dựa trên các giao thức từ lớp 2 đến lớp 7. Trong nhiều trường hợp người quản trị nên cài đặt lọc giao thức trong môi trường dùng chung, ví dụ trong trường hợp sau:



Hình 3.19. Tiến trình xác thực MAC

- Có một nhóm cầu nối không dây được đặt trên một Remote building trong một mạng WLAN của một trường đại học mà kết nối lại tới AP của tòa nhà kỹ thuật trung tâm.
- Vì tất cả những người sử dụng trong remote building chia sẻ băng thông 5Mbit/s giữa những tòa nhà này, nên một số lượng đáng kể các điều khiển trên các sử dụng này phải được thực hiện.
- Nếu các kết nối này được cài đặt với mục đích đặc biệt của sự truy nhập Internet của người sử dụng, thì bộ lọc giao thức sẽ loại trừ tất cả các giao thức, ngoại trừ HTTP, SMTP, HTTPS, FTP...



Hình 3.20. Lọc giao thức

3.5.10. Kết luận

Cho các điểm truy nhập tự động (hotspots), việc mã hoá không cần thiết, chỉ cần người dùng xác thực mà thôi.

Với người dùng sử dụng mạng WLAN cho gia đình, một phương thức bảo mật với WPA passphrase hay khóa chia sẻ (preshared key) được khuyến cáo sử dụng.

Với giải pháp doanh nghiệp, để tối ưu quá trình bảo mật với 802.1x EAP làm phương thức xác thực và TKIP hay AES làm phương thức mã hoá. Được dựa theo chuẩn WPA hay WPA2 và 802.11i Security.

Bảng 3.6. Escalating Security

Open Access	Basic Security	Enhanced Security	Remote Access
<ul style="list-style-type: none"> - No encryption - Basic authentication - Public “hotspots” 	<ul style="list-style-type: none"> - WPA Passphase - WEP Encryption - Home use 	<ul style="list-style-type: none"> - 802.1x EAP - Mutual Anthentication - TKIP Encrytion - WPA/WPA2 - 802.11i Security - Enterprise 	<ul style="list-style-type: none"> - Virtual Private Network (VPN) - Business Traveler - Telecommuter

- Bảo mật mạng WLAN cũng tương tự như bảo mật cho các hệ thống mạng khác. Bảo mật hệ thống phải được áp dụng cho nhiều tầng, các thiết bị nhận dạng phát hiện tấn công phải được triển khai. Giới hạn các quyền truy nhập tối thiểu cho những người dùng cần thiết. Dữ liệu được chia sẻ và yêu cầu xác thực mới cho phép truy cập. Dữ liệu truyền phải được mã hoá.
- Kẻ tấn công có thể tấn công mạng WLAN không bảo mật bất cứ lúc nào. Bạn cần có một phương án triển khai hợp lý.
- Phải ước lượng được các nguy cơ bảo mật và các mức độ bảo mật cần thiết để áp dụng.
- Đánh giá được toàn bộ các giao tiếp qua WLAN và các phương thức bảo mật cần được áp dụng.
- Đánh giá được các công cụ và các lựa chọn khi thiết kế về triển khai mạng WLAN.

Trong khi sử dụng VPN Fix qua các kết nối WLAN có thể là một ý tưởng hay và cũng sẽ là một hướng đi đúng. Nhưng sự không thuận tiện cũng như giá cả và tăng lưu lượng mạng cũng là rào cản cần vượt qua. Sự chuyển đổi sang 802.11i và mã hoá AES đem lại khả năng bảo mật cao nhất. Nhưng các tổ chức, cơ quan vẫn đang sử dụng hàng nghìn những card mạng WLAN không hỗ trợ chuẩn này. Hơn nữa AES không hỗ trợ các thiết bị cầm tay và máy quét mã vạch hoặc các thiết bị khác... Đó là những giới hạn khi lựa chọn 802.11i. Sự chuyển hướng sang WPA vẫn

còn là những thử thách. Mặc dù, vẫn còn những lỗ hổng về bảo mật và có thể những lỗ hổng mới sẽ được phát hiện. Nhưng tại thời điểm này, WPA là lựa chọn tốt.

3.6. BÀI TOÁN THỰC TẾ

Đây là bài toán thiết kế và xây dựng một kết nối, nối hai mạng cục bộ lại với nhau và tại một điểm đầu được phủ sóng không dây phục vụ các nhu cầu truy nhập Internet của các Wireless Client tại khu vực đầu cầu này. Sử dụng các công nghệ và thiết bị sẵn có trên thị trường. Bài toán này áp dụng thiết lập kết nối hệ thống mạng tại cơ sở X với trụ sở Y của một trường Đại học. Yêu cầu bản thiết kế phải đảm bảo được các vấn đề dưới đây khi xây dựng mạng và đưa vào sử dụng:

- Đảm bảo được việc kết nối thông suốt giữa hai vị trí và giữa các Wireless Client với mạng Internet.
- Đảm bảo được tốc độ truyền trong mạng trong giờ bình thường và giờ cao điểm, thực hiện nhiều công việc cùng lúc.
- Có thể nâng cấp mạng dựa trên cơ sở hạ tầng hiện tại. Đáp ứng được nhu cầu phát triển của những năm sắp đến.
- Đảm bảo các thiết bị hoạt động với hiệu năng cao.
- Có các biện pháp mã hóa, bảo vệ thông tin truyền thông trong mạng.
- Giá thành vừa phải.
- Dễ dàng nâng cấp, sửa chữa bảo trì, thay thế thiết bị.
- Chú trọng tính tương thích với các hệ thống khác.

3.6.1 Phân tích hiện trạng

Hiện tại ở hai đầu cầu X và Y đã có sẵn hệ thống mạng có dây phục vụ, xử lý tốt các công việc cục bộ ở hai điểm và có khả năng mở rộng tốt. Để mở rộng kết nối mạng theo yêu cầu trên, chúng ta cần phân tích và làm rõ một số thông số. Kết quả ghi nhận như sau:

Tra (Traffic): Số lượng các giao dịch phải xử lý trong một ngày khoảng 200 giao dịch. Phục vụ các công việc sau:

- Cập nhật cơ sở dữ liệu nộp học phí sinh viên từ phòng Kế Hoạch Tài Chính (KHTC).
- Chuyển văn bản và quyết định giữa khoa Xây dựng (KXD), phòng KHTC, các trung tâm và phòng ban khác với văn phòng nhà trường.
- Thực hiện copy/paste dữ liệu chia sẻ giữa các máy tính ở hai nơi.

CBH (Concertration Ratio to Busy Hours): Độ tập trung truyền thông cao điểm là 1/8 trên tổng số giờ truyền.

- Tại giờ cao điểm có khoảng 6 truy nhập giữa các máy tính ở hai vị trí với nhau. Và rất nhiều truy nhập tại nội bộ mỗi vị trí. Lưu lượng đường truyền lúc này trung bình là 10 Mb.
- Giờ thấp điểm có dưới 3 truy nhập vào giữa các máy này. Lưu lượng đường truyền trung bình là 4 Mb.
- Không có sự truy nhập nào ngoài giờ hành chính ngoài việc truy nhập của người quản trị nếu có. Do vậy, đường truyền không dây hoàn toàn rảnh khi hết giờ hành chính. Việc kết nối lúc này chỉ còn phục vụ cho việc quản lý. Tuy nhiên ta vẫn đảm bảo kết nối 24/24h.

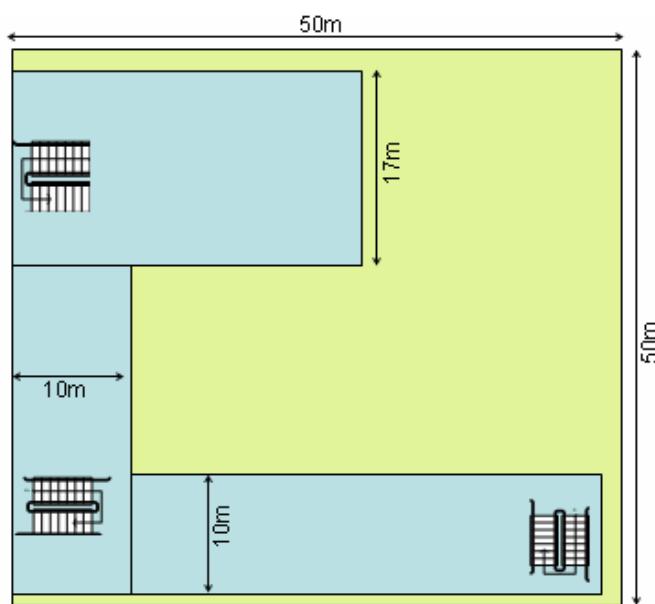
Đối với việc phủ sóng Wi-Fi phục vụ kết nối cho các Wireless Client tại khu vực Y. Qua khảo sát nhận thấy:

Về kiến trúc: Khu Y này được phân làm hai khu con, gồm một tòa nhà cao 11 tầng với diện tích 13 tầng (bao gồm hai tầng lửng) bằng nhau và bằng $17 \times 30 \text{ m}^2$ và một khu 7 tầng (bao gồm hai tầng lửng) diện tích mặt bằng theo hình chữ U với chiều dài hành lang phía mặt trong chữ U là $40+15\text{m}$. Độ cao mỗi tầng trừ hai tầng lửng ra là như nhau và bằng 3.6m (chưa tính sàn bê tông dày 0.15m), tổng chiều cao của hai tầng lửng là 5.2m . Nhìn kỹ ta sẽ thấy hệ thống hành lang ở hai khu nhà thông nhau và việc bố trí các phòng học, phòng làm việc tạo thành một hình chữ U.

Phân bố truy cập: Nhận thấy nhu cầu truy nhập tập trung cao nhất là ở các giảng đường khu vực tiền sảnh khu Y vì ở hai nơi này một là bộ mặt của trường, thường sử dụng để đón tiếp khách tham quan, liên hệ công tác với trường và một là nơi thường tập trung đông đúc để hội họp,

hội nghị thường xuyên nên cộng với hai khu này còn bao gồm tầng lửng có kiến trúc thấp, tập trung đông người, nhu cầu kết nối tại hai khu này do vậy sẽ tăng cao so với các khu vực khác. Cần chú ý nữa là khu vực tầng trệt và tầng lửng tập trung nhiều hoạt động có truy nhập Internet thường xuyên vì đây là dãy các phòng làm việc của cán bộ, thường xuyên tiếp khách đến làm việc và khu vực này còn có sân rộng là nơi tập trung nhiều người truy nhập. Khi chọn số lượng, vị trí đặt thiết bị ta cần chú ý tới đặc điểm này.

Cụ thể bố trí không gian hai toàn nhà tại khu vực này như sau:



Hình 3.21. Bố trí không gian tại khu vực

3.6.2. Xác định công nghệ, kiến trúc mạng

3.6.2.1. Cho kết nối hai mạng cục bộ lại với nhau

Với những yêu cầu sử dụng mạng như trên. Và khoảng cách giữa hai nơi khá xa cho một kết nối có dây. Nếu dùng cáp quang thì quá tốn kém và bất tiện, gây lãng phí. Còn nếu dùng các loại cáp khác thì khoảng cách đường truyền quá xa, không đảm bảo về mặt kết nối ổn định mà lại rất khó cấu hình, nâng cấp hệ thống. Dựa vào những phân tích trong phần

trước về WLAN (Xem Phần 2), dễ thấy WLAN có rất nhiều ưu điểm có thể áp dụng được ở đây: Khả năng di động tốt, độ tin cậy cao, khả năng tùy biến, lắp đặt dễ dàng, nhanh chóng, tốc độ lý thuyết đạt 54 Mbit/s ... rất thích hợp cho nhu cầu nối mạng của ta, phù hợp với yêu cầu bài toán. Chúng ta đi đến quyết định chọn kết nối không dây để kết nối hệ thống mạng ở hai nơi này lại. Vấn đề là ta phải chọn công nghệ nào trong số các công nghệ được trình bày ở trên. Ta không thể chọn mạng theo tiêu chuẩn IEEE 802.11b vì tốc độ của mạng khá chậm, sẽ không đảm bảo được yêu cầu sử dụng của mạng hiện tại. Mạng theo chuẩn IEEE 802.11a thì đảm bảo được vấn đề tốc độ nhưng công nghệ này đã cũ, ít được hỗ trợ, và tần số cao (5GHz) nên khả năng truyền xa của nó không tốt bằng mạng theo chuẩn 802.11g. Hiện nay giá cả các thiết bị đã rẻ hơn trước rất nhiều, và sẽ xuất hiện thêm nhiều chuẩn mới. Ta nên cân nhắc khi chọn thiết bị của chuẩn (802.11a/802.11b theo <http://www.vnmedia.vn>). Vì vậy ta chọn thiết bị kết nối theo chuẩn cho tốc độ truyền dữ liệu tối đa. Mặt khác hiện nay cũng còn rất nhiều thiết bị sử dụng kết nối theo chuẩn 802.11 a hoặc b, nên khi chọn thiết bị ta chọn những thiết bị có khả năng tương thích ngược, hỗ trợ cả hai chuẩn này để gia tăng tính tiện dụng của mạng để phòng có sự mở rộng kết nối sau này với một tòa nhà khác có thiết bị theo chuẩn thấp hơn.

Khoảng cách giữa hai điểm là 1,5 km, không vướng bất kỳ tòa nhà hay chướng ngại vật nào. Ta sử dụng hai cầu dẫn không dây dùng ngoài trời và hai Antenna Yagi truyền thẳng hướng phục vụ kết nối. Hai cầu dẫn không dây này kết nối trực tiếp với nhau theo kiến trúc Point-to-Point với một cầu dẫn được cấu hình hoạt động Root-mode và một cầu dẫn được cấu hình Non-root mode. Hai cầu dẫn này được nối vào Uplink của mạng trực hiện có của mỗi bên.

3.6.2.2. Cho kết nối không dây khu vực X

Từ những phân tích trên ta không thể chọn kiến trúc mạng khác kiến trúc hạ tầng (Infrastructure) để phục vụ việc kết nối của các Wireless Client được. Và kết nối nào cũng yêu cầu phải đảm bảo: dễ dàng kết nối, kết nối ổn định, ít nhiễu và tương thích cao. Trên thị trường hiện nay xu hướng các thiết bị kết nối không dây dùng chuẩn 802.11a ngày càng

hiếm, và chuẩn 802.11b cũng không nằm ngoài qui luật trên. Còn những mở rộng của chuẩn G như Wireless-G với SpeedBooster, Wireless-G với SRX của Linksys chẳng hạn thì không phải tất cả các Wireless Client đều tận dụng được khả năng này. Vả lại ta công nhận mục đích chính của các Wireless Client truy nhập mạng ở đây chủ yếu là truy nhập Internet chia sẻ với tốc độ tối đa ở Việt Nam 2 Mbit/s. Do vậy, đầu tư mạng không dây cho khu vực này với những chuẩn cho khả năng cao hơn 802.11g hiện tại sẽ gây lãng phí đầu tư. Ta chọn chuẩn 802.11g cho kết nối không dây với tốc độ 54 Mbit/s tại khu vực này. Cũng như mục trước ta cũng nên chọn thiết bị có khả năng tương thích ngược với chuẩn 802.11a/802.11b.

3.6.3. Xác định phần cứng

3.6.3.1. Cho kết nối hai mạng cục bộ lại với nhau

Đáp ứng các điều trên ta chọn thiết bị như sau:

Cisco Aironet 1300 Series Outdoor Wireless Bridge có đặc điểm kỹ thuật:

Tương thích	Với các loại cầu dẫn không dây 1300 và 350 Series của Cisco
Chuẩn không dây	802.11b hoặc 802.11g
Băng tần	Từ 2.412 đến 2.612 GHz
Điều biến không dây	<p>Với 802.11b:</p> <ul style="list-style-type: none"> - Trải phổ phân tần trực tiếp (DSSS - direct sequence spread spectrum) <ul style="list-style-type: none"> + Differential Binary Phase Shift Keying (DBPSK) at 1 Mbit/s + Differential Quadrature Phase Shift Keying (DQPSK) at 2 Mbit/s + Complementary Code Keying (CCK) at 5.5 and 11 Mbit/s <p>Với 802.11g</p> <ul style="list-style-type: none"> - OFDM – Orthogonal Frequency Divisional Multiplexing: <ul style="list-style-type: none"> + BPSK hỗ trợ 6 và 9 Mbit/s + QPSK hỗ trợ 12 và 18 Mbit/s + 16-quadrature amplitude modulation (QAM) hỗ trợ 24 và 36 Mbit/s + 64-QAM hỗ trợ 48 và 54 Mbit/s
Phương thức truy nhập đường truyền	CSMA/CA
Mã hóa/Bảo mật	WPA/WPA2/Message Integrity Check (MIC)/AES (802.11i)

Sở dĩ ta chọn thiết bị Wireless Bridge (WB) như trên đã không hỗ trợ được chuẩn 802.11a là do vấn đề kinh phí. Chuẩn 802.11a sử dụng băng tần 5GHz đã lỗi thời nhiều so với chuẩn 802.11b và chuẩn 802.11g sử dụng cùng băng tần 2.4GHz. Do khác nhau về băng tần truyền dẫn nên giá thiết bị WB hỗ trợ cả băng tần 5GHz và 2.4 GHz cao rất nhiều so với WB hỗ trợ 1 băng tần cho hai chuẩn 802.11b/g vậy nên trong đề tài đã chọn thiết bị không tương thích với chuẩn 802.11a.

Antenna Yagi truyền thẳng của Cisco System, Series 1300 AIR ANT1949 13.5dBi + thiết bị giá đỡ cho Antenna này. Đặc điểm như sau:

Tên gọi	Anten Yagi ngoài trời của Cisco AIR ANT1949
Băng tần	2,4 – 2,83 GHz
Độ khuếch đại	13,5 dBi
Đầu nối	RP-TNC
Phân cực	Dọc
Lắp đặt	Thẳng đứng/ Gắn tường
Độ dài cáp từ WB đến Antenna	0,6m

Phụ thuộc giữa khoảng cách và tốc độ truyền của ăng ten Yagi của Cisco AIR ANT-1949:

Khoảng cách	Tốc độ
29,49 km	2 Mbit/s
18,01 km	11 Mbit/s
2,27 km	54 Mbit/s

Ta còn cần chọn thêm 02 bộ khuếch đại để khuếch đại tín hiệu trước khi truyền ở mỗi đầu cầu nhằm giảm suy hao tín hiệu trong lúc truyền đảm bảo tốc độ như trong thiết kế

3.6.3.2. Cho kết nối không dây khu vực X

Tại khu vực này như đã phân tích ta sẽ chọn thiết bị lắp đặt để phủ sóng toàn bộ khu nhà với những vị trí đặc biệt đã nêu. Theo phân tích trên thì đáng chú ý nhất tại khu vực chữ U này là khu gồm có phần sân và hai tầng lửng, tiền sảnh, giảng đường A là khu vực tập trung đông nhất toàn trường. Tổng diện tích cần phủ sóng ở khu vực này là 50x50m²

tại khu vực tiền sảnh và sân cộng với diện tích sàn tầng lửng và giảng đường A. Vì vậy ta chọn Access Point Aironet 1130 của Cisco. Dựa vào đặc điểm của loại Access Point này như sau:

Chuẩn hỗ trợ	802.11a, 802.11b, 802.11g
Khả năng không giao thoa	Hỗ trợ tối đa 15 kênh không giao thoa
Số lượng Client kết nối đến	253 Client kết nối cùng lúc (lý thuyết)
Antenna tích hợp	Có
Uplink	Tương thích 802.3 10/100 BaseT Ethernet
Băng tần hỗ trợ	2.4GHz for 802.11a, 5GHz for 802.11b/g
Tuân thủ bảo mật	802.11i, WPA/WPA2, WEP with AES, TKIP

Phụ thuộc giữa khoảng cách và tốc độ truyền lý thuyết của Access Point Cisco 1130. Điều kiện môi trường trong nhà:

Tốc độ (Mbit/s)	Khoảng cách (m)	
	Chuẩn 802.11a	Chuẩn 802.11g
54	24	30
48	45	53
36	60	76
24	69	84
18	76	100
12	84	107
9	91	114
6	100	122
5.5		128
2		134
1		137

Tốc độ trên lý thuyết là vậy nhưng ta cần lưu ý là trên thực tế do sự sắp đặt thiết bị và các vật dụng khác trong tòa nhà vốn có sẽ làm hạn chế phần nào tốc độ và sự ổn định kết nối của thiết bị nối mạng. Chúng ta sẽ lắp đặt các thiết bị sao cho tại những điểm được khuyến cáo có nhiều truy nhập luôn đảm bảo tốc độ lý thuyết đạt 54Mbit/s. Và những vùng còn lại sẽ chấp nhận tốc độ chậm hơn với mức độ vừa phải. Cụ thể ở đây

ta sẽ lắp 02 Access Point (AP) phục vụ tầng trệt, sân, tiền sảnh và giảng đường A. AP sẽ được đặt cách mặt đất 5.2m AP này sẽ phục vụ được đến tầng 02 của cả hai tòa nhà với bảo đảm kết nối. Ta cần cấu hình hai AP này hoạt động ở hai kênh khác nhau để tránh giao thoa và tại một điểm bất kỳ của khu này có 02 sóng phát ra từ 02 AP khác nhau. Như vậy ta lắp theo mô hình này sẽ tận dụng được khả năng của mỗi AP và gia tăng lưu lượng kết nối lên gấp đôi, gánh vác kết nối cho nhau khi một trong hai AP bị quá tải. Tại tầng 06 của tòa nhà phía X ta lắp thêm một AP nữa. AP này sẽ phục vụ được các kết nối của phần còn lại trong tòa nhà này và các tầng trên của tòa nhà phía X. Lưu ý: Khi lắp hoàn thành các AP này ta cần dùng các công cụ kiểm tra tần số kết nối để đảm bảo chất lượng tín hiệu và không phải thực hiện các biện pháp bảo mật, quyền truy nhập hiện có trên AP để đảm bảo tất cả các Wireless Client ở những khu vực đều truy nhập được vào mạng và sử dụng Internet chia sẻ.

Ngoài ra còn có một số thiết bị phụ trợ khác đi kèm các thiết bị cơ bản trên phải có để các thiết bị này có thể vận hành được: Bộ cấp nguồn qua Ethernet, Adapter rời kèm theo AP, cá giắc đỡ Antenna, cáp Antenna, đầu nối...

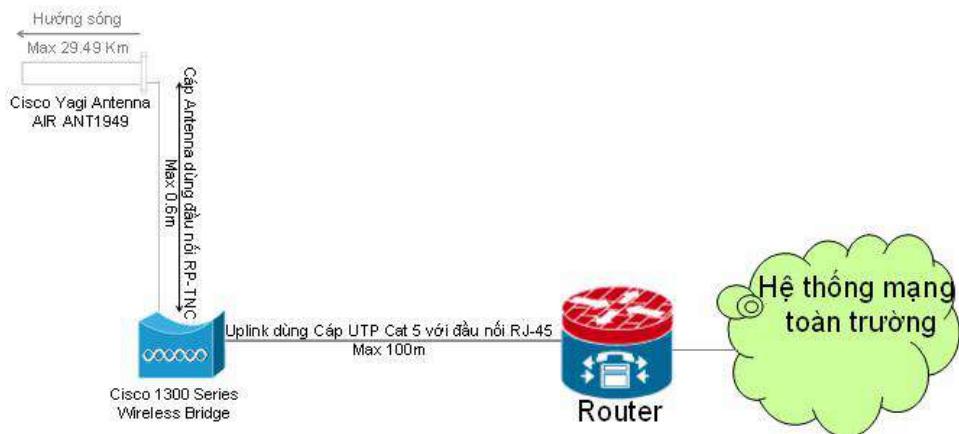
3.6.4. Thiết kế chi tiết kết nối WLAN

3.6.4.1. Sơ đồ phân bố thiết bị tại điểm X



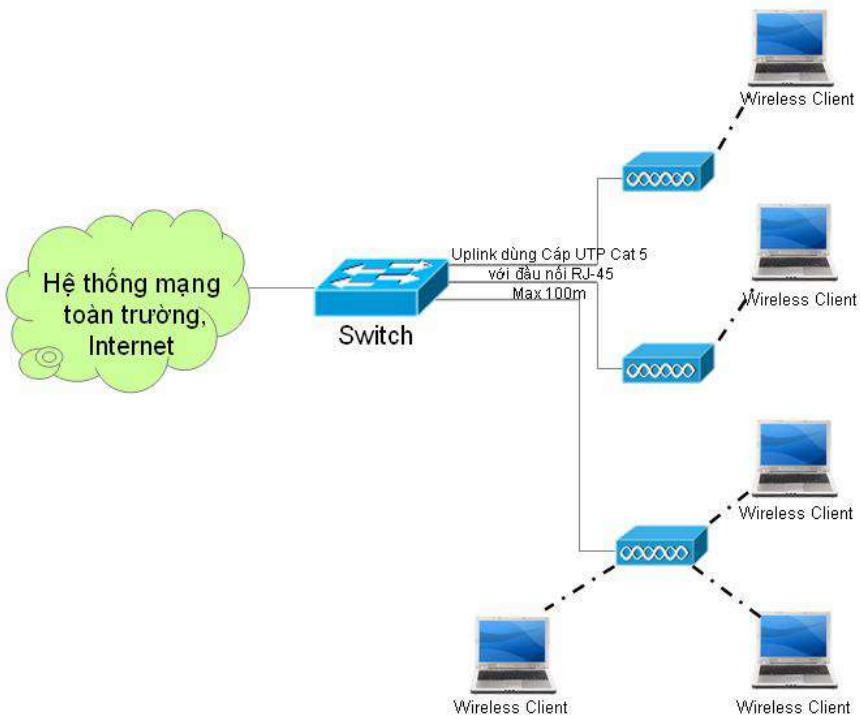
Hình 3.22. Sơ đồ phân bố thiết bị

3.6.4.2. Sơ đồ phân bố thiết bị tại điểm X



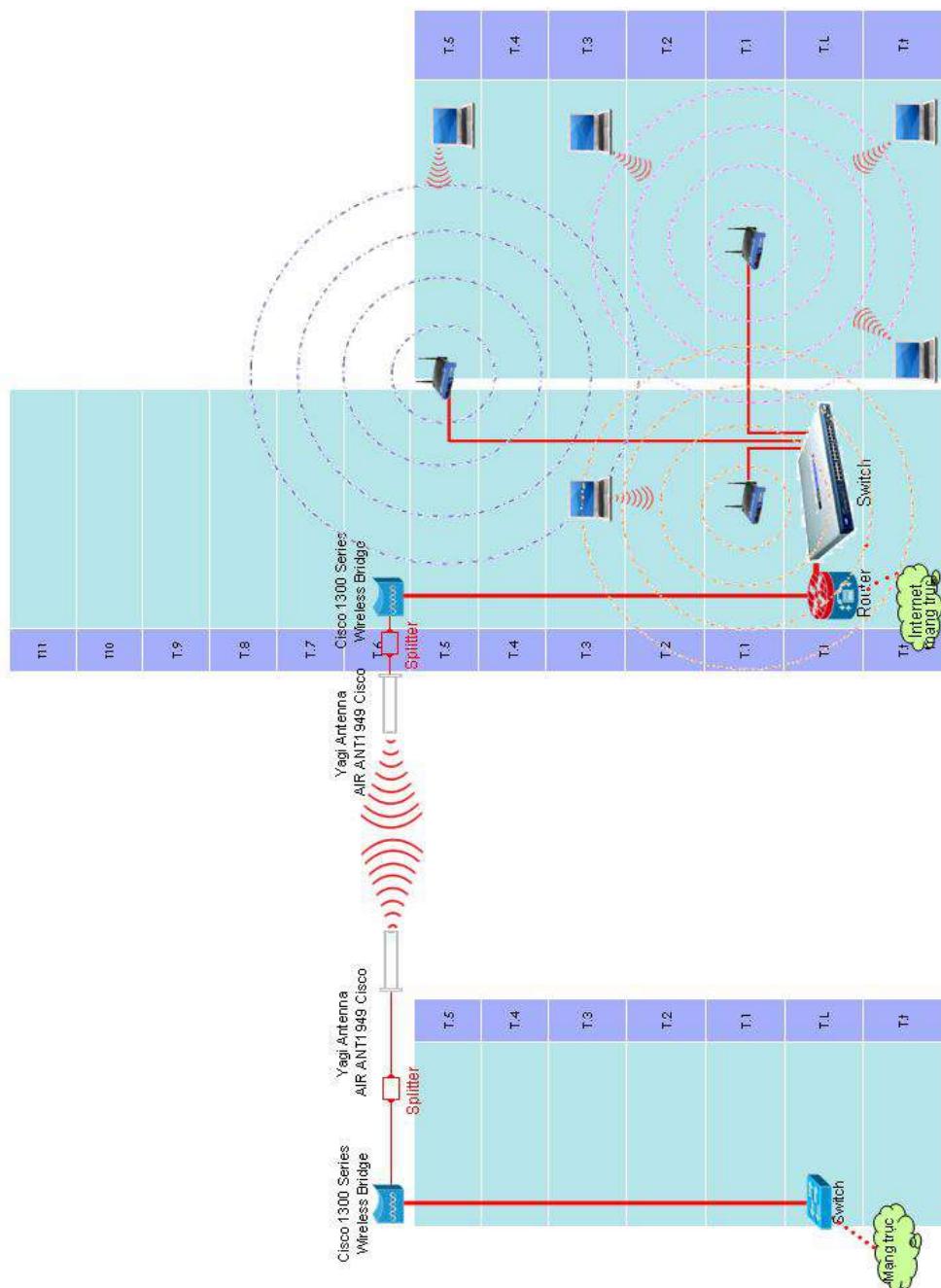
Hình 3.23. Sơ đồ phân bố thiết bị

3.6.4.3. Sơ đồ phân bố Access Point tại X



Hình 2.24. Sơ đồ phân bố Access Point

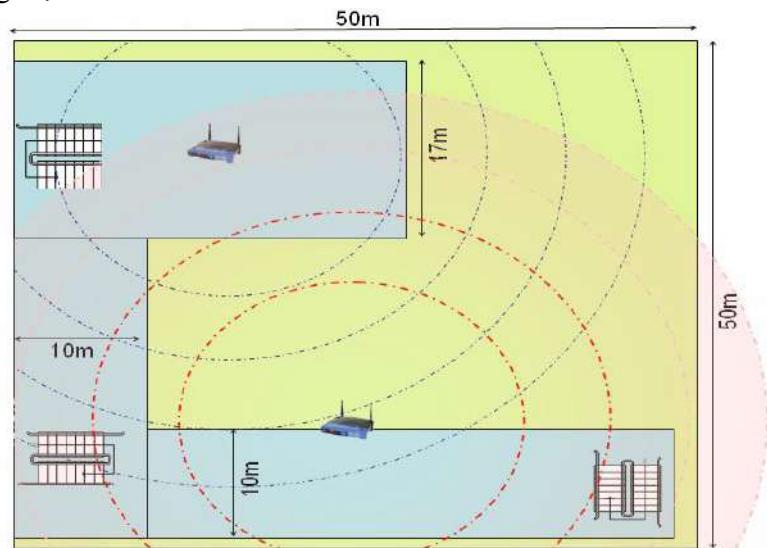
3.6.4.4. Sơ đồ mô phỏng kết nối không dây tổng thể toàn hệ thống



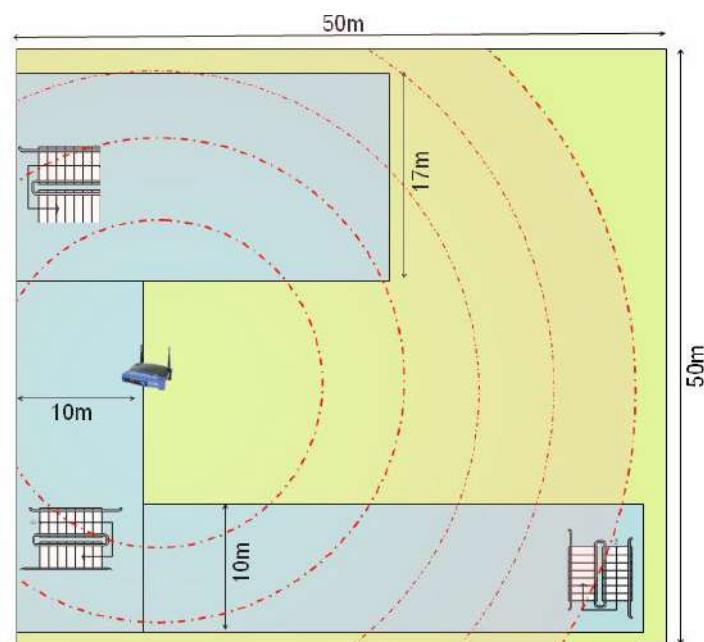
Hình 3.25. Sơ đồ phân bổ Access Point

3.6.5. Sơ đồ vị trí lắp đặt Access Point chia sẻ Internet

Tầng trệt:



Tầng 6:



Hình 3.26. Sơ đồ kết nối không dây tổng thể toàn hệ thống

Lưu ý: Vị trí đặt các Access Point này có thể được dịch chuyển qua lại tùy theo vị trí mà tại đó chất lượng phủ sóng của Access point là cao nhất.

3.6.6. Thực thi mạng WLAN

3.6.6.1. Định cấu hình hoạt động cho các thiết bị

Dựa vào các khả năng và cấu hình đã chọn lựa và mục đích sử dụng của mạng ta thực hiện cấu hình mạng để hoạt động theo yêu cầu sau:

Với kết nối giữa hai điểm sử dụng Wireless Bridge (WB) ta cấu hình theo kiến trúc Infrastructure. WB tại điểm Y ta cấu hình theo chế độ Non-Root. Ngoài ra còn chú ý các thông số: SSID, kênh truyền, tên điểm kết nối, gán địa chỉ IP tĩnh cho thiết bị, chọn công suất phát, Subnet Mask, Gateway IP, DNS Server IP... Tại điểm X cũng cấu hình tương tự, khác nhau về SSID, tên điểm ngoài ra WB tại đây ta phải cấu hình theo chế độ Root-mode Bridge để giao tiếp được với điểm Y.

Với cấu hình chia sẻ mạng Internet tại điểm X ta cũng cấu hình tương tự như cấu hình WB. Tuy nhiên, chế độ ở đây là Access Point Mode và vì tại đây chia sẻ kết nối cho tất cả các đối tượng sử dụng tại khu vực nên ta cấu hình cho phép AP cấp phát IP động cho Wireless Client.

3.6.6.2. Cài đặt các lựa chọn bảo mật trên mạng

Tại hai điểm này rất chú trọng bảo mật vì vậy ta cấm tất cả các kết nối khác đến hệ thống dùng địa chỉ MAC, chỉ cho phép kết nối từ/đến địa chỉ MAC của điểm X. Cung cấp khóa WEP mã hóa dữ liệu, đồng ý sử dụng chuẩn xác thực 802.1x, và WPA.

Tại kết nối chia sẻ Internet với lý do cho phép tất cả các kết nối đến nên ta không thiết đặt bất kỳ hạn chế kết nối nào, mọi Wireless Client đều có thể kết nối vào mạng và dùng Internet được.

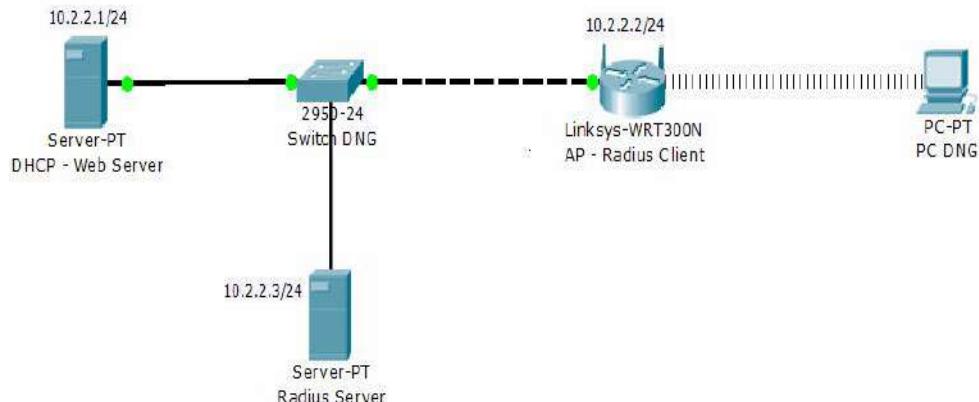
Lưu ý: Vì các thiết bị trên hoạt động trên băng tần 24.12 GHz đến 2.612 GHz là dài tần bắt buộc phải đăng ký hoạt động (theo Nghị định số 24/2004/NĐ-CP ngày 14/01/2004 của Chính phủ quy định chi tiết thi hành một số điều của Pháp lệnh Bưu chính, Viễn thông về tần số vô

tuyến điện) nên khi lắp đặt đưa vào sử dụng ta phải đăng ký sử dụng tần số với Cục quản lý tần số để đảm không bị chiếm dụng, gây nhiễu đường truyền.

3.7. BÀI TẬP ÚNG DỤNG

Mục tiêu: Rèn luyện kỹ năng thực hành mô phỏng thiết kế WLAN trên Packet tracer.

Yêu cầu: Sinh viên cần chuẩn bị lý thuyết về các chuẩn IEEE 802.11i, IEEE 802.1x. Sử dụng phần mềm Packet Tracer v5.3, hãy thiết kế một mạng WLAN như sau:



Hình 3.27. Cấu hình bảo mật WEP, WPA-Enterprise, WPA-PSK, WPA-Enterprise, WPA2-PSK.

3.8. CÂU HỎI ÔN TẬP

Câu 1: Các chuẩn mạng WLAN nào được sử dụng phổ biến nhất ở Việt Nam? Cho ví dụ và trình bày đặc điểm?

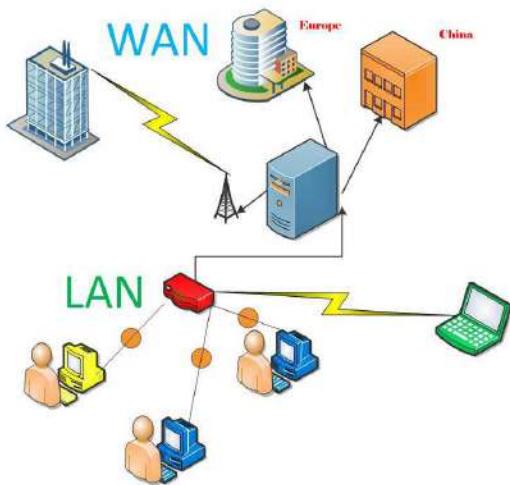
Câu 2: Trình bày quá trình chứng thực 802.1x – EAP.

Câu 3: Theo bạn thì hiện nay giải pháp bảo mật nào dành cho WLAN là tốt nhất? Tạo sao?

Câu 4: Theo bạn thì giải pháp bảo mật nào là tốt nhất để triển khai cho mạng không dây trong gia đình và các doanh nghiệp nhỏ?

Chương 4

THIẾT KẾ MẠNG DIỆN RỘNG



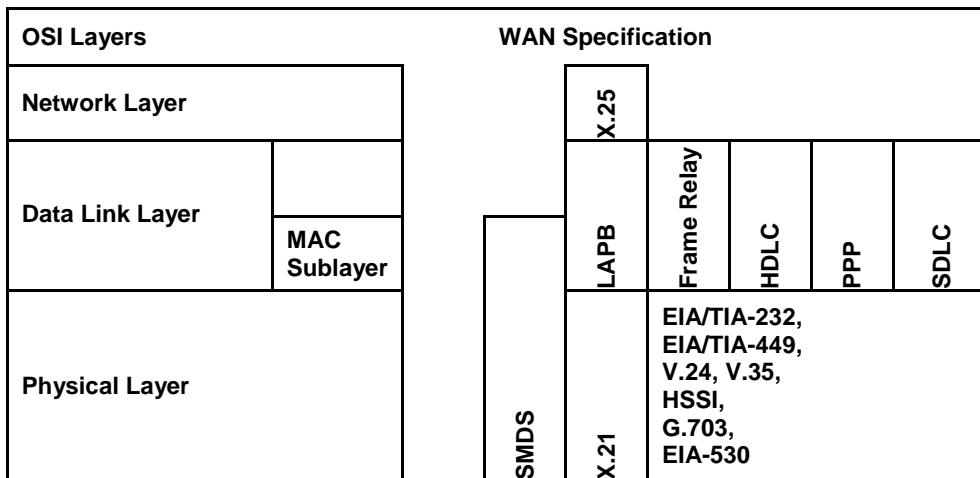
Giới thiệu các đặc trưng kỹ thuật cơ bản về mạng diện rộng WAN, các công nghệ kết nối WAN và phương pháp thiết kế WAN. Cuối chương là bài tập ứng dụng và bài tập tổng hợp về thiết kế mạng WAN.

4.1. GIỚI THIỆU WAN

Mạng diện rộng (Wide Area Network - WAN) là mạng kết nối nhiều máy tính, nhiều mạng LAN, mạng MAN trong phạm vi một quốc gia hay nhiều quốc gia trong một châu lục. Mạng WAN lớn nhất và điển hình nhất chính là mạng Internet.

WAN là một mạng truyền dữ liệu trải dài trên một khu vực địa lý rộng lớn và thường sử dụng các phương tiện và dịch vụ của các nhà cung cấp như các công ty điện thoại.

Công nghệ WAN thường nằm ở 3 lớp dưới của mô hình OSI: Lớp vật lý, lớp liên kết dữ liệu và lớp mạng (Network Layer).



Hình 4.1. Mối liên hệ giữa WAN và OSI

4.2. CÁC LỢI ÍCH VÀ CHI PHÍ KHI KẾT NỐI WAN

Xã hội càng phát triển, nhu cầu trao đổi thông tin càng đòi hỏi việc xử lý thông tin phải được tiến hành một cách nhanh chóng và chính xác. Sự ra đời và phát triển không ngừng của ngành công nghệ thông tin đã góp phần quan trọng vào sự phát triển chung đó. Với sự ra đời máy tính, việc xử lý thông tin hơn bao giờ hết đã trở nên đặc biệt nhanh chóng với hiệu suất cao. Đặc biệt hơn nữa, người ta đã nhận thấy việc thiết lập một hệ thống mạng diện rộng - WAN và truy nhập từ xa sẽ làm gia tăng gấp bội hiệu quả công việc nhờ việc chia sẻ và trao đổi thông tin được thực hiện một cách dễ dàng, tức thì (thời gian thực). Khi đó khoảng cách về mặt địa lý giữa các vùng được thu ngắn lại. Các giao dịch được diễn ra gần như tức thì, thậm chí ta có thể tiến hành các hội nghị từ xa, các ứng dụng đa phương tiện...

Nhờ có hệ thống WAN và các ứng dụng triển khai trên đó, thông tin được chia sẻ và xử lý bởi nhiều máy tính dưới sự giám sát của nhiều người đảm bảo tính chính xác và hiệu quả cao.

Phần lớn các cơ quan, các tổ chức và cả các cá nhân đều đã nhận thức được tính ưu việt của xử lý thông tin trong công việc thông qua mạng máy tính so với công việc văn phòng dựa trên giấy tờ truyền thống.

Do vậy, sớm hay muộn, các tổ chức, cơ quan đều cố gắng trong khả năng có thể, đều cố gắng thiết lập một mạng máy tính, đặc biệt là WAN để thực hiện các công việc khác nhau.

Với sự phát triển nhanh chóng của công nghệ thông tin, công nghệ viễn thông và kỹ thuật máy tính, mạng WAN và truy nhập từ xa dần trở thành một môi trường làm việc gần như là bắt buộc khi thực hiện yêu cầu về hội nhập quốc tế. Trên WAN người dùng có thể trao đổi, xử lý dữ liệu truyền thống thuận túy song song với thực hiện các kỹ thuật mới, cho phép trao đổi dữ liệu đa phương tiện như hình ảnh, âm thanh, điện thoại, họp hội nghị,... qua đó tăng hiệu suất công việc, và làm giảm chi phí quản lý cũng như chi phí sản xuất khác.

Đặc biệt đối với các giao dịch Khách – Chủ (Client – Server), hệ thống kết nối mạng diện rộng từ các LAN của văn phòng trung tâm (NOC) tới LAN của các chi nhánh (POP) sẽ là hệ thống trao đổi thông tin chính của cơ quan hay tổ chức. Nó giúp tăng cường và thay đổi về chất công tác quản lý và trao đổi thông tin, tiến bước vững chắc tới một nền kinh tế điện tử (e-commerce), chính phủ điện tử (e-government) trong tương lai không xa.

4.3. NHỮNG ĐIỀM CẦN CHÚ Ý KHI THIẾT KẾ WAN

Khi thiết kế WAN chúng ta cần chú ý đến ba yếu tố: *Môi trường, yêu cầu kỹ thuật và bảo mật*.

4.3.1. Môi trường

Các yếu tố liên quan đến mục tiêu thiết kế như môi trường của WAN, các yêu cầu về năng lực truyền thông của WAN (hiệu năng mạng), khả năng cung cấp động và các ràng buộc về băng thông, thoả mãn các đặc trưng của dữ liệu cần trao đổi trên WAN, đặc biệt các loại dữ liệu cần đảm bảo chất lượng dịch vụ như dữ liệu đa phương tiện, dữ liệu đòi hỏi đáp ứng thời gian thực như giao dịch về tài chính.

Môi trường của WAN ở đây được thể hiện qua các tham số như số lượng các trạm làm việc, các máy chủ chạy các dịch vụ, và vị trí đặt chúng, các dịch vụ và việc đảm bảo chất lượng các dịch vụ đang chạy trên WAN. Việc chọn số lượng và vị trí đặt các máy chủ, các máy trạm

trong WAN liên quan nhiều đến vấn đề tối ưu các luồng dữ liệu truyền trên mạng. Chẳng hạn khu vực nào có nhiều trạm làm việc, chúng cần thực hiện nhiều giao dịch với một hay nhiều máy chủ nào đó, thì các máy chủ đó cũng cần phải đặt trong khu vực đó, nhằm giảm thiểu dữ liệu truyền trên WAN.

Yêu cầu về hiệu năng cần được quan tâm đặc biệt khi thiết kế các WAN yêu cầu các dịch vụ đòi hỏi thời gian thực như VoIP, hay hội nghị truyền hình, giao dịch tài chính,...

Khi đó các giới hạn về tốc độ đường truyền, độ trễ,... cần được xem xét kỹ, nhất là khi dùng vệ tinh, vô tuyến,...

Các đặc trưng của dữ liệu cũng cần được quan tâm để nhằm giảm thiểu chi phí về băng thông khi kết nối WAN. Các đặc trưng dữ liệu để cập ở đây là dữ liệu client/server, thông điệp, quản trị mạng,... băng thông nào đảm bảo chất lượng dịch vụ?

4.3.2. Các yêu cầu kỹ thuật

Năm yêu cầu cần xem xét khi thiết kế WAN đó là: khả năng mở rộng, dễ triển khai, dễ phát hiện lỗi, dễ quản lý, hỗ trợ đa giao thức.

Khả năng mở rộng thể hiện ở vấn đề có thể mở rộng, bổ sung thêm dịch vụ, tăng số lượng người dùng, tăng băng thông mà không bị ảnh hưởng gì đến cấu trúc hiện có của WAN và các dịch vụ đã triển khai trên đó.

Tính dễ triển khai thể hiện bằng việc thiết kế phân cấp, mô-đun hoá, khôi hoá ở mức cao. Các khôi, các mô-đun của WAN độc lập một cách tương đối, quá trình triển khai có thể thực hiện theo từng khôi, từng mô-đun.

Tính dễ phát hiện lỗi là một yêu cầu rất quan trọng, vì luồng thông tin vận chuyển trên WAN rất nhạy cảm cho các tổ chức dùng WAN. Vậy việc phát hiện và cô lập lỗi cần phải thực hiện dễ và nhanh chóng với quản trị hệ thống.

Tính dễ quản lý đảm bảo cho người quản trị mạng làm chủ được toàn bộ hệ thống mạng trong phạm vi địa lý rộng hoặc rất rộng.

Hỗ trợ đa giao thức có thể thực hiện được khả năng tích hợp tất cả các dịch vụ thông tin và truyền thông cho một tổ chức trên cùng hạ tầng

công nghệ thông tin, nhằm giảm chi phí thiết bị và phí truyền thông, giảm thiểu tài nguyên con người cho việc vận hành hệ thống.

4.3.3. Bảo mật

Việc đảm bảo an ninh, xây dựng chính sách an ninh và thực hiện an ninh thế nào phải được tính đến ngay từ bước thiết kế.

4.4. MỘT SỐ CÔNG NGHỆ KẾT NỐI WAN

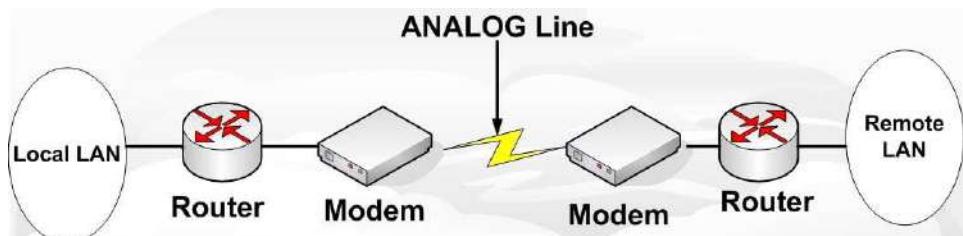
4.4.1. Mạng chuyển mạch kêt

Mạng chuyển mạch kêt (Circuit Switching Network) thực hiện việc liên kết giữa hai điểm nút qua một đường nối tạm thời hay giành riêng giữa điểm nút này và điểm nút kia. Đường nối này được thiết lập trong mạng thể hiện dưới dạng cuộc gọi thông qua các thiết bị chuyển mạch.

Một ví dụ của mạng chuyển mạch kêt là hoạt động của mạng điện thoại, các thuê bao khi biết số của nhau có thể gọi cho nhau và có một đường nối vật lý tạm thời được thiết lập giữa hai thuê bao.

Với mô hình này mọi nút mạng có thể kết nối với bất kỳ một nút khác. Thông qua những đường nối và các thiết bị chuyên dùng người ta có thể tạo ra một liên kết tạm thời từ nơi gửi tới nơi nhận, kết nối này duy trì trong suốt phiên làm việc và được giải phóng ngay sau khi phiên làm việc kết thúc. Để thực hiện một phiên làm việc cần có các thủ tục đầy đủ cho việc thiết lập liên kết trong đó có việc thông báo cho mạng biết địa chỉ của nút gửi và nút nhận. Hiện nay có 2 loại mạng chuyển mạch là chuyển mạch tương tự (analog) và chuyển mạch số (digital).

4.4.1.1. Chuyển mạch tương tự (Analog)

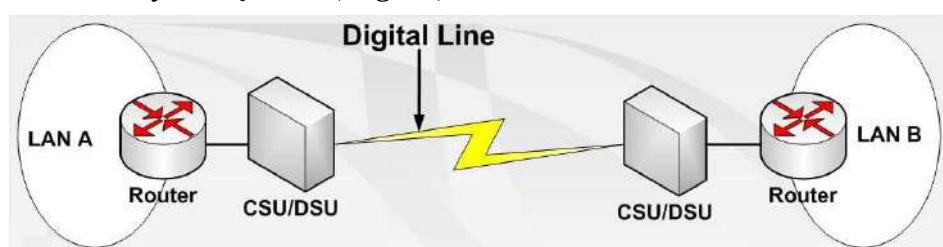


Hình 4.2. Analog Circuit Switching

Việc chuyển dữ liệu qua mạng chuyển mạch tương tự được thực hiện qua mạng điện thoại. Các trạm trên mạng sử dụng một thiết bị có tên là modem ("MODulator" and "DEModulator"), thiết bị này sẽ chuyển các tín hiệu số từ máy tính sang tín hiệu tương tự có thể truyền dữ liệu đi trên các kênh điện thoại và ngược lại biến tín hiệu dạng tương tự thành tín hiệu số.

Một minh họa kết nối dùng mạng chuyển mạch là kết nối qua mạng điện thoại PSTN, hay còn gọi là kết nối quay số (dial-up).

4.4.1.2. Chuyển mạch số (Digital)



Hình 4.3. Digital Circuit Switching

4.4.1.2.1. Kênh thuê riêng (Leased Lines)

Leased line là một kết nối viễn thông đối xứng theo hai chiều truyền dữ liệu lên và xuống, được sử dụng để kết nối hai điểm truyền dữ liệu với nhau. Không giống như dịch vụ PSTN truyền thống, các kết nối này không có số điện thoại cho mỗi kết nối, mỗi tuyến kết nối sử dụng một dạng kết nối theo dạng permanent.

Các dịch vụ viễn thông có thể được triển khai trên kết nối này như: điện thoại, dữ liệu, kết nối Internet, truyền hình...

Leased line có nhiều lựa chọn băng thông khác nhau phụ thuộc vào mức cần thiết của khách hàng với băng thông $n \times 64$ kbit/s với $n=1,..,31$.

Hiện nay, Leased Line được phân làm hai lớp chính là Tx (theo chuẩn của Mỹ và Canada) và Ex (theo chuẩn của châu Âu, Nam Mỹ và Mê-hi-cô), x là mã số chỉ băng thông (bandwidth) của kết nối. Thông số kỹ thuật của các đường truyền Tx và Ex được liệt kê trong bảng dưới.

Bảng 4.1. Thông số kỹ thuật của các đường Tx

Loại kênh	Thông lượng	Ghép kênh
T0	56 kbit/s	1 đường thoại
T1	1.544 Mbit/s	24 đường T0
T2	6.312 Mbit/s	4 đường T1
T3	44.736 Mbit/s	28 đường T1
T4	274.176 Mbit/s	168 đường T1

T0/E0 là tương đương với một kênh truyền thoại đơn lẻ, T0 hoạt động ở tốc độ 56 kbit/s và E0 hoạt động ở tốc độ 64 kbit/s.

Dịch vụ Leased line truyền thống được phân chia thành hai dạng chính

- Đường truyền dành riêng (Dedicate line): là một kết nối dạng trực tiếp và được sử dụng với mục đích dành riêng cho một dịch vụ xác định như điện thoại hoặc Internet.
- Đường truyền riêng (Private line): là một kết nối được sử dụng với mục đích cung cấp tuyến kết nối riêng cho hai điểm truyền thông với nhau. Kết nối này là một trường hợp riêng của Dedicate line, thông thường có thể là các tunnel chạy chung trong một tuyến truyền dẫn dung lượng lớn.

Các lợi ích của dịch vụ Leased-line

- Sử dụng dịch vụ Leased-line, khác hàng có thể triển khai các hệ thống mạng viễn thông và Internet riêng cho đơn vị mình. Các dịch vụ phổ biến bao gồm: DNS, mail, web, portal,
- Kênh truyền của dịch vụ này là kênh truyền riêng, do vậy không bị ảnh hưởng của các yếu tố khác trong hệ thống mạng gây nên. Các chỉ tiêu và tham số kỹ thuật luôn được đảm bảo ở chất lượng tốt nhất.
- Không giới hạn về mặt thời gian, 24h/24h và 7 ngày/tuần.
- Không bị giới hạn về số user truy nhập Internet, chỉ phụ thuộc vào tốc độ của đường leased line .

- Kết nối trỏ nêu phô biến với mọi user trong mạng LAN của bạn, gỡ bỏ các modem và đường điện thoại phức tạp không cần thiết cho mỗi người sử dụng Internet.
- Giám sát và quản lý kết nối có thể được thực hiện bởi nhà cung cấp dịch vụ.
- Chuyên nghiệp hóa đội ngũ Công nghệ thông tin và Viễn thông của doanh nghiệp.

4.4.1.2.2. Công nghệ xDSL

Giới thiệu:

Công nghệ đường dây thuê bao số xDSL (Digital Subscribers Line) cho phép tận dụng miềù tàn số cao để truyền số liệu tốc độ cao trên đôi dây cáp điện thoại thông thường. Modem xDSL biến đổi tín hiệu của người sử dụng thành các tín hiệu phù hợp với đường truyền DSL, có cấu trúc dữ liệu riêng, mã đường dây riêng và một số tín hiệu thông tin điều khiển. Công nghệ đường dây thuê bao số được tích hợp đầu tiên trong mạng tích hợp số ISDN (Integrated Services Digital Network) với tốc độ cơ bản BRI 144 bit/s. Nhiều phiên bản xDSL sau này được lấy từ thực tế của ISDN DSL. Các thế hệ DSL sau này được cải tiến về công suất, cách thức hoạt động và khả năng cung cấp dịch vụ. Tốc độ truyền tải đã phát triển từ 1,5 Mbit/s đến 2 Mbit/s trong công nghệ HDSL, 8 Mbit/s trong công nghệ ADSL và 52 Mbit/s trong công nghệ VDSL.

Công nghệ DSL đáp ứng được các yêu cầu ứng dụng đa phương tiện của người sử dụng, hiệu suất và độ tin cậy cao, rất kinh tế giá cước rẻ.

Tổng quan về họ công nghệ xDSL

IDS (ISDN DSL): Công nghệ đường dây thuê bao số truy nhập mạng tích hợp đa dịch vụ số ISDN sử dụng các kênh đối xứng BRI (128 kbit/s hoặc 144 kbit/s) kết hợp thành một kênh truyền dữ liệu giữa bộ định tuyến và máy tính của khách hàng. DSL làm việc với tốc độ 160 kbit/s tương ứng với tải tin là 144 kbit/s (2B+D). Trong IDS kết nối với tổng đài trung tâm bằng một kết cuối đường dây LT (Line Termination) và kết

nối thuê bao bằng thiết bị đầu cuối mạng NT (Network Termination). Công nghệ ADSL truyền theo chế độ song công và sử dụng kỹ thuật triệt tiếng vọng. Phần lớn các dạng IDSL làm việc với ISDN NT tiêu chuẩn ở đầu cuối khách hàng của đường dây. Do đó, IDSL chuyển mạch nội hạt ISDN được thay thế bởi bộ định tuyến gói. Cấu hình này được sử dụng cho Internet.

HDSL (High Data Rate DSL): Có khả năng truyền song công 1,544Mbit/s hoặc 2,048 Mbit/s trên đường dây điện thoại. HDSL truyền tin cậy với tỷ lệ lỗi bit từ 10^{-9} đến 10^{-10} . Hệ thống HDSL DS-1 (1,544 Mbit/s) sử dụng 2 đôi dây mỗi đôi dây truyền 768 Kbit/s trên mỗi hướng. HDSL E1 (2,048 Mbit/s) có thể lựa chọn sử dụng 2 hoặc 3 đôi dây, mỗi đôi dây sử dụng hoàn toàn song công. HDSL 2,048 Mbit/s 3 đôi dây sử dụng bộ thu phát giống bộ thu phát hệ thống 1,544 Mbit/s. Mạch vòng HDSL 2,048 Mbit/s có thể có mạch rẽ nhưng không cân bằng. Tiêu chuẩn HDSL2 có tốc độ bit và độ dài mạch vòng như HDSL thế hệ thứ nhất, chỉ khác là sử dụng một đôi dây thay vì 2 đôi dây. HDSL2 có kỹ thuật mã hóa cao và điều chế phức tạp hơn. Lựa chọn tần số phát và thu cho HDSL2 để chống xuyên âm.

SDSL (Single Pair DSL): Truyền đôi xứng với tốc độ 784 kbit/s trên một đôi dây, ghép thoại và số liệu trên cùng một đường dây, sử dụng mã 2B1Q. Công nghệ này chưa có tiêu chuẩn thống nhất nên chưa được phổ biến cho các dịch vụ có tốc độ cao. SDSL mới chỉ ứng dụng truy nhập trang WEB, tải dữ liệu và thoại với tốc độ 128 kbit/s, khoảng cách nhỏ hơn 6,7 Km và tốc độ tối đa là 1024 kbit/s trong khoảng 3,5 Km.

VDSL (Very High Data Rate DSL): Sử dụng mạch vòng từ tổng đài trung tâm (CO) đến khách hàng và các bộ ghép kênh phân phối. Tiêu chuẩn kỹ thuật VDSL được phát triển từ nhóm T1E1.4 mô tả các tốc độ và khoảng cách từ đơn vị mạng quang ONU tới thuê bao. Cáp từ mạng cho tới các ONU có thể được nối trực tiếp tới ONU theo hình tròn hoặc bộ tách quang thụ động. Các ứng dụng của VDSL hỗ trợ đồng thời tất cả những ứng dụng thoại, dữ liệu và video. Đặc biệt VDSL hỗ trợ truyền

hình tốc độ cao (HDTV), các ứng dụng máy tính tiên tiến. Tính đối xứng của VDSL cung cấp tốc độ dữ liệu 2 chiều lên tới 26 Mbit/s cho các khu vực không có cáp quang nối tới.

ADSL (Asymmetric Digital Subscriber Line): ADSL là công nghệ đường dây thuê bao số không đối xứng được phát triển cho nhu cầu truy nhập Internet tốc độ cao, các dịch vụ trực tuyến, video, ... ADSL cung cấp tốc độ truyền tới 8 Mbit/s đường xuống (download) và 16 đến 640 kbit/s đường lên (upload). Ưu điểm nổi bật của ADSL là cho phép người sử dụng sử dụng đồng thời 1 đường dây thoại cho cả 2 dịch vụ thoại và số liệu. Vì ADSL truyền ở miền tần số cao (4400Hz → 1,1MHz) không ảnh hưởng đến tín hiệu thoại. Các bộ lọc được đặt ở 2 đầu mạch vòng tách tín hiệu thoại và số liệu theo mỗi hướng. Một loại ADSL mới gọi là ADSL “Lite” hay ADSL không sử dụng bộ lọc chủ yếu cho các ứng dụng truy nhập internet tốc độ cao. Kỹ thuật này không đòi hỏi bộ lọc phía thuê bao nên giá thành thiết bị và chi phí lắp đặt giảm đi tuy nhiên tốc độ đường xuống chỉ còn 1,5 Mbit/s.

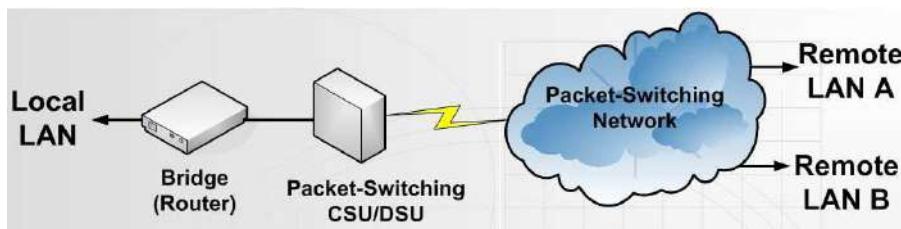
ADSL2 và ADSL2+: ADSL2 được chuẩn hóa trong ITU G.992.3, G.992.4 ADSL2+ được chuẩn hóa trong ITU-T G.925.5 là thế hệ thứ 3 của ADSL, phát triển dựa trên nền tảng ADSL và ADSL2 nên có đầy đủ đặc trưng của ADSL và ADSL2. ADSL2 và ADSL2+ bổ sung nhiều tính năng mới cho các ứng dụng, dịch vụ và tiến trình triển khai mới so với ADSL chuẩn. Công nghệ ADSL2+ đáp ứng các yêu cầu tốc độ cao, tốc độ đường lên là 1,2 Mbit/s và tốc độ đường xuống là 24 Mbit/s, băng thông rộng lên đến 2,208 MHz.

Bảng 4.2. Đặc điểm của họ công nghệ xDSL

Công nghệ	Tốc độ	Khoảng cách	Số đôi dây đồng
IDSL	144 Mbit/s đối xứng	5 km	1 đôi
HDSL	1,544 Mbit/s đối xứng 2,048 Mbit/s đối xứng	3,6 km → 4,5 km	2 đôi 3 đôi
HDSL2	1,544 Mbit/s đối xứng	3,6 km → 4,5 km	2 đôi

	2,048 Mbit/s đối xứng		3 đôi
SDSL	768 Kbit/s đối xứng 1,544 Mbit/s hoặc 2,048 Mbit/s một chiều	3 km 7 km	1 đôi
ADSL	1,5 → 8 Mbit/s đường xuống 1,544 Mbit/s đường lên	≤ 5 km	1 đôi
VDSL	26 Mbit/s đối xứng 13 → 52 Mbit/s đường xuống 1,5 → 2,3 Mbit/s đường lên	300 m → 1,5 km (tùy tốc độ)	1 đôi

4.4.2. Mạng chuyển mạch gói



Hình 4.4. Mô hình kết nối WAN dùng chuyển mạch gói

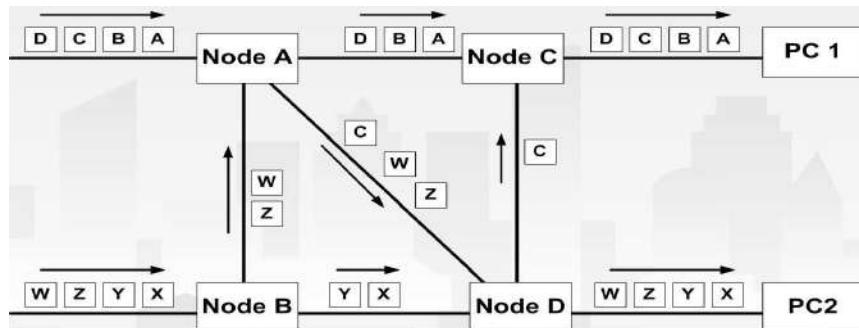
Mạng chuyển mạch gói (Packet Switching Network) hoạt động theo nguyên tắc sau: Khi một trạm trên mạng cần gửi dữ liệu nó cần phải đóng dữ liệu thành từng gói tin, các gói tin đó được đi trên mạng từ nút này tới nút khác tới khi đến được đích. Do việc sử dụng kỹ thuật trên nên khi một trạm không gửi tin thì mọi tài nguyên của mạng sẽ dành cho các trạm khác, do vậy mạng tiết kiệm được các tài nguyên và có thể sử dụng chúng một cách tốt nhất.

Người ta chia các phương thức chuyển mạch gói ra làm 2 phương thức:

- Phương thức chuyển mạch gói theo sơ đồ rời rạc.
- Phương thức chuyển mạch gói theo đường đi xác định.

Với phương thức chuyển mạch gói theo sơ đồ rời rạc các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ nơi gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xem đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin về mạng mà nút đó có. Việc truyền theo

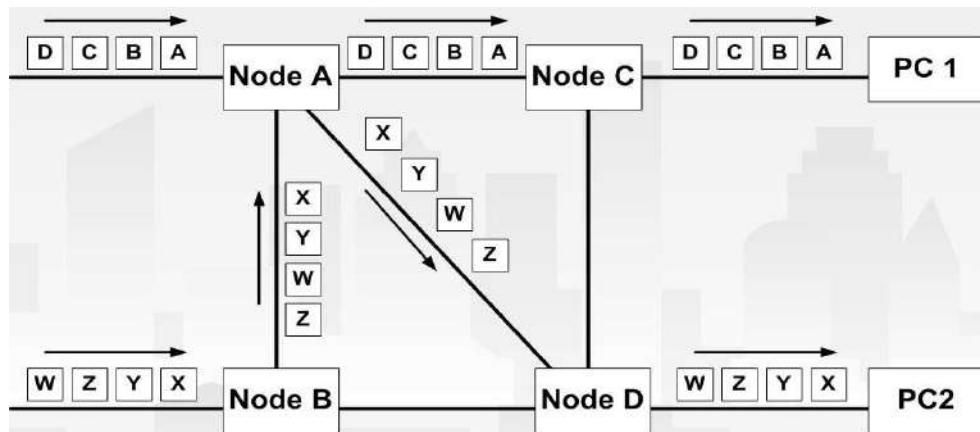
phương thức này cho ta sự mềm dẻo nhất định do đường đi với mỗi gói tin trở nên mềm dẻo tuy nhiên điều này yêu cầu một số lượng tính toán rất lớn tại mỗi nút nên hiện nay phần lớn các mạng chuyển sang dùng phương chuyển mạch gói theo đường đi xác định.



Hình 4.5. Phương thức sơ đồ rời rạc

4.4.2.1. Chuyển mạch gói theo đường đi xác định

Trước khi truyền dữ liệu thì một đường đi (đường đi ảo) được thiết lập giữa trạm gửi và trạm nhận thông qua các nút của mạng. Đường đi này mang số hiệu phân biệt với các đường đi khác, sau đó các gói tin được gửi đến đích theo đường đã thiết lập, các gói tin mang số hiệu của đường ảo để có thể được nhận biết khi qua các nút. Điều này khiến cho việc tính toán đường đi cho phiên liên lạc chỉ cần thực hiện một lần.



Hình 4.6. Phương thức đường đi xác định

4.4.2.2. Kết nối dùng ATM (Asynchronous Transfer Mode)

Giới thiệu về công nghệ ATM

- Mạng ATM (Cell relay), hiện nay kỹ thuật Cell Relay dựa trên phương thức truyền thông không đồng bộ (ATM) có thể cho phép thông lượng hàng trăm Mbit/s. Đơn vị dữ liệu dùng trong ATM được gọi là tế bào (cell). Các tế bào trong ATM có độ dài cố định là 53 bytes, trong đó 5 bytes dành cho phần chứa thông tin điều khiển (cell header) và 48 bytes chứa dữ liệu của tầng trên.
- Trong kỹ thuật ATM, các tế bào chứa các kiểu dữ liệu khác nhau được ghép kênh tới một đường dẫn chung được gọi là đường dẫn ảo (virtual path). Trong đường dẫn ảo đó có thể gồm nhiều kênh ảo (virtual channel) khác nhau, mỗi kênh ảo được sử dụng bởi một ứng dụng nào đó tại một thời điểm.
- ATM đã kết hợp những đặc tính tốt nhất của dạng chuyển mạch liên tục và dạng chuyển mạch gói, nó có thể kết hợp dài thông linh hoạt và khả năng chuyển tiếp cao tốc và có khả năng quản lý đồng thời dữ liệu số, tiếng nói, hình ảnh và multimedia tương tác.
- Mục tiêu của kỹ thuật ATM là nhằm cung cấp một mạng dồn kênh, và chuyển mạch tốc độ cao, độ trễ nhỏ đáp ứng cho các dạng truyền thông đa phương tiện (multimedia).
- Chuyển mạch cell cần thiết cho việc cung cấp các kết nối đòi hỏi băng thông cao, tình trạng tắc nghẽn thấp, hỗ trợ cho lớp dịch vụ tích hợp lưu thông dữ liệu âm thanh hình ảnh. Đặc tính tốc độ cao là đặc tính nổi bật nhất của ATM.
- ATM sử dụng cơ cấu chuyển mạch đặc biệt: Ma trận nhị phân các thành phần chuyển mạch (a matrix of binary switching elements) để vận hành lưu thông. Khả năng vô hướng (scalability) là một đặc tính của cơ cấu chuyển mạch ATM. Đặc tính này tương phản trực tiếp với những gì diễn ra khi các trạm cuối được thêm vào một thiết bị liên mạng như router. Các router có năng suất tổng cố định được chia cho các trạm cuối có kết nối với chúng. Khi số lượng trạm cuối gia tăng, năng suất của router tương thích cho trạm cuối thu nhỏ lại. Khi cơ cấu ATM mở rộng, mỗi thiết bị thu

trạm cuối, băng con đường của chính nó đi qua bộ chuyển mạch bằng cách cho mỗi trạm cuối băng thông chỉ định. Băng thông rộng được chỉ định của ATM với đặc tính có thể xác nhận khiến nó trở thành một kỹ thuật tuyệt hảo dùng cho bất kỳ nơi nào trong mạng cục bộ của doanh nghiệp.

- Như tên gọi của nó chỉ rõ, kỹ thuật ATM sử dụng phương pháp truyền không đồng bộ (Asynchronous) các tế bào từ nguồn tới đích của chúng. Trong khi đó, ở tầng vật lý người ta có thể sử dụng các kỹ thuật truyền thông đồng bộ như SDH (hoặc SONET – Synchronous Optical Network).
- Nhận thức được vị trí chưa thể thay thế được (ít nhất cho đến những năm đầu của thế kỷ XXI) của kỹ thuật ATM, hầu hết các hãng không lò về máy tính và truyền thông như IBM, ATT, Digital, Hewlett - Packard, Cisco Systems, Cabletron, Bay Network,... đều đang quan tâm đặc biệt đến dòng sản phẩm hướng đến ATM của mình để tung ra thị trường. Có thể kể ra đây một số sản phẩm đó như DEC 900 Multiwitch, IBM 8250 hub, Cisco 7000 Router, Cabletron, ATM module for MMAC hub.
- Nhìn chung thị trường ATM sôi động do nhu cầu thực sự của các ứng dụng đa phương tiện. Sự nhập cuộc ngày một đông của các hãng sản xuất đã làm giảm đáng kể giá bán của các sản phẩm loại này, từ đó càng mở rộng thêm thị trường. Ngay ở Việt Nam, các dự án lớn về mạng tin học đều đã được thiết kế với hạ tầng chấp nhận được với công nghệ ATM trong tương lai.

Các đặc trưng chính của công nghệ ATM: Mạng chuyển mạch ATM là mạng cho phép xử lý tốc độ cao, dung lượng lớn, chất lượng truy nhập cao, và việc điều khiển quá trình chuyển mạch dễ dàng và đơn giản. Đặc tính của chuyển mạch ATM là ở chỗ nó thử nghiệm sự biến đổi của độ trễ tế bào thông qua việc sử dụng kỹ thuật tự định tuyến của lớp phần cứng, và có thể dễ dàng hỗ trợ cho truyền thông đa phương tiện sử dụng dữ liệu, tiếng nói và hình ảnh. Hơn thế nữa, nó có thể đảm

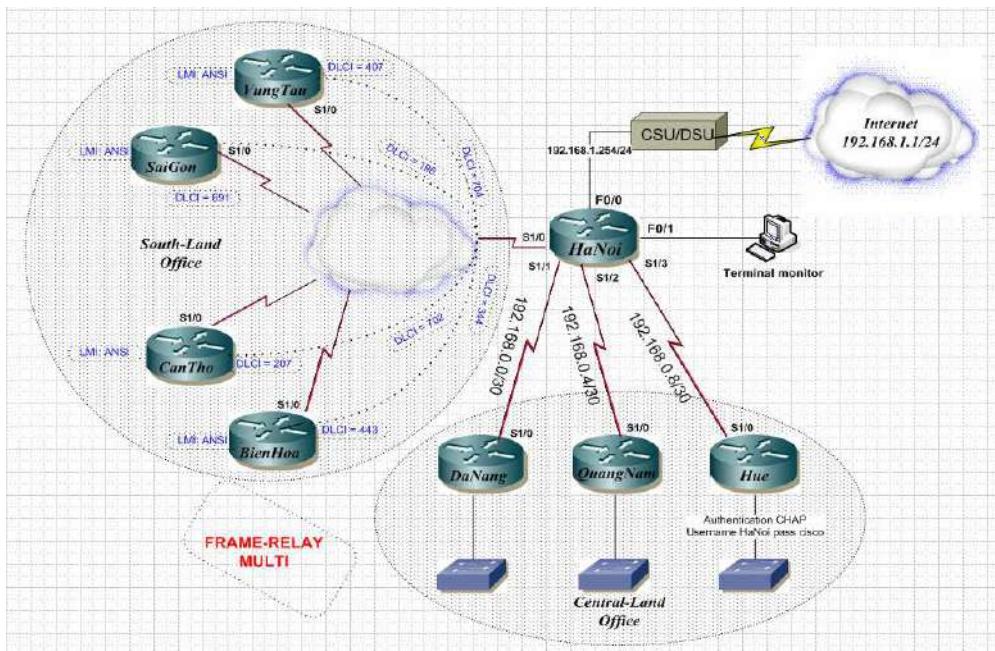
bảo việc điều khiển phân tán và song song ở mức độ cao. Nhược điểm của hệ thống chuyển mạch ATM là sự phức tạp của phần cứng và sự tăng thêm của trễ truyền dẫn tế bào, và là sự điều khiển phức tạp do việc chức năng sao chép và xử lý phải được thực hiện đồng thời.

Đánh giá khi dùng kết nối ATM

- Khi môi trường của xã hội thông tin được hoàn thiện, thì mạng giao tiếp thông tin băng rộng cần thiết phải tỏ ra thích nghi với các tính năng như tốc độ cao, băng rộng, đa phương tiện. Và vì vậy phải tính đến việc thiết lập mạng thông tin tốc độ siêu cao ở tầm quốc gia.
- Mạng thông tin tốc độ siêu cao đã dựa vào sử dụng công nghệ ATM (phương thức truyền tải không đồng bộ) để tạo ra mạng lưới quốc gia rộng khắp với tính kinh tế và hiệu quả cho phép các nhà cung cấp dịch vụ có thể cung cấp nhiều loại hình dịch vụ thông tin khác nhau.
- Công nghệ ATM là công nghệ đang trên quá trình hoàn thiện và chuẩn hóa, nên việc triển khai nó cần được nghiên cứu chuẩn bị rất đầy đủ và chi tiết, để có khả năng duy trì và mở rộng.

4.4.2.3. Kết nối dùng Frame Relay

Giới thiệu về mạng Frame Relay



Hình 4.7. Mô hình kết nối dùng mạng Frame Relay

Bước sang thập kỷ 80 và đầu thập kỷ 90, công nghệ truyền thông có những bước tiến nhảy vọt đặc biệt là chế tạo và sử dụng cáp quang vào mạng truyền dẫn tạo nên chất lượng thông tin rất cao. Việc sử dụng thủ tục hỏi đáp X25 để thực hiện truyền số liệu trên mạng cáp quang luôn đạt được chất lượng rất cao, và vì thế khung truyền từ 128 byte cho X25 được mở rộng với khung lớn hơn, thế là công nghệ Frame Relay ra đời. Frame relay có thể chuyên nhận các khung lớn tới 4096 byte, và không cần thời gian cho việc hỏi đáp, phát hiện lỗi và sửa lỗi ở lớp 3 (No protocol at Network layer) nên Frame Relay có khả năng chuyển tải nhanh hơn hàng chục lần so với X25 ở cùng tốc độ. Frame Relay rất thích hợp cho truyền số liệu tốc độ cao và cho kết nối LAN to LAN và cả cho âm thanh, nhưng điều kiện tiên quyết để sử dụng công nghệ Frame relay là chất lượng mạng truyền dẫn phải cao.

Các thiết bị dùng cho kết nối Frame Relay

- Các thiết bị truy nhập mạng FRAD (Frame Relay Access Device)

- Các thiết bị mạng chuyển tiếp khung FRND (Frame Relay Network Device)

Đường nối giữa các thiết bị và mạng trực Frame Relay, mô tả trong hình 4.8.



Hình 4.8. Mạng Frame Relay - Mạng chuyển mạch khung

- Thiết bị FRAD có thể là các LAN bridge, LAN Router v.v...
- Thiết bị FRND có thể là các Tổng đài chuyển mạch khung (Frame) hay tổng đài chuyển mạch tế bào (Cell Relay - chuyển tải tổng hợp các tế bào của các dịch vụ khác nhau như âm thanh, truyền số liệu, video v.v..., mỗi tế bào độ dài 53 byte, đây là phương thức của công nghệ ATM). Đường kết nối giữa các thiết bị là giao diện chung cho FRAD và FRND, giao thức người dùng và mạng hay gọi F.R UNI (Frame Relay User Network Interface). Mạng trực Frame Relay cũng tương tự như các mạng viễn thông khác có nhiều tổng đài kết nối với nhau trên mạng truyền dẫn, theo thủ tục riêng của mình. Trong OSI 7 lớp, lớp 3 - lớp mạng, Frame Relay không dùng thủ tục nào (Transparent).

Các đặc tính của Frame Relay

- Người sử dụng gửi một Frame (khung) đi với giao thức LAP-D hay LAP-F (Link Access Protocol D hay F), chứa thông tin về nơi đến và thông tin người sử dụng, hệ thống sẽ dùng thông tin này để định tuyến trên mạng.
- Công nghệ Frame Relay có một ưu điểm đặc trưng rất lớn là cho phép người sử dụng dùng tốc độ cao hơn mức họ đăng ký trong một khoảng thời gian nhất định, có nghĩa là Frame Relay không

cố định độ rộng băng thông (Bandwidth) cho từng cuộc gọi một mà phân phối bandwidth một cách linh hoạt, điều mà dịch vụ X25 và thuê kênh riêng không có. Ví dụ người sử dụng ký hợp đồng sử dụng với tốc độ 64 kbit/s, khi họ chuyển đi một lượng thông tin quá lớn, Frame Relay cho phép truyền chúng ở tốc độ cao hơn 64 kbit/s. Hiện tượng này được gọi là "bùng nổ" - Bursting.

- Thực tế trên mạng lưới rộng lớn có rất nhiều người sử dụng với vô số frame chuyển qua chuyển lại, hơn nữa Frame Relay không sử dụng thủ tục sửa lỗi và điều khiển thông lượng (Flow control) ở lớp 3 (Network layer), nên các Frame có lỗi đều bị loại bỏ thì vấn đề các frame được chuyển đi đúng địa chỉ, nguyên vẹn, nhanh chóng và không bị thừa bị thiếu là không đơn giản. Để đảm bảo được điều này Frame relay sử dụng một số giao thức sau:
 - DLCI (Data Link Connection Identifier- Nhận dạng đường nối dữ liệu). Cũng như X.25, trên một đường nối vật lý frame relay có thể có rất nhiều các đường nối ảo, mỗi một đối tác liên lạc được phân một đường nối ảo riêng để tránh bị lẫn, được gọi tắt là DLCI.
 - CIR (Committed Information Rate - Tốc độ cam kết). Đây là tốc độ khách hàng đặt mua và mạng lưới phải cam kết thường xuyên đạt được tốc độ này. CBIR (Committed Burst Information Rate - Tốc độ cam kết khi bùng nổ thông tin). Khi có lượng tin truyền quá lớn, mạng lưới vẫn cho phép khách hàng truyền quá tốc độ cam kết CIR tại tốc độ CBIR trong một khoảng thời gian (Tc) rất ngắn vài ba giây một đợt, điều này tuỳ thuộc vào độ "nghẽn" của mạng cũng như CIR.
 - DE bit (Discard Eligibility bit) - Bit đánh dấu Frame có khả năng bị loại bỏ. Về lý mà nói nếu chuyển các Frame vượt quá tốc độ cam kết, thì những Frame đó sẽ bị loại bỏ và bit DE được sử dụng. Tuy nhiên có thể chuyển các frame đi với tốc độ lớn hơn CIR hay thậm chí hơn cả

CBIR tuỳ thuộc vào trạng thái của mạng Frame relay lúc đó có độ nghẽn ít hay nhiều (Thực chất của khả năng này là mượn độ rộng băng thông "Bandwith" của những người sử dụng khác khi họ chưa dùng đến). Nếu độ nghẽn của mạng càng nhiều (khi nhiều người cùng làm việc) thì khả năng rủi ro bị loại bỏ của các Frame càng lớn. Khi Frame bị loại bỏ, thiết bị đầu cuối phải phát lại. Do mạng Frame relay không có thủ tục điều khiển thông lượng (Flow control) nên độ nghẽn mạng sẽ không kiểm soát được, vì vậy công nghệ Frame relay sử dụng hai phương pháp sau để giảm độ nghẽn và số frame bị loại bỏ.

- Sử dụng FECN (Forward Explicit Congestion Notification): Thông báo độ nghẽn cho phía thu và BECN (Backward Explicit Congestion Notification). Thông báo độ nghẽn về phía phát. Thực chất của phương pháp này để giảm tốc độ phát khi mạng lưới có quá nhiều người sử dụng cùng lúc.
- Sử dụng giao diện quản lý cục bộ LMI (Local Management Interface): Để thông báo trạng thái nghẽn mạng cho các thiết bị đầu cuối biết. LMI là chương trình điều khiển giám sát đoạn kết nối giữa FRAD và FRND.

Đánh giá khi dùng kết nối Frame Relay

- Hiện nay nhu cầu kết nối WAN được đặt ra và biến đổi theo từng ngày, có rất nhiều công nghệ được đưa ra thảo luận và thử nghiệm để xây dựng nền tảng mạng lưới cung cấp các dịch vụ truyền số liệu cho quốc gia. Theo xu thế chung, tất cả các dịch vụ thoại và phi thoại dần dần sẽ tiến tới được sử dụng trên nền của mạng thông tin băng rộng tích hợp IBCN (Integrated Broadband Communication Network). Trên cơ sở mạng IBCN, ngoài các dịch vụ truyền thống về thoại và truyền số liệu còn có thể cung cấp rất nhiều dịch vụ liên quan tới hình ảnh động và dịch vụ từ xa

như: truyền hình chất lượng cao, hội thảo truyền hình, thư viện điện tử, đào tạo từ xa, video theo yêu cầu (video on demand),...

- Quá trình tiến tới mạng IBCN hiện tại có thể xem như có hai con đường: Hướng thứ nhất là từ các mạng điện thoại tiến tới xây dựng mạng số đa dịch vụ tích hợp ISDN rồi tiến tới BISDN hay IBCN. Hướng thứ hai là từ các mạng phi thoại tức là các mạng truyền số liệu tiến tới xây dựng các mạng chuyên tiếp khung (Frame-Relay) rồi mạng truyền dẫn không đồng bộ ATM để làm nền tảng cho IBCN.
- Công nghệ Frame-Relay với những ưu điểm của nó như là một công nghệ sẽ được ứng dụng trên mạng truyền số liệu của Việt nam trong thời gian tới. Theo số liệu của diễn đàn Frame-Relay thì nguyên nhân để người dùng chọn Frame-Relay là:
 - Kết nối LAN to LAN: 31%
 - Tạo mạng truyền ảnh: 31%
 - Tốc độ cao: 29%
 - Giá thành hợp lý: 24%
 - Dễ dùng, độ tin cậy cao: 16%
 - Xử lý giao dịch phân tán: 16%
 - Truyền hình hội nghị: 5%
- Rõ ràng là các ứng dụng trên Frame-Relay đều sử dụng khả năng truyền số liệu tốc độ cao và cần đến dịch vụ băng tần rộng có tính đến khả năng bùng nổ lưu lượng (traffic bursty) mà ở các công nghệ cũ hơn như chuyển mạch kênh hay chuyển mạch gói không thể tạo ra.

4.4.2.4. Kết nối dùng dịch vụ chuyển mạch dữ liệu nhiều Megabit

4.4.2.4.1. Giới thiệu chung

SMDS (Switched Multimegabit Data Service) là một dịch vụ WAN được thiết kế cho các kết nối LAN-to-LAN. SMDS được Bellcore và các công ty Regional Bell Operating (RBOCs) phát triển nhằm thỏa mãn nhu cầu người sử dụng về kết nối LAN Multimegabit trong vùng mạng chính.

SMDS được thiết kế cho dịch vụ chuyển mạch gói với giá cả hợp lý, cung cấp các kết nối và mở rộng chất lượng cao.

Tuy nhiên, khác với sự thành công của SMDS ở châu Âu, ở Mỹ SMDS không được phát triển. SMDS Interest Group, một tổ chức lớn nhất tài trợ cho SMDS đã ngừng hoạt động từ năm 1997. Hơn nữa, trong ngày kỷ niệm lần thứ 25 của Truyền thông số liệu – Data Communications (ngày 21/10/1997), SMDS được bình chọn là một trong 25 thất bại tiêu biểu nhất.

4.4.2.4.2. SMDS là gì ?

SMDS là một dịch vụ mạng diện rộng được thiết kế dành cho kết nối mạng LAN với mạng LAN. Mạng SMDS là một mạng MAN có các đặc trưng : Đơn vị dữ liệu sử dụng được gọi là tế bào (Cell-Based), không liên kết (Connectionless), tốc độ cao, chuyển mạch gói bằng thông rộng. SMDS cũng là một dịch vụ dữ liệu, nghĩa là chỉ truyền dữ liệu (mặc dù có thể truyền cả âm thanh và hình ảnh). SMDS là một dịch vụ thực sự, không gắn với một công nghệ truyền số liệu nào.

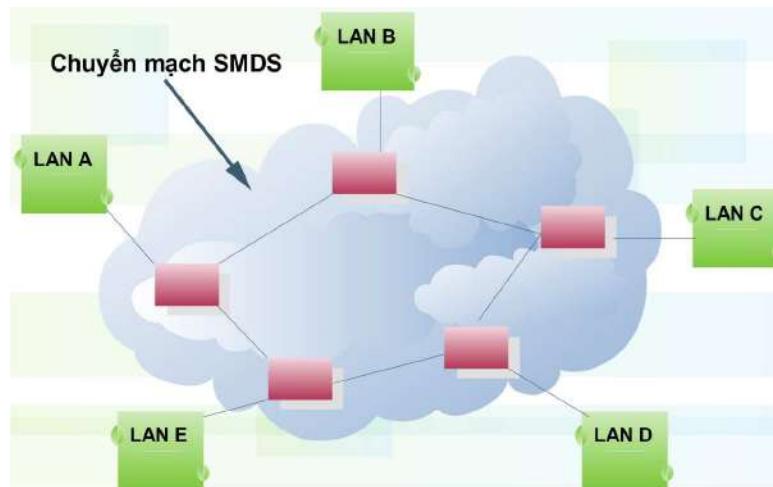
4.4.2.4.3. Tổng quan về SMDS

Tế bào của SMDS là đơn vị cơ bản có độ dài cố định. Tương tự như tế bào của ATM gồm 53 byte – 44 byte dữ liệu, 7 byte là Header và 2 byte dấu vết. Điều này tạo cho nó sự tương thích với các mạng diện rộng công cộng B-ISDN sử dụng công nghệ chuyển mạch gói nhanh và công nghệ ATM. Mỗi tế bào của SMDS chứa địa chỉ đích cho phép các thuê bao SMDS có thể truyền dữ với nhau. Là một dịch vụ dữ liệu không liên kết, SMDS thiết lập một kênh ảo (Virtual Circuit) giữa 2 thực thể thu và phát, các tế bào dữ liệu được truyền đi một cách độc lập với nhau và không tuân theo một thứ tự đặc biệt nào.

Mạng SMDS cung cấp băng thông theo yêu cầu cho các bùng nổ giao thông, là một thuộc tính của các ứng dụng mạng cục bộ LAN.

Vì không cần phải định nghĩa trước đường truyền giữa các thiết bị, dữ liệu có thể đi qua những đường ít tắt nghẽn nhất trong mạng SMDS. Tuy nhiên dịch vụ cũng có khả năng cung cấp một đường truyền nhanh

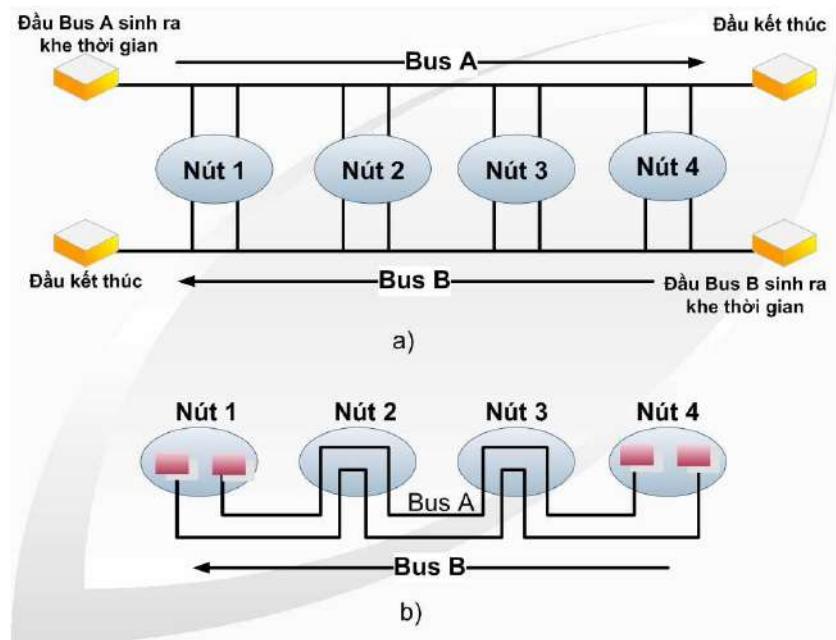
hơn, tính năng bảo mật và mềm dẻo hơn. Khía cạnh băng rộng của SMDS là từ sự tương thích của nó với B-ISDN và tiềm năng truyền tiếng nói và hình ảnh. SMDS tương thích với chuẩn IEEE.802.6 MAN.



Hình 4.9. Mạng SMDS

SMDS dựa trên lớp MAC (Media Access Control) và lớp vật lý của chuẩn IEEE 802.6, vì vậy nó hoạt động như Token Ring tốc độ cao.

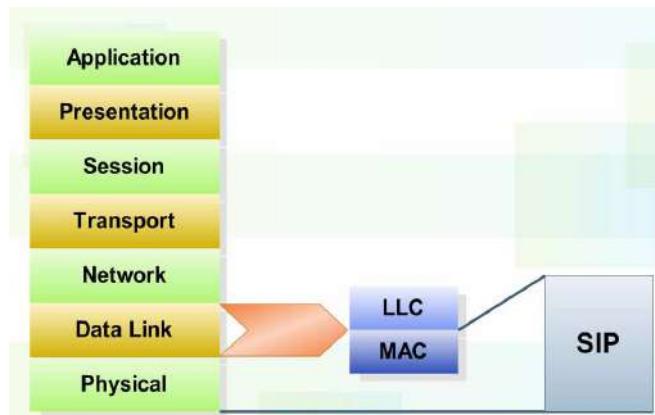
- Đặc điểm vật lý IEEE 802.6 có thể được thiết kế như một Bus hở hoặc một Bus vòng. Bus hở, các Bus khởi đầu và kết thúc tại các nút khác nhau. Với Bus dạng vòng, các Bus khởi đầu và kết thúc tại cùng một nút.
- Đặc điểm tầng liên kết dữ liệu – DQDB (Distributed Queue Dual Bus): Mạng SMDS được quản lý bởi giao thức DQDB Bus quang bá đa truy nhập . IEEE 802.6, chia mỗi Bus thành nhiều khe để truyền dữ liệu. Trong mỗi Bus có một bit bận và một bit yêu cầu. DQDB làm việc như sau:
 - Trước khi truyền, đặt trước một khe trên một Bus để sử dụng Bus thứ hai bằng cách đặt bit yêu cầu (Req). Ví dụ nút 2 muốn gửi dữ liệu tới nút 3 thì phải gửi thông qua Bus A. Nút 2 sẽ đặt bit Req trên Bus B để thông báo cho các Bus phía trên của Bus A biết rằng tại nút đó đang có dữ liệu cần gửi.



Hình 4.10. Cấu hình vật lý của mạng SMDS

- Sau khi yêu cầu một khe, nút đó quan sát cả 2 Bus và duy trì một số đếm các yêu cầu. Số đếm tăng 1 khi nút 2 thấy bit yêu cầu được thiết lập trên Bus B và giảm đi 1 cho mọi khe trống trên Bus A. Như vậy số đếm tại mỗi nút cho biết chiều dài hàng các té bào đang đợi để truyền bởi các nút phía trên.
- Khi số đếm bằng 0 nghĩa là không còn nút dưới nào có dữ liệu cần gửi thì nút đó bắt đầu gửi dữ liệu. Tiến trình này được biểu diễn một dạng của CSMA/CA, để phòng sự xung đột khi các nút gửi dữ liệu tại cùng một thời điểm. DQDB hỗ trợ cả dịch vụ không liên kết và hướng liên kết và có khả năng truyền dữ liệu, tiếng nói và hình ảnh, mặc dù SMDS chỉ truyền dữ liệu.
- Giao thức giao diện mạng SMDS (SMDS Interface Protocol – SIP): Được định nghĩa bởi Bellcore và cấu thành bởi ba mức giao thức SIP mức 3, SIP mức 2 và SIP mức 1. Mặc dù ba giao thức này được dựa trên 3 tầng đầu

tiên của mô hình OSI, nhưng không tương ứng với các tầng này. Thay vào đó, ba mức giao thức này biểu diễn cho tầng MAC dưới của OSI và do vậy vận hành tại tầng liên kết dữ liệu.



Hình 4.11. Các tầng của SIP tương ứng với mô hình OSI

4.4.2.4.3. SMDS so sánh với các công nghệ ATM và Frame Relay

SMDS là một dịch vụ, không phải là một công nghệ. Frame Relay và ATM là các công nghệ.

SMDS dịch vụ chuyển mạch gói không kết nối (Connectionless) Frame Relay và ATM là mạng hướng liên kết (Connection-Oriented).

SMDS cung cấp nhiều cách quản lý mạng đặc trưng như cách tính tiền hay thống kê lượng sử dụng của người sử dụng.

Cách đánh địa chỉ của SMDS cung cấp một loại biện pháp bảo mật có sẵn bằng cách giới hạn dữ liệu được truyền đến các nút được gắn với một địa chỉ nhóm cụ thể.

SMDS bị cạnh tranh bởi ATM và Frame Relay ở nước Mỹ.

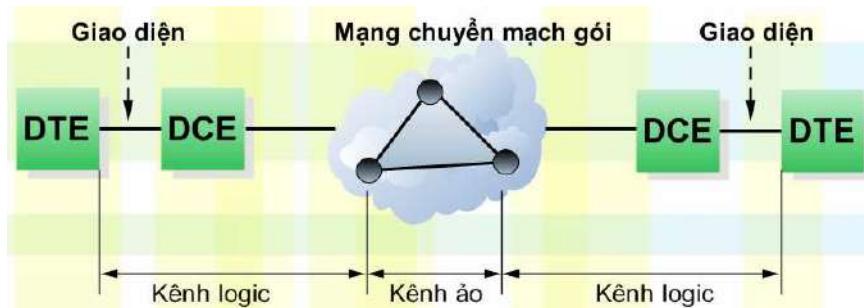
SMDS không thiết kế để truyền các ứng dụng âm thanh, hình ảnh theo thời gian thực, mặc dù phương pháp tiếp cận DQDB cung cấp các công nghệ cần thiết cho sự hỗ trợ này.

SMDS có sẵn tính bảo mật cho phép sử dụng các mạng công cộng, chia sẻ như là xương sống của một mạng riêng. Khái niệm này đã bị che lấp bởi Internet và mạng riêng ảo VPN (Virtual Private Network).

SMDS là một dịch vụ, không phải là một công nghệ nên nó có thể vận hành trên cả Frame Relay và ATM. Không phụ thuộc về giao thức, vì vậy có thể hỗ trợ cho nhiều giao thức mạng LAN hay cho mạng máy tính. Băng thông từ 56/64 kbit/s với tốc độ SONET nên phù hợp với dài thông cho mọi ứng dụng. Là dịch vụ không kết nối nên tránh được sự cần thiết trong việc định nghĩa các PVC như đối với Frame Relay. Chuyển mạch gói nên các gói tin được truyền đi ngay mà không cần phải đợi. Là một mạng công cộng chia sẻ chung nên các thuê bao có thể trao đổi dữ liệu với nhau, sử dụng tần số 53 byte tương thích với công nghệ ATM, vì vậy có thể chuyển đổi một cách thuận tiện từ mạng SMDS sang mạng ATM.

Tuy nhiên một số điểm không thuận lợi đã làm cho SMDS bị ATM và Frame Relay che khuất như là được nhìn nhận là một dịch vụ đắt tiền, mặc dù có đủ khả năng truyền được hình ảnh nhưng SMDS không hỗ trợ tính năng này...

4.4.2.5. Kết nối dùng X.25



Hình 4.12. Mạng X.25 đơn giản

Mạng X.25 được CCITT công bố lần đầu tiên vào 1970, lúc đó lĩnh vực viễn thông lần đầu tiên tham gia vào thế giới truyền dữ liệu với các đặc tính:

- X.25 cung cấp quy trình kiểm soát luồng giữa các đầu cuối để lại chất lượng đường truyền cao cho dù chất lượng mạng lưới đường dây truyền thông không cao.

- X.25 được thiết kế cho cả truyền thông chuyển mạch lân truyền thông kiểu điểm nối điểm. Được quan tâm và triển khai nhanh chóng trên toàn cầu.
- Trong X.25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ phức tạp trong việc phối hợp các thủ tục giữa hai tầng kè nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên.
- X.25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm hạn chế tốc độ trên đường truyền có chất lượng rất cao như mạng cáp quang . Tuy nhiên do vậy khối lượng tích toán tại mỗi nút khá lớn, đối với những đường truyền của những năm 1970 thì điều đó là cần thiết nhưng hiện nay khi kỹ thuật truyền dẫn đã đạt được những tiến bộ rất cao thì việc đó trở nên lãng phí. Do vậy công nghệ X.25 nhanh chóng trở thành lạc hậu.
- Hiện nay X.25 không còn phù hợp với công nghệ truyền số liệu.

4.5. GIAO THỨC KẾT NỐI WAN

Một số giao thức được sử dụng trong việc kết nối WAN như: PPP, HDLC, SDLC, X.25, Frame Relay, ISDN, ...

4.5.1. Giao thức HDLC

Giao thức HDLC (High-level Data Link Control) là giao thức liên kết dữ liệu mức cao, thuộc tầng 2 –tầng liên kết dữ liệu-trong mô hình tham chiếu OSI.

Giao thức HDLC là một giao thức chuẩn hóa quốc tế và đã được định nghĩa bởi ISO để dùng cho cả liên kết điểm- nối- điểm và đa điểm. Nó hỗ trợ hoạt động ở chế độ trung suốt, song công hoàn toàn và ngày nay được dùng một cách rộng rãi trong các mạng đa điểm và trong các mạng máy tính. Tiền thân của HDLC là giao thức SDLC (Synchronous

Data Link Control : điều khiển liên kết dữ liệu đồng bộ). Đây là một giao thức liên kết dữ liệu rất quan trọng, rất nhiều nghi thức liên kết dữ liệu khác tương tự hoặc dựa trên nghi thức này. HDLC là một giao thức hướng đến bit.

Đặc điểm chung của giao thức HDLC

- Hoạt động ở chế độ full-duplex.
- Liên kết điểm-nối-điểm hoặc đa điểm.
- Truyền dẫn đồng bộ.
- Điều khiển lỗi “Continuous RQ”.

Các chế độ hoạt động của giao thức HDLC: HDLC có 3 chế độ hoạt động

- Chế độ đáp ứng thông thường NRM (Normal Response Mode): Chế độ này được dùng trong cấu hình không cân bằng. Trong chế độ này, trạm sơ cấp khởi động việc trao đổi dữ liệu, trạm thứ cấp chỉ có thể truyền khi nhận được chỉ thị đặc biệt của trạm sơ cấp. Liên kết này có thể là điểm-nối-điểm hay đa điểm. Trong trường hợp đa điểm chỉ cho phép một trạm sơ cấp.
- Chế độ đáp ứng bất đồng bộ ARM (Asynchronous Response Mode): Chế độ này cũng được dùng trong cấu hình không cân bằng. Nó cho phép một trạm thứ cấp xúc tiến một hoạt động truyền mà không cần sự cho phép từ trạm sơ cấp. Chế độ này thường được dùng trong các cấu hình điểm-nối-điểm và các liên kết song công và cho phép thứ cấp truyền các frame một cách bất đồng bộ với sơ cấp.
- Chế độ cân bằng bất đồng bộ ABM (Asynchronous Balanced Mode): Chế độ này được dùng chủ yếu trên các liên kết song công điểm-nối-điểm cho ứng dụng truyền số liệu máy tính-đến-máy tính và cho các kết nối giữa máy tính và mạng số liệu công cộng (PSDN). Trong chế độ này, mỗi trạm có một trạng thái như

nhau và thực hiện cả hai chức năng sơ cấp và thứ cấp. Nó là chế độ được dùng trong giao thức nối tiếng X.25.

4.5.2. Giao thức PPP

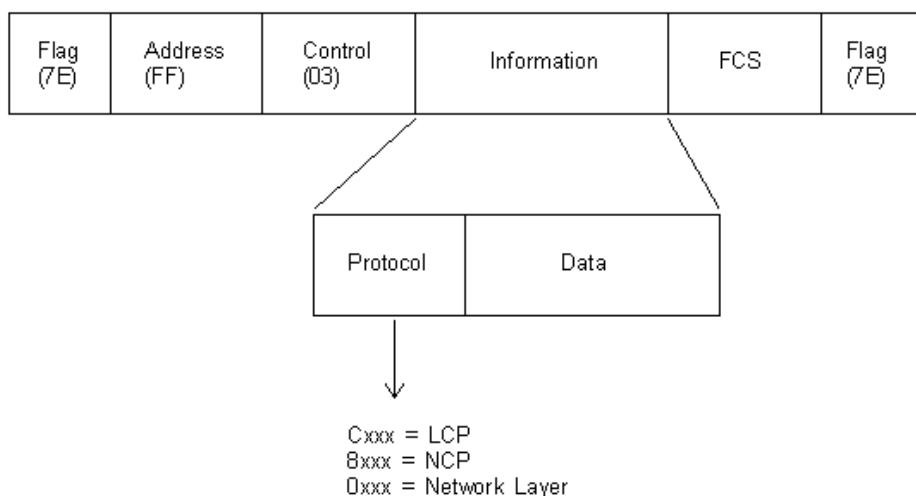
PPP được xây dựng dựa trên nền tảng giao thức điều khiển truyền dữ liệu lớp cao (HDLC - High-Level Data link Control) nó định ra các chuẩn cho việc truyền dữ liệu các giao diện DTE và DCE của mạng WAN như V.35, T1, E1, HSSI, EIA-232-D, EIA-449. PPP được ra đời như một sự thay thế giao thức Serial Line Internet Protocol (SLIP), một dạng đơn giản của TCP/IP.

PPP cung cấp cơ chế chuyển tải dữ liệu của nhiều giao thức trên một đường truyền, cơ chế sửa lỗi nén header, nén dữ liệu và multilink. PPP có hai thành phần:

- Link Control Protocol (LCP): Thiết lập, điều chỉnh cấu hình và hủy bỏ một liên kết. Hơn thế nữa LCP còn có cơ chế Link Quality Monitoring (LQM) có thể được cấu hình kết hợp với một trong hai cơ chế chứng thực Password Authentication Protocol (PAP) hay Challenge Handshake Authentication Protocol (CHAP).
- Network Control Protocol (NCP): NCP làm nhiệm vụ thiết lập, điều chỉnh cấu hình và hủy bỏ việc truyền dữ liệu của các giao thức của lớp network như IP, IPX, AppleTalk and DECnet.

Cả LCP và NCP đều hoạt động ở lớp 2. Hiện đã có mở rộng của PPP phục vụ cho việc truyền dữ liệu sử dụng nhiều links một lúc, đó là **Multilink PPP (MPPP)** trong đó sử dụng **Multilink Protocol (MLP)** để liên kết các lớp LCP và NCP.

Định dạng khung dữ liệu



Hình 4.13. Định dạng khung dữ liệu của PPP

4.6. CÁC THIẾT BỊ KẾT NỐI WAN

WAN sử dụng nhiều loại thiết bị để kết nối như: Wan Switch, Access Server, Modem, CSU/DSU, ISDN Terminal Adapter, ... Ngoài ra chúng ta có thể tìm thấy các thiết bị khác được sử dụng trong môi trường WAN như: Router, ATM Switch và Multiplexer.

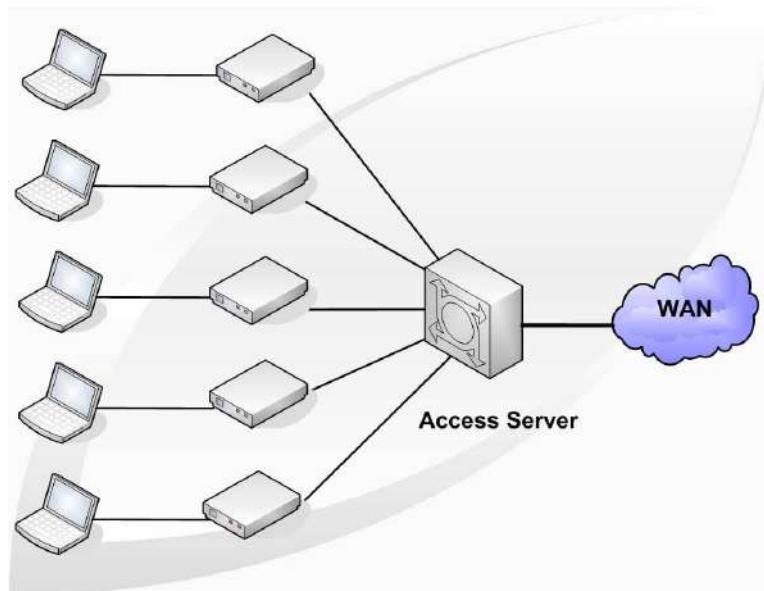
4.6.1. Router

Bạn đọc xem trong chương 2, mục 2.3.6.

4.6.2. Access Server

Access Server đóng vai trò như một điểm tập trung cho các kết nối dial-in và dial-out. Kết nối WAN, truy nhập từ xa dùng access server là giải pháp đơn giản, tiết kiệm chi phí nhất.

Access server làm nhiệm vụ chờ kết nối từ xa đến, và tự nó có thể quay số để kết nối với access server khác. Khi người dùng từ xa, hay mạng xa kết nối vào access server, nếu được phép thì người dùng có thể sử dụng các tài nguyên mạng đang kết nối với access server này, hoặc access server này là một trạm chuyển tiếp để kết nối đi tiếp.



Hình 4.14. Access Server tập trung Dial-out kết nối vào WAN

4.6.3. Modem



Hình 4.15. Modem

Modem: Là một thiết bị điều chế tín hiệu tương tự để mã hóa dữ liệu số, và giải điều chế tín hiệu mang để giải mã tín hiệu số.

Một thí dụ quen thuộc nhất của modem bằng tần tiếng nói là chuyển tín hiệu số '1' và '0' của máy tính thành âm thanh mà nó có thể truyền qua dây điện thoại của Plain Old Telephone Systems (POTS), và khi nhận được ở đầu kia, nó sẽ chuyển âm thanh đó trở về tín hiệu '1' và '0'.

Modem thường được phân loại bằng lượng dữ liệu truyền nhận trong một khoảng thời gian, thường được tính bằng đơn vị bit trên giây, hoặc "bps".

4.6.4. CSU/DSU



Hình 4.16. CSU/DSU

CSU/DSU (Channel Service Unit/Data Service Unit) là thiết bị phần cứng tại các điểm đầu cuối của các kênh thuê riêng. Nó làm nhiệm vụ chuyển dữ liệu trên đường truyền WAN sang dữ liệu trên LAN và ngược lại. Thiết bị này dùng để kết nối WAN khi dùng các kênh thuê riêng.

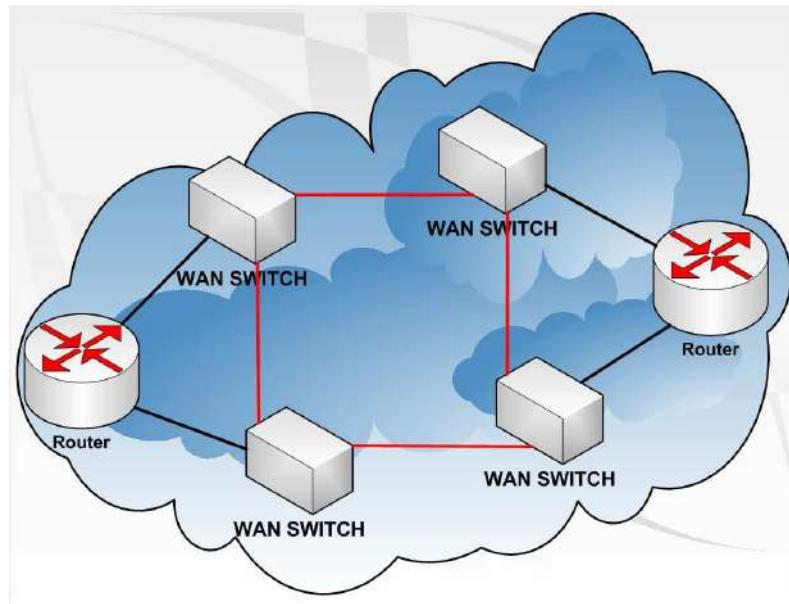
CSU/DSU dùng các giao diện chuẩn RS-232C, RS-449, hay V.xx

4.6.5. Chuyển mạch WAN

Phương pháp chuyển mạch WAN là qua nhà cung cấp dịch vụ viễn thông thiết lập và duy trì mạch dùng riêng cho mỗi phiên truyền thông. Một minh họa cho chuyển mạch WAN là mạng chuyển mạch số đa dịch vụ ISDN.

WAN Switch là một thiết bị kết nối nhiều cổng liên mạng, được sử dụng trong mạng viễn thông. Wan Switch được dùng trong mạng Frame Relay, X.25, SMDS (Switched MultiMegabit Data Service - Dịch vụ dữ liệu chuyển mạch MultiMegabit) và hoạt động ở lớp liên kết dữ liệu trong mô hình tham chiếu OSI.

Ví dụ: WAN Switch đa dịch vụ **B-STDX** của Lucent sử dụng công nghệ Fram Relay, IP và các dịch vụ ATM, hay bộ chuyển mạch DSLAM dùng trong công nghệ ADSL, G.SHDSL.



Hình 4.17. Hai router đầu cuối trong Wan có thể được kết nối bằng Wan Switch

Lý do dùng chuyển mạch WAN: Chuyển mạch WAN được dùng để cùng một lúc duy trì nhiều cầu nối giữa các thiết bị mạng, do vậy tức thời tạo được loại đường truyền xương sống (backbone) nội tại tốc độ cao theo yêu cầu. Chuyển mạch WAN có nhiều cổng, mỗi cổng có thể hỗ trợ một tuyến thuê bao riêng với tốc độ theo yêu cầu.

4.6.6. ISDN Terminal Adapter

Là thiết bị đầu cuối để kết nối PC hay LAN vào WAN qua mạng ISDN. Mặc dù nó được gọi là Terminal Adapter nhưng nó không chuyển đổi từ tín hiệu analog sang tín hiệu số.

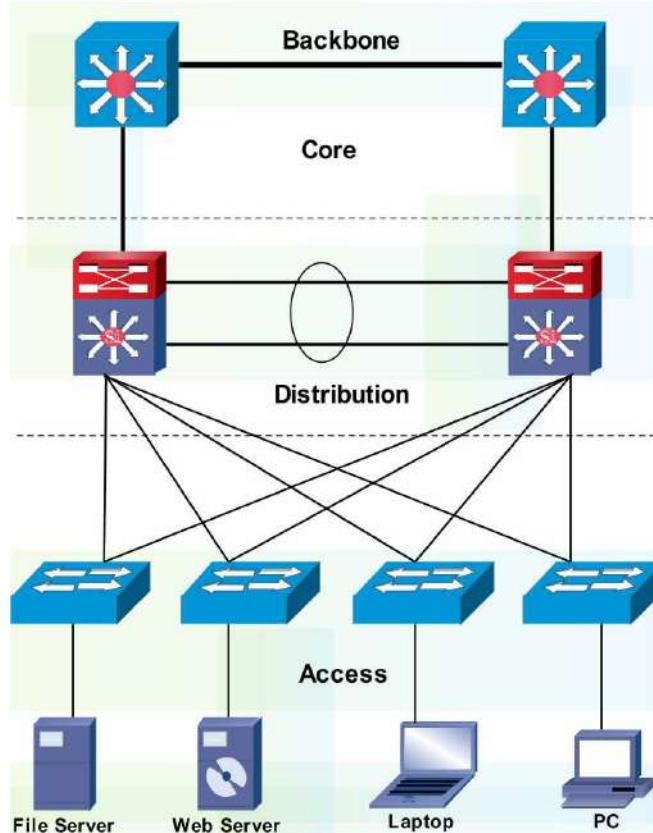
4.7. THIẾT KẾ WAN

4.7.1. Các mô hình thiết kế WAN

4.7.1.1. Mô hình phân cấp

Mô hình phân cấp hỗ trợ thiết kế WAN thường là mô hình phân cấp ba tầng (Do Cisco đưa ra): Tầng 1 là tầng lõi (Core), tầng 2 phân tán

(Distribution), tầng 3 là tầng truy nhập (Access), gọi tắt là mô hình phân cấp phục vụ cho việc khảo sát và thiết kế WAN.



Hình 4.18. Mô hình phân cấp 3 lớp

Tầng lõi là phần kết nối mạng trực(WAN backbone) kết nối các trung tâm mạng (NOC) của từng vùng, thông thường khoảng cách giữa các NOC là xa hay rất xa, do vậy chi phí kết nối và độ tin cậy cần phải được xem xét kỹ. Hơn nữa vấn đề đảm bảo chất lượng dịch vụ QoS cũng được đặt ra, dẫn đến phân loại, phân cấp ưu tiên dịch vụ.

Tầng phân tán là phần kết nối các điểm đại diện POP, hay các nhánh mạng vào NOC.

Tầng truy nhập từ xa là phần kết nối của người dùng di động, hay các chi nhánh nhỏ vào POP hay vào NOC.

Các ưu điểm của mô hình phân cấp: Nhờ mô hình phân cấp người thiết kế WAN dễ tổ chức khảo sát, dễ lựa chọn các phương án, và công nghệ kết nối, dễ tổ chức triển khai, cũng như đánh giá kết quả.

4.7.1.2. Mô hình an ninh – an toàn

4.7.1.2.1. An ninh – an toàn mạng là gì?

Một số khái niệm

- Computer Security (an toàn máy tính) – Là một tiến trình ngăn chặn và phát hiện sử dụng không hợp pháp vào máy tính của bạn bằng cách lựa chọn các công cụ thiết kế để bảo vệ dữ liệu và tấn công của tin tặc.
- Network Security (an toàn mạng) – Các phương pháp để bảo vệ dữ liệu trong suốt quá trình chuyển động của chúng.
- Internet Security (an toàn Internet) – Các phương pháp để bảo vệ dữ liệu trong suốt quá trình vận chuyển của chúng ra ngoài đến kết nối Internet

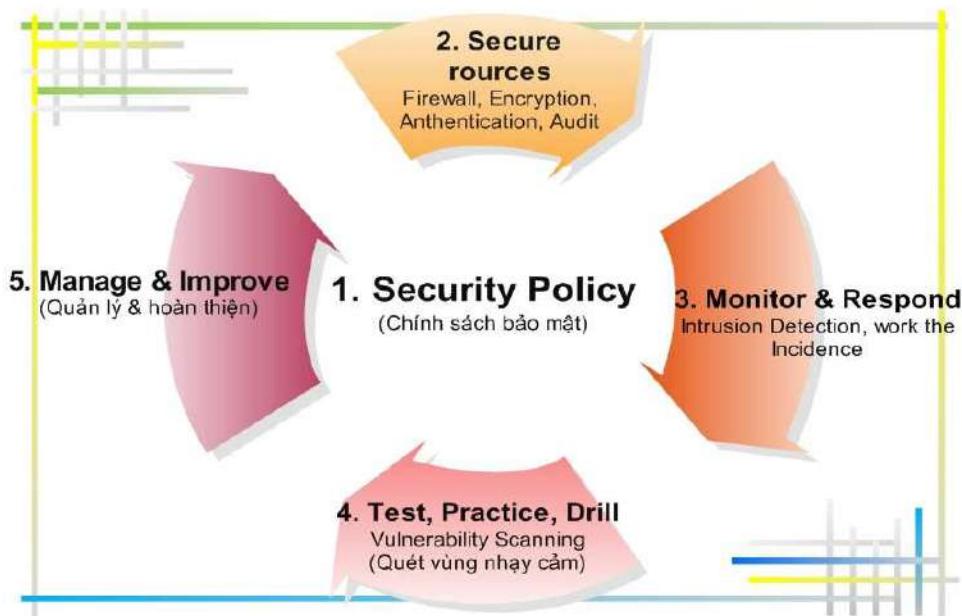
Tài nguyên mà chúng ta muốn bảo vệ là gì?

- Là các dịch vụ mà mạng đang triển khai
- Là các thông tin quan trọng mà mạng đó đang lưu giữ, hay cần lưu chuyển
- Là các tài nguyên phần cứng và phần mềm mà hệ thống mạng đó để cung ứng cho những người dùng mà nó cho phép, ...

Nhìn từ một phía khác thì vấn đề an ninh – an toàn mạng khi thực hiện kết nối WAN còn được thể hiện qua tính bảo mật (confidentiality), tính toàn vẹn (integrity) và tính sẵn dùng (availability) của các tài nguyên về phần cứng, phần mềm, dữ liệu và các dịch vụ của hệ thống mạng.

Vấn đề an ninh – an toàn mạng còn thể hiện qua mối quan hệ giữa người dùng với hệ thống mạng và tài nguyên trên mạng. Các quan hệ này được xác định, được đảm bảo qua phương thức xác thực (authentication), xác định được phép (authorization) dùng, và bị từ chối (repudiation).

- Tính bảo mật: Bảo đảm tài nguyên mạng không bị tiếp xúc, bị sử dụng bởi những người không có thẩm quyền. Chẳng hạn dữ liệu truyền trên mạng được đảm bảo không bị lấy trộm cần được mã hoá trước khi truyền. Các tài nguyên đó đều có chủ và được bảo vệ bằng các công cụ và các cơ chế an ninh mạng.
- Tính toàn vẹn: Đảm bảo không có việc sử dụng và sửa đổi nếu không được phép, ví dụ như lấy hay sửa đổi dữ liệu, cũng như thay đổi cấu hình hệ thống bởi những người không được phép hoặc không có quyền. Thông tin lưu hay truyền trên mạng và các tệp cấu hình hệ thống luôn được đảm bảo giữ toàn vẹn. Chúng chỉ được sử dụng và được sửa đổi bởi những người chủ của nó hay được cho phép.



Hình 4.19. Mô hình an ninh – an toàn

- **Tính sẵn dùng:** Tài nguyên trên mạng luôn được bảo đảm không thể bị chiếm giữ bởi người không có quyền. Các tài nguyên đó luôn sẵn sàng phục vụ những người được phép sử dụng. Những người có quyền có thể dùng bất cứ khi nào, bất cứ lúc nào.

Thuộc tính này rất quan trọng, nhất là trong các dịch vụ mạng phục vụ công cộng (ngân hàng, tư vấn, chính phủ điện tử, ...).

- **Việc xác thực:** Thực hiện xác định người dùng được quyền dùng một tài nguyên nào đó như thông tin hay tài nguyên phần mềm và phần cứng trên mạng. Việc xác thực thường kết hợp với sự cho phép, hay từ chối phục vụ. Xác thực thường dùng là mật khẩu (password), hay căn cước của người dùng như vân tay hay các dấu hiệu đặc dụng. Sự cho phép xác định người dùng được quyền thực hiện một hành động nào đó như đọc/ghi một tệp (lấy thông tin), hay chạy chương trình (dùng tài nguyên phần mềm), truy nhập vào một đoạn mạng (dùng tài nguyên phần cứng), gửi hay nhận thư điện tử, tra cứu cơ sở dữ liệu - dịch vụ mạng,... Người dùng thường phải qua giai đoạn xác thực bằng mật khẩu (password, RADIUS,...) trước khi được phép khai thác thông tin hay một tài nguyên nào đó trên mạng.

Các vấn đề về an ninh – an toàn mạng khi kết nối WAN cần được xem xét và thực hiện sau khi đã chọn giải pháp kết nối, nhất là khi kết nối WAN cho các mạng công tác, mà sử dụng các mạng dữ liệu công cộng, hay mạng Internet.

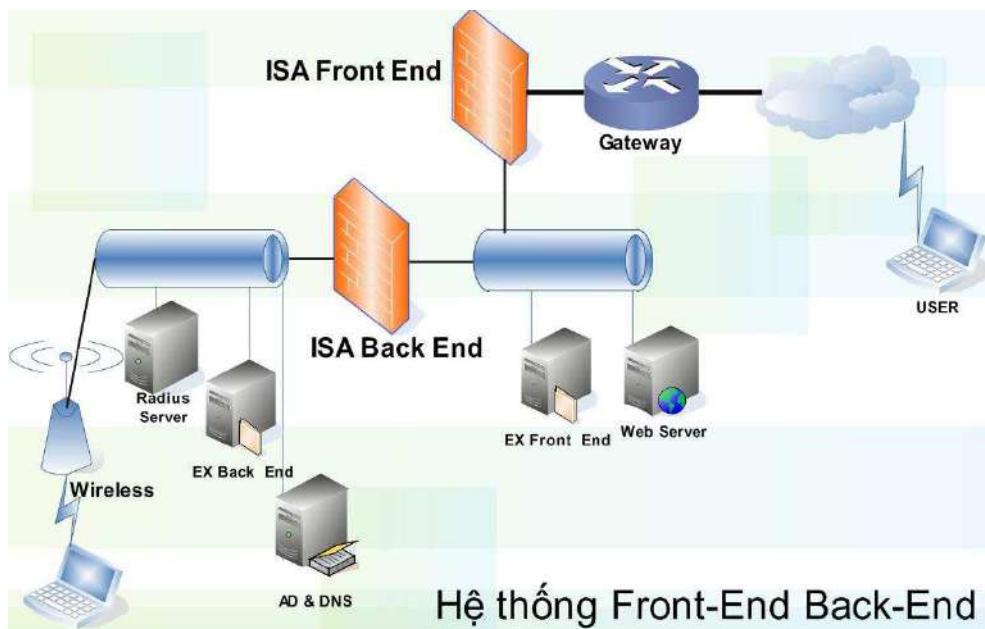
Xây dựng mô hình an ninh – an toàn khi kết nối WAN: Các bước xây dựng

- Xác định cần bảo vệ cái gì?
- Xác định bảo vệ khỏi các loại tấn công nào?
- Xác định các mối đe dọa an ninh mạng có thể?
- Xác định các công cụ để bảo đảm an ninh mạng?
- Xây dựng mô hình an ninh – an toàn

Thường xuyên kiểm tra các bước trên, nâng cấp, cập nhật và vá lỗi hệ thống khi có một lỗ hổng an ninh mạng được cảnh báo.

Mục đích của việc xây dựng mô hình an ninh – an toàn khi kết nối WAN là xây dựng các phương án để triển khai vấn đề an ninh – an toàn mạng khi kết nối và đưa WAN vào hoạt động.

- Đầu tiên, mục đích và yêu cầu về an ninh mạng hệ thống ứng dụng phải được vạch ra rõ ràng. Chẳng hạn mục tiêu và yêu cầu an ninh mạng khi kết nối WAN cho các cơ quan hành chính nhà nước sẽ khác với việc kết nối WAN cho các trường đại học.
- Thứ hai, mô hình an ninh – an toàn mạng phải phù hợp với các chính sách, nguyên tắc và luật lệ hiện hành.
- Thứ ba, phải giải quyết các vấn đề liên quan đến an ninh – an toàn mạng một cách toàn cục. Có nghĩa là phải đảm bảo cả về phương tiện kỹ thuật và con người triển khai.



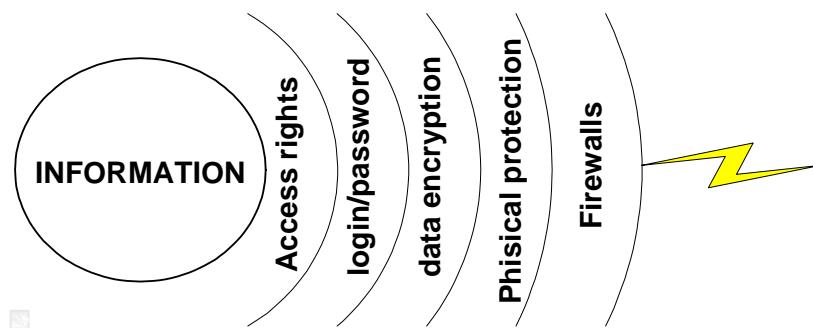
Hình 4.20. Mô hình Firewall Front End – Back End

4.7.1.2.2. Một số công cụ triển khai mô hình an ninh – an toàn mạng

Hệ thống tường lửa (Firewall): Là một điểm chặn trong quá trình điều khiển và giám sát. Tường lửa có tác dụng ngăn chặn, cho phép hay đưa ra các luật cho các địa chỉ và các vùng địa chỉ khác nhau. Firewall có các chức năng sau:

- Ngăn ngừa khả năng tấn công từ các mạng ngoài.

- Kiểm soát luồng thông tin giữa mạng được ủy thác (Trusted Network) và internet thông qua các chính sách truy nhập đã được thiết lập.
- Cho phép hoặc cấm các dịch vụ truy nhập hai chiều, từ trong ra ngoài và từ ngoài vào trong.
- Kiểm soát địa chỉ truy nhập và dịch vụ sử dụng.
- Kiểm soát khả năng truy nhập người sử dụng giữa hai mạng.



Hình 4.21. Chức năng Firewall

Firewall có những hạn chế của nó, đó là:

- Không thể bảo vệ từ các cuộc tấn công vòng qua nó (bypassing)
- Không thể bảo vệ chống lại đe dọa từ bên trong
- Không thể bảo vệ chống lại sự di chuyển của tất cả các loại chương trình hoặc file bị nhiễm virus

Hệ thống phát hiện và ngăn ngừa xâm nhập (IDS/IPS)

IDS (Intrusion Detection System – hệ thống phát hiện xâm nhập) là một hệ thống giám sát lưu thông mạng, các hoạt động khả nghi và cảnh báo cho hệ thống, nhà quản trị. IDS cũng có thể phân biệt giữa những tấn công bên trong từ bên trong (từ những người trong công ty) hay tấn công từ bên ngoài (từ các hacker). IDS phát hiện dựa trên các dấu hiệu đặc biệt về các nguy cơ đã biết (giống như cách các phần mềm diệt virus dựa vào các dấu hiệu đặc biệt để phát hiện và diệt virus) hay dựa trên so sánh lưu thông mạng hiện tại với baseline (thông số đo đặc chuẩn của hệ thống) để tìm ra các dấu hiệu khác thường. Các chức năng của IDS:

- Bảo vệ tính toàn vẹn (integrity) của dữ liệu, bảo đảm sự nhất quán của dữ liệu trong hệ thống. Các biện pháp đưa ra ngăn chặn được việc thay đổi bất hợp pháp hoặc phá hoại dữ liệu.
- Bảo vệ tính bí mật, giữ cho thông tin không bị lộ ra ngoài. Bảo vệ tính khả dụng, tức là hệ thống luôn sẵn sàng thực hiện yêu cầu truy nhập thông tin của người dùng hợp pháp.
- Bảo vệ tính riêng tư, tức là đảm bảo cho người sử dụng khai thác tài nguyên của hệ thống theo đúng chức năng, nhiệm vụ đã được phân cấp, ngăn chặn được sự truy nhập thông tin bất hợp pháp.
- Cung cấp thông tin về sự xâm nhập, đưa ra những chính sách đối phó, khôi phục, sửa chữa ...

IPS (Intrusion Prevention System – hệ thống chống xâm nhập) được định nghĩa là một phần mềm hoặc một thiết bị chuyên dụng có khả năng phát hiện xâm nhập và có thể ngăn chặn các nguy cơ gây mất an ninh mạng.

Hệ thống phát hiện lỗ hổng an ninh mạng

Hệ thống phát hiện lỗ hổng an ninh mạng là hệ thống gồm các công cụ quét và thử thăm dò tấn công mạng. Nó được người quản trị mạng dùng để phát hiện ra các lỗ hổng về an ninh mạng an toàn trước khi đưa mạng vào hoạt động và thường xuyên theo dõi để nâng cấp, và các lỗ hổng an ninh mạng.

4.7.1.3. Topo mạng

Topo của WAN mô tả cấu trúc và cách bố trí phần tử của WAN cũng như phương thức kết nối giữa chúng với nhau. Phần tử của WAN ở đây là NOC – trung tâm mạng, POP - điểm đại diện của một vùng, hay các LAN, PC, Laptop,... Các NOC, hay POP có thể là các campus LAN, hay là một WAN.

Mô hình topo giúp các nhà thiết kế WAN thực hiện việc:

- Tổ chức khảo sát
- Phân tích và quản lý trong quá trình thiết kế

Thi công hiệu quả.

- Cấu trúc, địa phương hóa mạng cần triển khai.

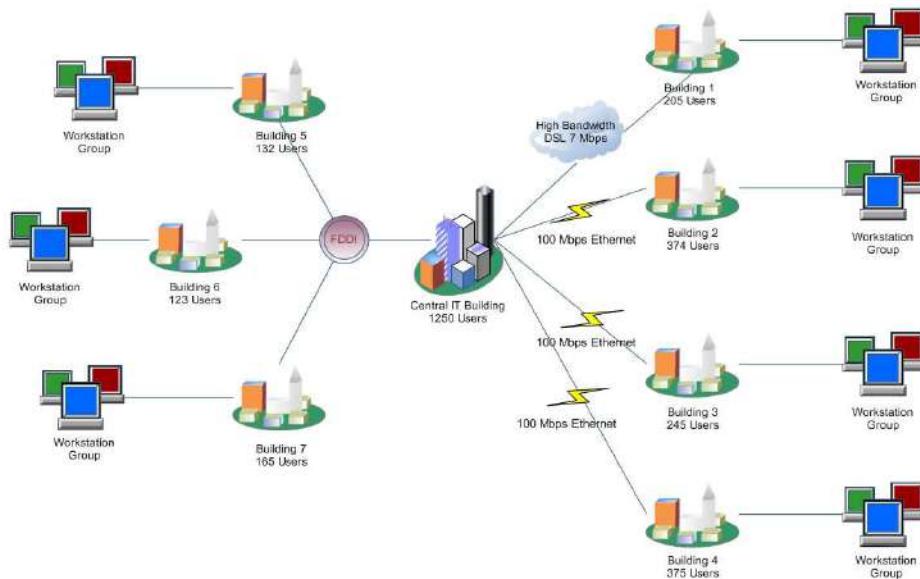
- Các mô hình chức năng của hệ thống
- Phân tích các chức năng của hệ thống để dự báo và xác định các yêu cầu trao đổi thông tin.

4.7.1.3. Mô hình ứng dụng

Mô hình ứng dụng là mô hình xây dựng trên các ứng dụng. Phân tích kết nối dựa trên các yêu cầu ứng dụng.

Tách, gộp các ứng dụng, đánh giá yêu cầu dải thông, đánh giá các yêu cầu về chất lượng dịch vụ, đánh giá yêu cầu độ tin cậy của các kết nối...

4.7.2. Phân tích một số WAN mẫu



Hình 4.22. Mô hình kết nối mạng giữa Văn phòng trung tâm và các chi nhánh

4.7.2.1. Mục tiêu hệ thống

Trụ sở chính (Main Office) đặt tại Trung tâm thông tin mạng

Tại các Trụ sở chính, hệ thống mạng được thiết kế mở, cho phép dễ dàng kết nối tới chi nhánh (Branch Office) và trụ sở khác qua nhiều cách

thức kết nối mạng điện rộng khác nhau hiện có tại Việt Nam như Leased line, vô tuyến trai phô, ISDN, Frame Relay, VPN, Dialup ...

Các hệ thống đều có độ ổn định, chính xác cao

Phải bảo toàn được đầu tư ban đầu cho hệ thống của chúng ta.

4.7.2.2. Các yêu cầu của hệ thống

Kết nối được với Internet

Có thể truy nhập vào trung tâm mạng qua mạng điện thoại công cộng PSTN

Hệ thống được thiết kế như một ISP cỡ nhỏ.

Hệ thống kết nối và truy nhập phải có tốc độ cao, hoạt động ổn định, đảm bảo các yêu cầu về bảo mật thông tin, an toàn tuyệt đối cho dữ liệu và các thông tin quan trọng

Hệ thống mạng được thiết kế và xây dựng để đảm bảo có thể đáp ứng một cách đầy đủ nhu cầu khai thác thông tin, cũng như tốc độ truy xuất thông tin từ trung tâm mạng tới các chi nhánh và tới Internet

Hỗ trợ các cách thức kết nối mạng điện rộng với các chi nhánh hiện có tại Việt Nam và tương lai như Leased line, ISDN, Frame Relay, xDSL, dialup qua mạng điện thoại công cộng ...

Có khả năng mở rộng và đáp ứng được yêu cầu của các ứng dụng đòi hỏi tốc độ cao hiện nay và trong tương lai sẽ triển khai thư viện điện tử, các ứng dụng đa phương tiện, truyền hình hội nghị, ... mà không bị phá vỡ cấu trúc thiết kế ban đầu

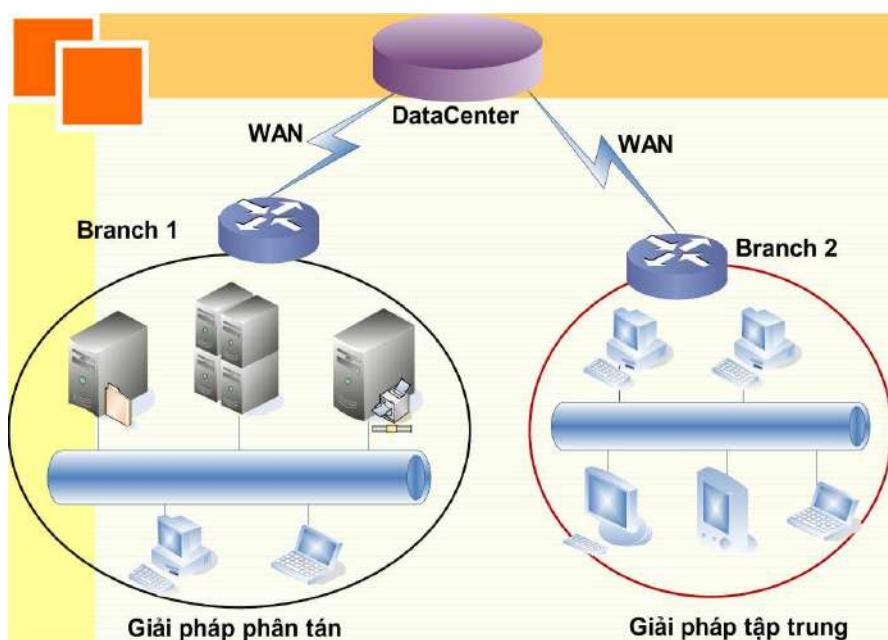
Phân mạng truy nhập các phân mạng nhỏ phải được bảo vệ qua hệ thống tường lửa thông qua chính sách an ninh chặt chẽ đối với từng phân mạng.

Đường kết nối với Internet phải đảm bảo tốc độ cao, ổn định và độ sẵn sàng cao thông qua hai kênh thuê riêng tới hai nhà cung cấp IXP/ISP khác nhau. Để có thể thực hiện các mục tiêu như Quảng bá Website: Cho phép người dùng từ ngoài Internet (bao gồm trong và ngoài Việt Nam) có thể truy nhập đến các trang Web đặt tại máy chủ trong hệ thống. Đây

chính là môi trường quảng bá thông tin, chính sách, v.v... nhanh nhất, tiện lợi nhất. Truy nhập Internet: Cho phép người sử dụng trong nội bộ mạng có khả năng truy nhập các thông tin trên Internet. Cho phép người dùng trong mạng sử dụng các dịch vụ Internet như Web, FTP, trao đổi thông tin, diễn đàn thảo luận, ... và cuối cùng là băng thông đường truyền kết nối Internet phải được đảm bảo, cho phép các hệ thống dịch vụ như Hệ thống tìm kiếm (Search Engine) dùng để thu thập thông tin trên Internet, cập nhật Website, v.v...

Các thiết bị kết nối và truy nhập được chọn lựa từ các hãng cung cấp thiết bị mạng nổi tiếng có uy tín trên thế giới như Cisco, Nortel, .. để đảm bảo độ ổn định, độ bền và dễ dàng nâng cấp khi cần thiết.

Hiện nay có 2 phương án triển khai cơ sở hạ tầng Công nghệ thông tin cho các chi nhánh là: **Giải pháp phân tán** - Đầu tư phần cứng, phần mềm tại chi nhánh và **Giải pháp tập trung** - tập trung phần cứng, phần mềm ứng dụng tại DataCenter và cung cấp dịch vụ cho chi nhánh.



Hình 4.23. Giải pháp kết nối mạng giữa các chi nhánh và văn phòng trung tâm

- *Giải pháp phân tán:* Các dịch vụ được cung cấp ngay tại chi nhánh do vậy có tính sẵn sàng cao, tuy nhiên chi phí cao. Bên cạnh chi phí phần cứng (Server, hệ thống backup, lưu trữ, router, ...), các phần mềm ứng dụng, chi phí đường truyền WAN kết nối tới DataCenter,... mỗi chi nhánh cần có bộ phận CNTT để quản lý vận hành hệ thống.
- *Giải pháp tập trung:* Có chi phí thấp hơn nhiều do không phải mua sắm thiết bị mạng, phần mềm ứng dụng mà các dịch vụ được cung cấp từ DataCenter thông qua đường truyền kết nối mạng (WAN). Bên cạnh ưu điểm về chi phí, giải pháp này còn có ưu điểm về khả năng chuẩn hóa về công nghệ, khả năng quản lý tập trung tại DataCenter. Nhược điểm của giải pháp này là số lượng các dịch vụ bị hạn chế, hiệu năng của các ứng dụng thấp do đường truyền WAN kém chất lượng (tốc độ thấp, lỗi đường truyền, ...).

Như vậy chúng ta cần thiết kế, cài đặt hệ thống mạng của chi nhánh như thế nào để có thể tạo ra một giải pháp “lai”, vừa thỏa mãn yêu cầu nghiệp vụ của doanh nghiệp, vừa tiết kiệm chi phí. Để giải quyết vấn đề này, chúng ta đi làm rõ cần phân tích các vấn đề sau:

- *Tính tập trung của dịch vụ:* Dịch vụ nào sẽ cài đặt ở DataCenter và dịch vụ nào sẽ cài đặt tại Chi nhánh?
- *Chuẩn hóa các Server:* Xây dựng các Server như thế nào (vai trò, chức năng, số lượng ...) để đảm bảo các yêu cầu dịch vụ IT của doanh nghiệp?
- *Hợp nhất các dịch vụ trên cùng một Server:* những dịch vụ nào có thể cùng được cài đặt trên cùng một Server để tiết kiệm chi phí phần cứng?
- Thiết lập các dịch vụ kết nối mạng LAN, WAN tại chi nhánh như thế nào để giải quyết vấn đề về chất lượng đường truyền cũng như khả năng dự phòng khi có sự cố xảy ra?

Các dịch vụ hệ thống: Nhóm dịch vụ cơ bản và nhóm dịch vụ mở rộng

- Nhóm dịch vụ cơ bản
 - Directory service: Cung cấp dịch vụ xác thực cho các máy client
 - Dịch vụ DHCP: Cung cấp tính năng đánh địa chỉ động (IPv4/IPv6) cho các máy client
 - Dịch vụ DNS: Phân giải tên miền cho các máy client
 - Dịch vụ file: Cung cấp các kỹ thuật để quản lý việc lưu trữ dữ liệu, đồng bộ dữ liệu, chia sẻ file và đảm bảo tốc độ tìm kiếm.
 - Dịch vụ in ấn
 - Dịch vụ máy trạm: Chống virus, truy nhập máy trạm từ xa
 - Dịch vụ quản lý: Cập nhật dữ liệu, giám sát dịch vụ, sao lưu và khôi phục dữ liệu
- Nhóm dịch vụ mở rộng
 - Dịch vụ Terminal.
 - Web caching: Cung cấp các tính năng liên quan đến việc cập Internet, ví dụ tăng tốc độ duyệt Web, proxy bảo vệ.
 - Dịch vụ email
 - Dịch vụ mang tính cộng tác, chia sẻ thông tin
 - Dịch vụ ảo hóa.
 - Dịch vụ tường lửa

Các dịch vụ kết nối mạng: Một vấn đề rất quan trọng cần xem xét là đường truyền dẫn WAN kết nối từ chi nhánh đến Datacenter. Một đường truyền WAN có tốc độ thấp, chất lượng không tốt, xác suất sự cố cao, ... là rào cản chính đối với việc triển khai dịch vụ từ DataCenter tới chi nhánh. Các dịch vụ kết nối mạng bao gồm

- Dịch vụ WAN: Cung cấp kết nối từ Chi nhánh về DataCenter
- Dịch vụ LAN: Cung cấp kết nối cho các thiết bị tại chi nhánh
- Dịch vụ đánh địa chỉ và định tuyến: EIGRP, OSPF, BGP, Static route, RIP, NAT...

- Các dịch vụ về QoS: Queuing, Dropping, Shaping,...
- Các dịch vụ bảo mật và an ninh mạng: Phòng chống tấn công, bảo đảm truyền dữ liệu tin cậy, tránh mất cáp dữ liệu.
- Dịch vụ di động: Cung cấp các kết nối cho người sử dụng ở mọi nơi thông qua các công nghệ WirelessLAN, cellular,...

Trên cơ sở các mô hình phân cấp, mô hình topo, mô hình ứng dụng, và mô hình an ninh của WAN cần thiết kế đã được xây dựng, chúng ta tiến hành các bước phân tích các yêu cầu của WAN.

Phân tích yêu cầu về hiệu năng mạng

- Từ mô hình topo chúng ta có thể tính khoảng cách kết nối, mô hình ứng dụng để dự tính dải thông, phối hợp mô hình an ninh để lựa chọn thiết bị khi đã chọn công nghệ kết nối ở phần trên. Đánh giá thời gian đáp ứng giữa các trạm hay các thiết bị trên mạng, Đánh giá độ trễ đối với các ứng dụng khi người dùng truy nhập hay yêu cầu. Đánh giá yêu cầu các đòi hỏi về băng thông của các ứng dụng trên mạng.
- Đánh giá công suất mạng đáp ứng khi người sử dụng tăng đột biến tại các điểm cổ chai. Toàn bộ các yêu cầu này cần được tối ưu chọn giải pháp hợp lý thỏa mãn các chỉ tiêu: Dịch vụ tin cậy, chi phí truyền thông tối thiểu, băng thông sử dụng tối ưu.

Phân tích các yêu cầu về quản lý mạng

Từ mô hình topo, mô hình ứng dụng, và mô hình an ninh có thể dự báo qui mô độ phức tạp của WAN, để đưa ra các yêu cầu về quản lý mạng, và đảm bảo dịch vụ, cũng như đảm bảo về an ninh mạng. Các yêu cầu về quản lý mạng cần xác định như: Phương thức - kỹ thuật quản lý mạng, phương thức quan sát hiệu năng mạng, phương thức phát hiện lỗi của mạng, và phương thức quản lý cấu hình mạng.

Phân tích các yêu cầu về an ninh - an toàn mạng

- Xác định các kiểu an ninh-an toàn.
- Xác định các yêu cầu cần bảo vệ khi kết nối với mạng ngoài, và kết nối với Internet, ...

Phân tích các yêu cầu về ứng dụng

- Từ mô hình tôpô, mô hình ứng dụng, mô hình phòng ban xác định các ứng dụng cần triển khai ngay trên mạng, dự báo các ứng dụng có khả năng triển khai trong tương lai, dự tính số người sử dụng trên từng ứng dụng, dải thông cần thiết cho từng ứng dụng, các giao thức mạng triển khai ngay và các giao thức sẽ dùng trong tương lai gần, tương lai xa, ... tính toán phân bổ tối ưu thời gian dùng mạng, ...
- Xác định các yêu cầu về ứng dụng và các ràng buộc về tài chính, thời gian thực hiện, yêu cầu về chính trị của dự án, xác định nguồn nhân lực, xác định các tài nguyên đã có và có thể tái sử dụng.

Chọn công nghệ kết nối theo các chỉ tiêu

- Giá thành và tốc độ truyền là 2 yếu tố quan trọng nhất khi lựa chọn công nghệ kết nối WAN, sau đó là độ tin cậy và khả năng đáp ứng yêu cầu dài thông của các ứng dụng.
- Chi phí cho kết nối bao gồm chi phí thiết bị, chi phí cài đặt ban đầu, đặc biệt phải xem xét là chi phí hàng tháng, chi phí duy trì hệ thống.
- Ở Việt Nam hiện nay đã có nhiều nhà cung cấp dịch vụ viễn thông, vấn đề chọn nhà cung cấp dịch vụ viễn thông nào, hay tự đầu tư là vấn đề cần cân nhắc trong thiết kế đưa ra các giải pháp kết nối khả thi.
- Xác định công nghệ kết nối, nhà cung cấp dịch vụ viễn thông
- Lựa chọn phương án kết nối WAN cho các chi nhánh
 - Dùng kết nối Leased Line
 - Dùng kết nối mạng riêng ảo (VPN – Virtual Private Network)
 - Dùng kết nối ADSL

Thực hiện lựa chọn các thiết bị phần cứng

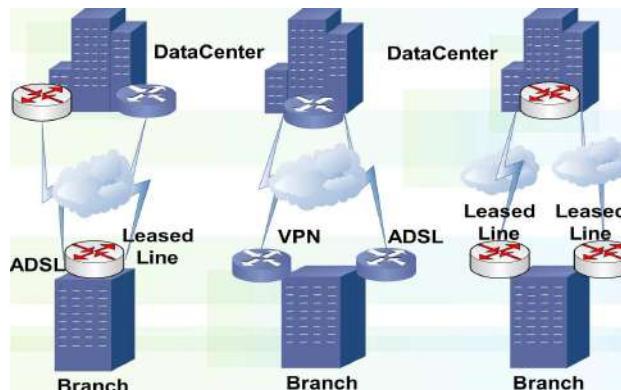
- Chọn router, chọn gateway
- Chọn modem, NTU,...

- Chọn Access server
- Chọn bộ chuyển mạch WAN
- Chọn các Server ứng dụng(Web, mail, CSDL,...)
- Lựa chọn phần mềm ứng dụng, các bộ phần mềm tích hợp,...
- Lựa chọn hệ điều hành mạng
- Lựa chọn các hệ quản trị cơ sở dữ liệu
- Lựa chọn các phương thức giao tác trên mạng

Đánh giá khả năng: Để kiểm tra thiết kế đã đưa ra chúng ta phải đánh giá được tất cả các mô hình, các phân tích, và các lựa chọn. Một trong phương pháp đánh giá sát với thực tế nhất là xây dựng Pilot thử nghiệm, hay thực hiện triển khai pha thử nghiệm với việc thể hiện các yếu tố cơ bản nhất của thiết kế.

Triển khai thử nghiệm

- Lựa chọn một phần của dự án để đưa vào triển khai thử nghiệm.
- Lập hội đồng đánh giá sau pha thử nghiệm.



Hình 4.24. Phương thức kết nối WAN cho chi nhánh

4.8. BÀI TẬP ÚNG DỤNG

Bài 1.

Mục tiêu:

Rèn luyện khả năng phân tích và thiết kế hệ thống mạng. Thông qua các yêu cầu thiết kế, bạn đọc có khả năng phân tích và đưa ra bảng đặc tả yêu cầu chi tiết.

Thiết kế giải pháp mạng thông qua sơ đồ logic và sơ đồ vật lý tổng quan.

Lập bảng dự toán kinh phí khi thiết kế và triển khai hệ thống mạng.

Yêu cầu:

Những thông tin ban đầu

- ABC là một công ty chuyên sản xuất các phần mềm liên quan đến lĩnh vực khoa học đặc biệt, gần đây công ty mở rộng hoạt động sang 1 thành phố mới và có mua 1 tòa nhà ở đây.
- Tòa nhà được xây dựng vào những năm 1940 gồm có 3 tầng. Trước khi được mua bởi Liware, mỗi tầng lầu được thuê bởi những công ty khác nhau và cấu trúc của mỗi tầng bị sửa đổi khá nhiều do những nhu cầu công việc khác nhau của mỗi công ty. Hệ thống cable hiện có là tách biệt giữa các tầng, cáp, đầu ra, bảng nối mạch được những người thuê trước đó để lại.

Tình trạng hiện tại của 3 tầng:

- Tầng 1: được cấp cho bộ phận kế toán gồm 10 phòng riêng biệt, các phòng đã có cáp UTP cat5
- Tầng 2: được cấp cho bộ phận bán hàng, thực hiện chào hàng qua điện thoại. Tầng 2 gồm 1 phòng lớn duy nhất.
- Tầng 3: cấp cho bộ phận nghiên cứu và phát triển của công ty cần sử dụng băng thông rộng và hiện tại đã được chạy cáp quang.

Công việc của bạn là thiết kế mạng cho tòa nhà để có khả năng cung cấp những tiện ích sau:

- Tại bộ phận bán hàng bên trong, được coi là trung tâm nhận các cuộc gọi đặt hàng từ khách hàng. Các nhân viên tại đây sử dụng máy tính của họ để nhập những thông tin vào trong cơ sở dữ liệu về khách hàng, tạo các hóa đơn báo hàng và cung cấp các thông

tin về sản phẩm, đơn đặt hàng có thể đặt thông qua Email hoặc điện thoại.

- Bộ phận bán hàng bên ngoài gồm những nhân viên phải đi đến làm việc với những khách hàng tiềm năng trong thành phố, cung cấp thông tin sản phẩm. những nhân viên này khi ra ngoài cũng có khả năng truy nhập CSDL bên trong công ty, có khả năng chạy thử được những phần mềm từ văn phòng công ty để chứng minh cho khách hàng thấy sản phẩm phần mềm của công ty.
- Phòng nghiên cứu và phát triển gồm những nhà khoa học và các lập trình viên làm việc cùng với nhau để có khả năng khám phá ra những ý tưởng và sản phẩm mới. Những người này cần phải sử dụng những máy tính có cấu hình mạnh và đường truyền tốc độ cao dùng cho quá trình kiểm tra các sản phẩm phần mềm của họ, như yêu cầu, phòng này phải được bảo mật tối đa để những thông tin nghiên cứu không thể lọt ra ngoài.

Những thông tin tiếp theo

- Tầng 1: gồm 10 phòng nhỏ, mỗi phòng có 1 máy PC, sử dụng cáp 100base Fast Ethernet
- Tầng 2: gồm 55 máy PC sử dụng cáp 10baset
- Tầng 3: gồm có 100 PC sử dụng cáp 100Base-FX Fast ethernet

Ba mạng LAN được kết nối đến mạng Backbone tốc độ 1000 Mbit/s Gigabit. Ethernet và sử dụng những máy tính Windows server 2003 làm router. Hệ thống Backbone này cũng được kết nối về văn phòng chính ở 1 thành phố khác sử dụng Router cung với đường truyền T-1. 1 đường T-1 khác dùng nối tòa nhà với IPS (nhà cung cấp Internet).

Từ văn phòng chính thông báo họ cũng muốn triển khai một số Web server ở tòa nhà mới. Với yêu cầu này, bạn cần phải thiết kế thêm vào một LAN khác gồm 6 Web server kết nối thông qua cáp UTP 100Base-T Fast Ethernet, một trong số các máy tính chạy Windows server 2003 có thêm 1 Lan card 1000Base-T Gigabit Etherne để làm router nối đến Backbone.

Các Web Server phải được truy nhập từ Internet và các khách hàng, những máy này phải có những IP đã đăng ký từ các nhà cung cấp. Văn phòng chính thông báo họ đã đăng ký địa chỉ mạng 207.46.230.0 từ ISP. Địa chỉ này sử dụng 3 bit để tạo ra các mạng con và tất cả các subnet đã được sử dụng bởi những công ty khác chỉ còn lại Subnet sau cùng được cấp cho tòa nhà.

3 LAN còn lại, sử dụng những địa chỉ IP dạng Private Address. Những máy tính ở 3 LAN này có thể truy nhập Internet thông qua cơ chế NAT của Router truy nhập Internet nằm trên Backbone. Các LAN sử dụng lớp địa chỉ 172.19.0.0/22 với yêu cầu với 1 và chỉ 1 subnet được cấp cho mỗi LAN.

Bài 2.

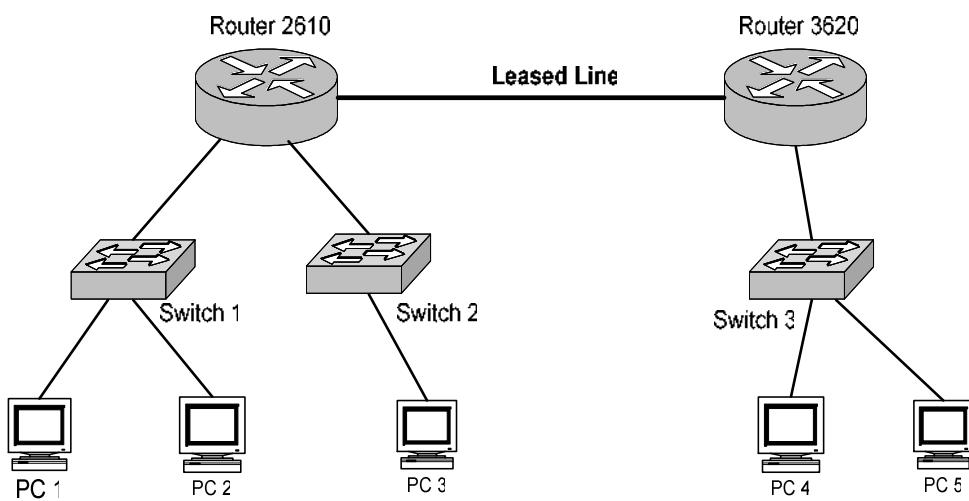
Mục tiêu:

Thực hành mô phỏng thiết kế WAN trên Packet tracer.

Yêu cầu:

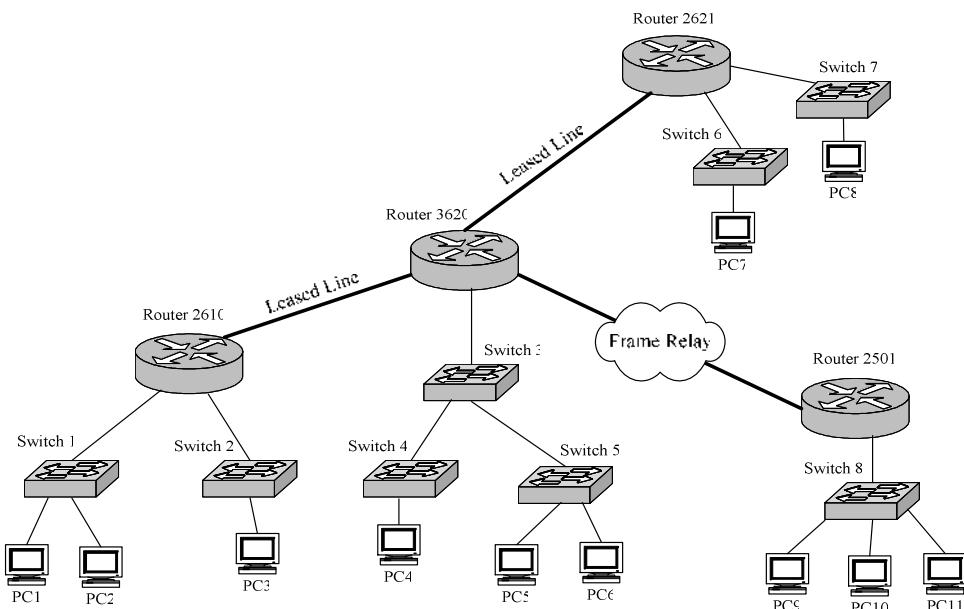
Các máy tính có cài phần mềm mô phỏng mạng **Packet Tracer 5.3**

1. Sử dụng phần mềm **Packet Tracer 5.3**, thiết kế một mạng WAN đơn giản như sau:



Sau đó định địa chỉ IP của các PC và cấu hình định tuyến tĩnh cho các Router sao cho các PC liên lạc được với nhau. Các máy trong Router 2610 thuộc lớp B, còn các máy trong Router 3620 thuộc lớp C.

2. Dùng phần mềm Packet Tracer 5.3, thiết kế mạng WAN sau:



Phân bổ địa chỉ IP cho các mạng trong Router 3620 thuộc lớp B, các mạng trong Router 2610, 2621, 2501 thuộc lớp C.

Cấu hình cho các Router sao cho tất cả các máy tính trong mạng WAN liên lạc được với nhau. Dùng các kỹ thuật định tuyến động RIP, IGRP hay OSPF

Mục tiêu:

- Đây là bài thực hành tổng hợp thiết kế mạng.
- Thiết kế một hệ thống mạng hoàn chỉnh với các kiến thức đã biết.
- Kết quả của bài thực hành là một hồ sơ thiết kế mạng đầy đủ các nội dung của qui trình thiết kế mạng.

Yêu cầu hiện trạng hệ thống mạng:

- Công ty ABC có một văn phòng chính tại thành phố Đà Nẵng và một nhà máy tại khu công nghiệp Hòa Khánh
- Việc đầu tư sẽ chia làm hai giai đoạn: Giai đoạn 1- xây dựng hệ thống mạng tại văn phòng chính. Giai đoạn 2- xây dựng hệ thống mạng tại nhà máy, kết nối hai site với nhau.
- Trụ sở văn phòng chính là một tòa nhà gồm 6 tầng, 30m x 50m. Số lượng users khoảng 200 người, chia làm 5 phòng (Marketing, Sale, CEO, IT, Acc)
- Phòng IT đặt tại lầu 3.
- Nhà máy có diện tích 1000m x 800 m, gồm một văn phòng và các phân xưởng nằm rải rác.

Yêu cầu của khách hàng

1. Xây dựng hệ thống mạng LAN cho văn phòng và mạng LAN cho nhà máy.
2. Hệ điều hành mạng chọn Windows server 2003.
3. Các dịch vụ cần đáp ứng: Active directory, mail, database SQL để chạy phần mềm kế toán, phòng chống virus, backup, Web ...
4. Có thể truy nhập wireless
5. Có có firewall ngăn cách Internal và External
6. Publish mail và web server để có thể truy nhập từ Internet
7. Chọn phương thức kết nối để nối 2 site với nhau
8. Người dùng đi công tác có thể kết nối vào văn phòng bằng VPN

4.9. CÂU HỎI ÔN TẬP

Câu 1: Trình bày hai mô hình Phân cấp và An ninh – An toàn. Phân tích đặc điểm của mỗi loại.

Câu 2: Kết nối WAN mang lại những lợi ích gì?

Câu 3: Người ta thường sử dụng công nghệ gì để kết nối WAN? Trình bày một số công nghệ kết nối WAN hiện nay.

Câu 4: So sánh 2 công nghệ kết nối WAN: ATM và Frame Relay.

Câu 5: Trình bày các giao thức trong kết nối WAN?

TÀI LIỆU THAM KHẢO

- [1] **Nguyễn Thúc Hải** (1997), Mạng máy tính và các hệ thống mở, NXB Giáo dục
- [2] **Phạm Thê Quê** (2008), Công nghệ Mạng máy tính, NXB Bưu điện
- [3] **Ngô Bá Hùng** (2005), Giáo trình Thiết kế - Cài đặt mạng, Đại học Cần Thơ
- [4] **Cisco Press Top** (2011), Down Network Design 3nd Edition
- [5] **CCIE Network Design** (Cisco)
- [6] **Wireless LAN Design** (Cisco)
- [7] **IP Network Design Guide** (June 1999), IBM
- [8] **Joshua Backfield** (2008), Network Security Mode, SANS Institute
- [9] <http://www.rhyshaden.com/ppp.htm>
- [10] http://www.interfacebus.com/Design_HDLC.html
- [11] Một số tài liệu trên Internet.

MỤC LỤC

<i>Lời nói đầu.....</i>	3
Chương 1: TỔNG QUAN VỀ THIẾT KẾ MẠNG	5
1.1. Tiến trình xây dựng mạng	5
1.1.1. Thu thập yêu cầu của khách hàng	6
1.1.2. Phân tích yêu cầu	7
1.1.3. Thiết kế giải pháp.....	8
1.1.4. Cài đặt mạng	10
1.1.5. Kiểm thử mạng.....	11
1.1.6. Bảo trì hệ thống.....	11
1.2. Câu hỏi ôn tập.....	11
Chương 2: THIẾT KẾ MẠNG CỤC BỘ.....	13
2.1. Phân loại mạng.....	13
2.1.1. Phân loại mạng theo vùng địa lý	13
2.1.2. Phân loại mạng máy tính theo topology mạng.....	14
2.1.3. Phân loại mạng máy tính theo chức năng	16
2.2. Mạng cục bộ và giao thức điều khiển truy cập đường truyền	16
2.2.1. Giao thức CSMA/CD	17
2.2.2. Giao thức truyền thẻ bài (Token passing)	17
2.2.3. Giao thức FDDI.....	18
2.3. Các loại thiết bị sử dụng trong mạng LAN	19
2.3.1. Network Adapter	19
2.3.2. Repeater.....	22
2.3.3. Hub.....	23
2.3.4. Bridge	24
2.3.5. Switch.....	27
2.3.6. Router	29
2.4. Các tổ chức chuẩn hóa về mạng	31

2.5. Mạng Ethernet	34
2.5.1. Lịch sử hình thành.....	34
2.5.2. Một số chuẩn mạng Ethernet phổ biến.....	36
2.6. Thiết kế hạ tầng cáp mạng	38
2.6.1. Các tiêu chuẩn về cáp mạng.....	40
2.6.2. Cấu trúc cáp.....	43
2.6.3. Cáp mạng	48
2.7. Kết nối LAN	53
2.7.1. Vị trí nút mạng	53
2.7.2. Vị trí đặt Hub	54
2.7.3. Chọn tuyến đường xương sống	55
2.7.4. Kết nối các workgroup tại Hub trung tâm.....	56
2.7.5. Kiểm tra phương pháp dự kiến	56
2.7.6. Liên kết các cơ sở.....	57
2.7.7. Chọn thiết bị.....	57
2.8. Hồ sơ thiết kế mạng LAN	59
2.8.1. Tài liệu lưu trữ	59
2.8.2. Chi tiết các bản ghi.....	59
2.8.3. Các bản ghi dây nối và đầu cắm.....	60
2.8.4. Quản trị hệ thống.....	60
2.8.5. Bảo trì và sửa chữa.....	61
2.9. Một số nguyên tắc hướng dẫn	61
2.9.1. Hướng dẫn ngăn cách cáp UTP khỏi nguồn có độ nhiễu từ cao.....	61
2.9.2. Bán kính uốn cong tối thiểu cho dây cáp	61
2.9.3. Khuyến cáo cable trên thực tiễn.....	62
2.9.4. Thực hành cài đặt cable UTP	63
2.9.5. Lắp đặt kết nối phần cứng sợi quang	63
2.9.6. Lắp đặt sợi cáp quang.....	64

2.10. Giới thiệu tiến trình thiết kế mạng LAN.....	64
2.10.1. Lập sơ đồ thiết kế mạng	65
2.10.2. Phát triển sơ đồ mạng ở tầng vật lý.....	65
2.10.3. Nối kết tầng 2 bằng switch.....	69
2.10.4. Thiết kế mạng ở tầng 3.....	73
2.10.5. Xác định vị trí đặt Server	74
2.10.6. Lập tài liệu cho tầng 3	75
2.11. Bài tập ứng dụng Thiết kế LAN.....	76
2.12. Câu hỏi ôn tập.....	103
Chương 3: MẠNG CỤC BỘ KHÔNG DÂY	105
3.1. Tổng quan về WLAN	105
3.1.1. Lịch sử hình thành và phát triển.....	105
3.1.2. Dải tần số không dây.....	106
3.1.3. Ưu điểm của WLAN	110
3.1.4. Nhược điểm của WLAN	110
3.2. Các chuẩn thông dụng của WLAN.....	111
3.2.1. Chuẩn IEEE 802.11b.....	112
3.2.2. Chuẩn IEEE 802.11a.....	112
3.2.3. IEEE 802.11g	113
3.2.4. Chuẩn IEEE 802.11n.....	113
3.2.5. So sánh các chuẩn IEEE 802.11x.....	115
3.3. Cấu trúc và các mô hình WLAN	119
3.3.1. Cấu trúc cơ bản của WLAN.....	119
3.3.2. Các thiết bị hạ tầng mạng không dây	120
3.3.3. Các mô hình WLAN	123
3.4. Phương pháp thiết kế và lắp đặt WLAN	126
3.4.1. Xem xét trước khi thiết kế.....	126
3.4.2. Triển khai Access Point	129
3.4.3. Các phần mềm hỗ trợ	132

3.5. Bảo mật WLAN	133
3.5.1. Tại sao phải bảo mật WLAN?.....	133
3.5.2. WEP	135
3.5.3. WLAN VPN.....	136
3.5.4. TKIP	137
3.5.5. AES	137
3.5.6. 802.1X và EAP	137
3.5.7. WPA.....	139
3.5.8. WPA2.....	140
3.5.9. Lọc (Filtering).....	140
3.5.10. Kết luận	142
3.6. Bài toán thực tế	144
3.6.1. Phân tích hiện trạng.....	144
3.6.2. Xác định công nghệ, kiến trúc mạng.....	146
3.6.3. Xác định phần cứng	148
3.6.4. Thiết kế chi tiết kết nối WLAN	151
3.6.5. Sơ đồ vị trí lắp đặt Access Point chia sẻ Internet.....	154
3.6.6. Thực thi mạng WLAN	155
3.7. Bài tập ứng dụng	156
3.8. Câu hỏi ôn tập	156
Chương 4: THIẾT KẾ MẠNG DIỆN RỘNG	157
4.1. Giới thiệu WAN	157
4.2. Các lợi ích và chi phí khi kết nối WAN	158
4.3. Những điểm cần chú ý khi thiết kế WAN	159
4.3.1. Môi trường	159
4.3.2. Các yêu cầu kỹ thuật	160
4.3.3. Bảo mật	161
4.4. Một số công nghệ kết nối WAN	161
4.4.1. Mạng chuyển mạch kênh	161

4.4.2. Mạng chuyên mạch gói	167
4.5. Giao thức kết nối WAN	181
4.5.1. Giao thức HDLC	181
4.5.2. Giao thức PPP	183
4.6. Các thiết bị kết nối WAN	184
4.6.1. Router	184
4.6.2. Access Server	184
4.6.3. Modem	185
4.6.4. CSU/DSU	186
4.6.5. Chuyển mạch WAN	186
4.6.6. ISDN Terminal Adapter	187
4.7. Thiết kế WAN	187
4.7.1. Các mô hình thiết kế WAN	187
4.7.2. Phân tích một số WAN mẫu	195
4.8. Bài tập ứng dụng	202
4.9. Câu hỏi ôn tập	207
Tài liệu tham khảo	209

Giáo trình thiết kế mạng

Chịu trách nhiệm xuất bản

NGUYỄN THỊ THU HÀ

Biên tập: NGÔ MỸ HẠNH
NGUYỄN TIẾN SỸ

Trình bày sách: NGUYỄN THANH HƯƠNG

Sửa bản in: NGUYỄN THỌ VIỆT

Thiết kế bìa: TRẦN HỒNG MINH

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

Trụ sở chính:

Số 18 Nguyễn Du, Hai Bà Trưng, Hà Nội
Điện thoại: 04.35772143; 35772145 Fax: 04.35772194
Email: nxb.tttt@mic.gov.vn
Website: www.nxbthongtintruyenthong.vn

Chi nhánh thành phố Hồ Chí Minh:

Số 8A đường D2, phường 25, Q. Bình Thạnh, TP. Hồ Chí Minh
Điện thoại: 08.35127750 Fax: 08.35127751
Email: cnsg.nxbtttt@mic.gov.vn

Chi nhánh thành phố Đà Nẵng:

42 Trần Quốc Toản, TP. Đà Nẵng
Điện thoại: 0511.3897467 Fax: 0511.3843359
Email: cndn.nxbtttt@mic.gov.vn

In 550 bản, khổ 17x24 cm tại Công ty TNHH SX và TM Thái Việt

Số đăng ký kế hoạch xuất bản 37-2011/CXB/4-920/TTTT

Số quyết định xuất bản: 80/QĐ-NXB TTTT ngày 27 tháng 4 năm 2011

In xong nộp lưu chiểu tháng 5 năm 2011.