TRUNG TÂM KHOA HỌC TỰ NHIÊN VÀ CÔNG NGHỆ QUỐC GIA
VIỆN CÔNG NGHỆ THÔNG TIN

GIÁO TRÌNH

THIẾT KẾ VÀ XÂY DỰNG MẠNG LAN VÀ WAN

Hà nội, 01/2004

MỤC LỤC

1 Chương I - Tổng quan Mạng Máy Tính

1.1 Kiến thức cơ bản

1.1.1 Sơ lược lịch sử phát triển:

Vào giữa những năm 50, những hệ thống máy tính đầu tiên ra đời sử dụng các bóng đèn điện tử nên kích thước rất cồng kềnh và tiêu tốn nhiều năng lượng. Việc nhập dữ liệu vào máy tính được thực hiện thông qua các bìa đục lỗ và kết quả được đưa ra máy in, điều này làm mất rất nhiều thời gian và bất tiện cho người sử dụng.

Đến giữa những năm 60, cùng với sự phát triển của các ứng dụng trên máy tính và nhu cầu trao đổi thông tin với nhau, một số nhà sản xuất máy tính đã nghiên cứa chế tạo thành công các thiết bị truy cập từ xa tới các máy tính của họ, và đây chính là những dạng sơ khai của hệ thống mạng máy tính.

Đến đầu những năm 70, hệ thống thiết bị đầu cuối 3270 của IBM ra đời cho phép mở rộng khả năng tính toán của các trung tâm máy tính đến các vùng ở xa. Đến giữa những năm 70, IBM đã giới thiệu một loạt các thiết bị đầu cuối được thiết kế chế tạo cho lĩnh vực ngân hàng, thương mại. Thông qua dây cáp mạng các thiết bị đầu cuối có thể truy cập cùng một lúc đến một máy tính dùng chung. Đến năm 1977, công ty Datapoint Corporation đã tung ra thị trường hệ điều hành mạng của mình là "Attache Resource Computer Network" (Arcnet) cho phép liên kết các máy tính và các thiết bị đầu cuối lại bằng dây cáp mạng, và đó chính là hệ điều hành mạng đầu tiên.

1.1.2 Khái niệm cơ bản

Nói một cách cơ bản, mạng máy tính là hai hay nhiều máy tính được kết nối với nhau theo một cách nào đó sao cho chúng có thể trao đổi thông tin qua lại với nhau.

Hình 1-1: Mô hình mạng cơ bản

Mạng máy tính ra đời xuất phát từ nhu cầu muốn chia sẻ và dùng chung dữ liệu. Không có hệ thống mạng thì dữ liệu trên các máy tính độc lập muốn chia sẻ với nhau phải thông qua việc in ấn hay sao chép qua đĩa mềm, CD ROM, … điều này

gây rất nhiều bất tiện cho người dùng. Các máy tính được kết nối thành mạng cho phép các khả năng:

- Sử dụng chung các công cụ tiện ích
- Chia sẻ kho dữ liệu dùng chung
- Tăng độ tin cậy của hệ thống
- Trao đổi thông điệp, hình ảnh,
- Dùng chung các thiết bị ngoại vi (máy in, máy vẽ, Fax, modem …)
- Giảm thiểu chi phí và thời gian đi lại.

1.1.3 Phân biệt các loại mạng

- **Phương thức kết nối mạng được sử dụng chủ yếu trong liên kết mạng: có hai phương thức chủ yếu, đó là điểm - điểm và điểm - nhiều điểm.**
  - Với phương thức "điểm - điểm", các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Mỗi máy tính có thể truyền và nhận trực tiếp dữ liệu hoặc có thể làm trung gian như lưu trữ những dữ liệu mà nó nhận được rồi sau đó chuyển tiếp dữ liệu đi cho một máy khác để dữ liệu đó đạt tới đích.
  - Với phương thức "điểm - nhiều điểm", tất cả các trạm phân chia chung một đường truyền vật lý. Dữ liệu được gửi đi từ một máy tính sẽ có thể được tiếp nhận bởi tất cả các máy tính còn lại, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi máy tính căn cứ vào đó kiểm tra xem dữ liệu có phải dành cho mình không nếu đúng thì nhận còn nếu không thì bỏ qua.
- **Phân loại mạng máy tính theo vùng địa lý:**
  - GAN (Global Area Network) kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.
  - WAN (Wide Area Network) - Mạng diện rộng, kết nối máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong cùng một châu lục. Thông thường kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.
  - MAN (Metropolitan Area Network) kết nối các máy tính trong phạm vi một thành phố. Kết nối này được thực hiện thông qua các môi trường truyền thông tốc độ cao (50-100 Mbit/s).

- LAN (Local Area Network) - Mạng cục bộ, kết nối các máy tính trong một khu vực bán kính hẹp thông thường khoảng vài trăm mét. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao ví dụ cáp đồng trục thay cáp quang. LAN thường được sử dụng trong nội bộ một cơ quan/tổ chức...Các LAN có thể được kết nối với nhau thành WAN.

➢ **Phân loại mạng máy tính theo tôpô**

- 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 phương thức "điểm - điểm".
- Mạng hình tuyến (Bus Topology): Trong dạng hình tuyến, các máy tính đều được nối vào một đường dây 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).
- 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.
- Mạng dạng kết hợp: trong thực tế tuỳ 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.

➢ **Phân loại mạng theo chức năng**

- Mạng 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 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.

➢ **Phân biệt mạng LAN-WAN**

- Địa phương hoạt động
  - Mạng LAN sử dụng trong một khu vực địa lý nhỏ.
  - Mạng WAN cho phép kết nối các máy tính ở các khu vực địa lý khác nhau, trên một phạm vi rộng.
- Tốc độ kết nối và tỉ lệ lỗi bit
  - Mạng LAN có tốc độ kết nối và độ tin cậy cao.
  - Mạng WAN có tốc độ kết nối không thể quá cao để đảm bảo tỉ lệ lỗi bit có thể chấp nhận được.
- Phương thức truyền thông:
  - Mạng LAN chủ yếu sử dụng công nghệ Ethernet, Token Ring, ATM
  - Mạng WAN sử dụng nhiều công nghệ như Chuyển mạch vòng (Circuit Switching Network), chuyển mạch gói (Packet Switching Network), ATM (Cell relay), chuyển mạch khung (Frame Relay), …

1.1.4 Mạng toàn cầu Internet:

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

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

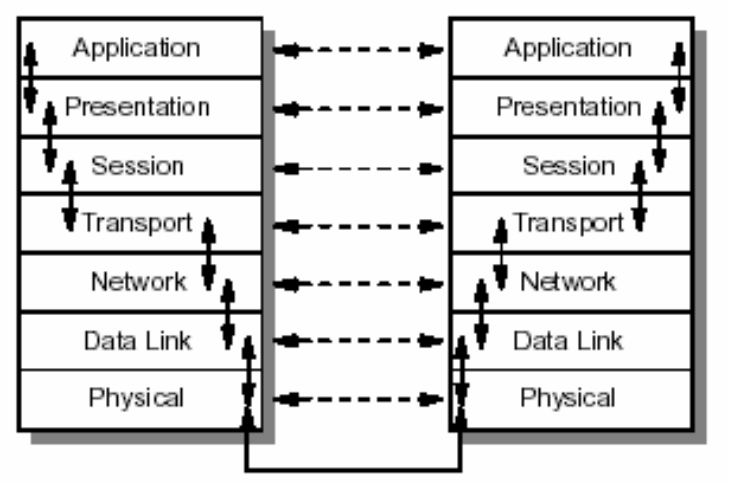
Số lượng máy tính kết nối mạng và số lượng người truy cập vào mạng Internet trên toàn thế giới ngày càng tăng lên nhanh chóng, đặc biệt từ những năm 90 trở đi. Mạng Internet không chỉ cho phép chuyển tải thông tin nhanh chóng mà còn giúp cung cấp thông tin, nó cũng là diễn đàn và là thư viện toàn cầu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

1.1.5 Mô hình OSI (Open Systems Interconnect)

Ở thời kỳ đầu của công nghệ nối mạng, việc gửi và nhận dữ liệu ngang qua mạng thường gây nhầm lẫn do các công ty lớn như IBM, Honeywell và Digital Equipment Corporation tự đề ra những tiêu chuẩn riêng cho hoạt động kết nối máy tính.

Năm 1984, tổ chức Tiêu chuẩn hoá Quốc tế - ISO (International Standard Organization) chính thức đưa ra mô hình OSI (Open Systems Interconnection), là tập hợp các đặc điểm kỹ thuật mô tả kiến trúc mạng dành cho việc kết nối các thiết bị không cùng chủng loại.

Mô hình OSI được chia thành 7 tầng, mỗi tầng bao gồm những hoạt động, thiết bị và giao thức mạng khác nhau.



Hình 1-2: Mô hình OSI bảy tầng

1.1.5.1 Các giao thức trong mô hình OSI

Trong mô hình OSI có hai loại giao thức chính được áp dụng: giao thức có liên kết (connection - oriented) và giao thức không liên kết (connectionless).

- Giao thức có liên kết: trước khi truyền dữ liệu hai tầng đồng mức cần thiết lập một liên kết logic và các gói tin được trao đổi thông qua liên kết náy, việc có liên kết logic sẽ nâng cao độ an toàn trong truyền dữ liệu.
- Giao thức không liên kết: trước khi truyền dữ liệu không thiết lập liên kết logic và mỗi gói tin được truyền độc lập với các gói tin trước hoặc sau nó.

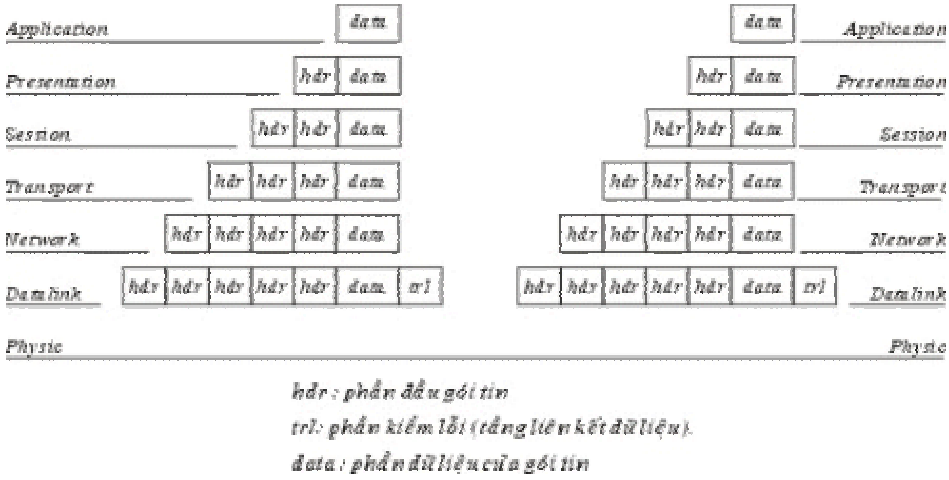
Như vậy với giao thức có liên kết, quá trình truyền thông phải gồm 3 giai đoạn phân biệt:

- Thiết lập liên kết (logic): hai thực thể đồng mức ở hai hệ thống thương lượng với nhau về tập các tham số sẽ sử dụng trong giai đoạn sau (truyền dữ liệu).
- Truyền dữ liệu: dữ liệu được truyền với các cơ chế kiểm soát và quản lý kèm theo (như kiểm soát lỗi, kiểm soát luồng dữ liệu, cắt/hợp dữ liệu...) để tăng cường độ tin cậy và hiệu quả của việc truyền dữ liệu.

– Hủy bỏ liên kết (logic): giải phóng tài nguyên hệ thống đã được cấp phát cho liên kết để dùng cho liên kết khác.

Đối với giao thức không liên kết thì chỉ có duy nhất một giai đoạn truyền dữ liệu mà thôi.

Gói tin của giao thức: Gói tin (Packet) được hiểu như là một đơn vị thông tin dùng trong việc liên lạc, chuyển giao dữ liệu trong mạng máy tính. Những thông điệp (message) trao đổi giữa các máy tính trong mạng, được tạo dạng thành các gói tin ở máy nguồn. Và những gói tin này khi đích sẽ được kết hợp lại thành thông điệp ban đầu. Một gói tin có thể chứa đựng các yêu cầu phục vụ, các thông tin điều khiển và dữ liệu.



Hình 1-3: Phương thức xác lập các gói tin trong mô hình OSI

Trên quan điểm mô hình mạng phân tầng tầng mỗi tầng chỉ thực hiện một chức năng là nhận dữ liệu từ tầng bên trên để chuyển giao xuống cho tầng bên dưới và ngược lại. Chức năng này thực chất là gắn thêm và gỡ bỏ phần đầu (header) đối với các gói tin trước khi chuyển nó đi. Nói cách khác, từng gói tin bao gồm phần đầu (header) và phần dữ liệu. Khi đi đến một tầng mới gói tin sẽ được đóng thêm một phần đầu đề khác và được xem như là gói tin của tầng mới, công việc trên tiếp diễn cho tới khi gói tin được truyền lên đường dây mạng để đến bên nhận.

Tại bên nhận các gói tin được gỡ bỏ phần đầu trên từng tầng tướng ứng và đây cũng là nguyên lý của bất cứ mô hình phân tầng nào.

1.1.5.2 Các chức năng chủ yếu của các tầng của mô hình OSI.

- **Tầng Vật lý (Physical)**

Tầng vật lý (Physical layer) là tầng dưới cùng của mô hình OSI là. Nó mô tả các đặc trưng vật lý của mạng: Các loại cáp được dùng để nối các thiết bị, các loại đầu nối được dùng , các dây cáp có thể dài bao nhiêu v.v... Mặt khác các tầng vật lý

cung cấp các đặc trưng điện của các tín hiệu được dùng để khi chuyển dữ liệu trên cáp từ một máy này đến một máy khác của mạng, kỹ thuật nối mạch điện, tốc độ cáp truyền dẫn.

Tầng vật lý không qui định một ý nghĩa nào cho các tín hiệu đó ngoài các giá trị nhị phân 0 và 1. Ở các tầng cao hơn của mô hình OSI ý nghĩa của các bit được truyền ở tầng vật lý sẽ được xác định.

Ví dụ: Tiêu chuẩn Ethernet cho cáp xoắn đôi 10 baseT định rõ các đặc trưng điện của cáp xoắn đôi, kích thước và dạng của các đầu nối, độ dài tối đa của cáp.

Khác với các tầng khác, tầng vật lý là không có gói tin riêng và do vậy không có phần đầu (header) chứa thông tin điều khiển, dữ liệu được truyền đi theo dòng bit. Một giao thức tầng vật lý tồn tại giữa các tầng vật lý để quy định về phương thức truyền (đồng bộ, phi đồng bộ), tốc độ truyền.

- **Tầng Liên kết dữ liệu (Data link)**

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

Tầng liên kết dữ liệu có hai phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức "điểm - điểm" và phương thức "điểm - điểm". Với phương thức "điểm - điểm" các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Phương thức "điểm - điểm" tất cả các máy phân chia chung một đường truyền vật lý.

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

Các giao thức tầng liên kết dữ liệu chia làm 2 loại chính là các giao thức hướng ký tư và các giao thức hướng bit. Các giao thức hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII hay EBCDIC), trong khi đó các giao thức hướng bit lại dùng các cấu trúc nhị phân (xâu bit) để xây dựng các phần tử của giao thức (đơn vị dữ liệu, các thủ tục.) và khi nhận, dữ liệu sẽ được tiếp nhận lần lượt từng bit một.

- **Tầng Mạng (Network)**

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

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

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

Việc chọn đường là sự lựa chọn một con đường để truyền một đơn vị dữ liệu (một gói tin chẳng hạn) từ trạm nguồn tới trạm đích của nó. Một kỹ thuật chọn đường phải thực hiện hai chức năng chính sau đây:

- Quyết định chọn đường tối ưu dựa trên các thông tin đã có về mạng tại thời điểm đó thông qua những tiêu chuẩn tối ưu nhất định.
- Cập nhật các thông tin về mạng, tức là thông tin dùng cho việc chọn đường, trên mạng luôn có sự thay đổi thường xuyên nên việc cập nhật là việc cần thiết.

Người ta có hai phương thức đáp ứng cho việc chọn đường là phương thức xử lý tập trung và xử lý tại chỗ.

- Phương thức chọn đường xử lý tập trung được đặc trưng bởi sự tồn tại của một (hoặc vài) trung tâm điều khiển mạng, chúng thực hiện việc lập ra các bảng đường đi tại từng thời điểm cho các nút và sau đó gửi các bảng chọn đường tới từng nút dọc theo con đường đã được chọn đó. Thông tin tổng

thể của mạng cần dùng cho việc chọn đường chỉ cần cập nhập và được cất giữ tại trung tâm điều khiển mạng.

- Phương thức chọn đường xử lý tại chỗ được đặc trưng bởi việc chọn đường được thực hiện tại mỗi nút của mạng. Trong từng thời điểm, mỗi nút phải duy trì các thông tin của mạng và tự xây dựng bảng chọn đường cho mình. Như vậy các thông tin tổng thể của mạng cần dùng cho việc chọn đường cần cập nhập và được cất giữ tại mỗi nút.

Thông thường các thông tin được đo lường và sử dụng cho việc chọn đường bao gồm:

- Trạng thái của đường truyền.
- Thời gian trễ khi truyền trên mỗi đường dẫn.
- Mức độ lưu thông trên mỗi đường.
- Các tài nguyên khả dụng của mạng.

Khi có sự thay đổi trên mạng (ví dụ thay đổi về cấu trúc của mạng do sự cố tại một vài nút, phục hồi của một nút mạng, nối thêm một nút mới... hoặc thay đổi về mức độ lưu thông) các thông tin trên cần được cập nhật vào các cơ sở dữ liệu về trạng thái của mạng.

- **Tầng Vận chuyển (Transport)**

Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên. nó là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở. Nó cùng các tầng dưới cung cấp cho người sử dụng các phục vụ vận chuyển.

Tầng vận chuyển (transport layer) là tầng cơ sở mà ở đó một máy tính của mạng chia sẻ thông tin với một máy khác. Tầng vận chuyển đồng nhất mỗi trạm bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm. Tầng vận chuyển cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi. Thông thường tầng vận chuyển đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự.

Tầng vận chuyển là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức tầng vận chuyển phụ thuộc rất nhiều vào bản chất của tầng mạng.

- **Tầng giao dịch (Session)**

Tầng giao dịch (session layer) thiết lập "các giao dịch" giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi thành phần muốn đối thoại với nhau và lập ánh xa giữa các tên với địa chỉ của chúng. Một giao dịch phải được thiết lập trước khi dữ

liệu được truyền trên mạng, tầng giao dịch đảm bảo cho các giao dịch được thiết lập và duy trì theo đúng qui định.

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

- Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách lôgic) các phiên (hay còn gọi là các hội thoại - dialogues)
- Cung cấp các điểm đồng bộ để kiểm soát việc trao đổi dữ liệu.
- Áp đặt các qui tắc cho các tương tác giữa các ứng dụng của người sử dụng.
- Cung cấp cơ chế "lấy lượt" (nắm quyền) trong quá trình trao đổi dữ liệu.

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

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

Tầng giao dịch có các hàm cơ bản sau:

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

- **Tầng Thể hiện (Presentation)**

Trong giao tiếp giữa các ứng dụng thông qua mạng với cùng một dữ liệu có thể có nhiều cách biểu diễn khác nhau. Thông thường dạng biểu diễn dùng bởi ứng dụng nguồn và dạng biểu diễn dùng bởi ứng dụng đích có thể khác nhau do các ứng dụng được chạy trên các hệ thống hoàn toàn khác nhau (như hệ máy Intel và hệ

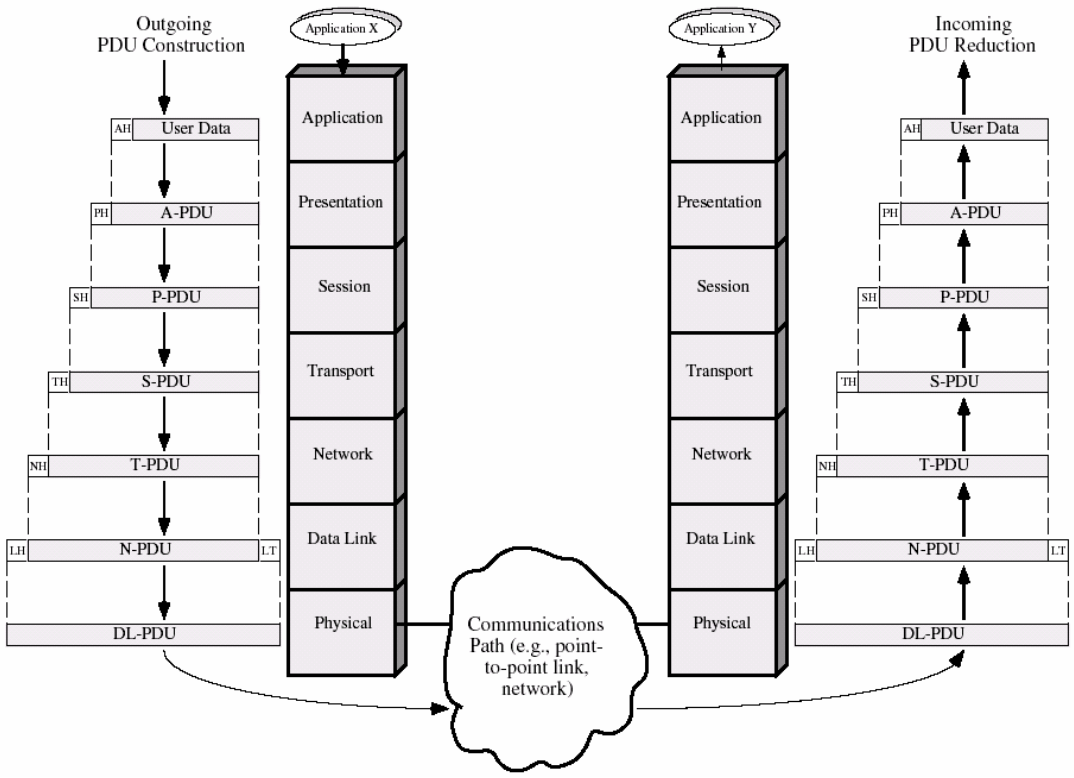
máy Motorola). Tầng thể hiện (Presentation layer) phải chịu trách nhiệm chuyển đổi dữ liệu gửi đi trên mạng từ một loại biểu diễn này sang một loại khác. Để đạt được điều đó nó cung cấp một dạng biểu diễn chung dùng để truyền thông và cho phép chuyển đổi từ dạng biểu diễn cục bộ sang biểu diễn chung và ngược lại.

Tầng thể hiện cũng có thể được dùng kĩ thuật mã hóa để xáo trộn các dữ liệu trước khi được truyền đi và giải mã ở đầu đến để bảo mật. Ngoài ra tầng thể hiện cũng có thể dùng các kĩ thuật nén sao cho chỉ cần một ít byte dữ liệu để thể hiện thông tin khi nó được truyền ở trên mạng, ở đầu nhận, tầng trình bày bung trở lại để được dữ liệu ban đầu.

- **Tầng Ứng dụng (Application)**

Tầng ứng dụng (Application layer) là tầng cao nhất của mô hình OSI, nó xác định giao diện giữa người sử dụng và môi trường OSI và giải quyết các kỹ thuật mà các chương trình ứng dụng dùng để giao tiếp với mạng.

1.1.5.3 Luồng dữ liệu trong OSI



Hình 1-4: luồng dữ liệu trong OSI (PDU: protocol data unit)

1.1.6 Một số bộ giao thức kết nối mạng

1.1.6.1 TCP/IP

- Ưu thế chính của bộ giao thức này là khả năng liên kết hoạt động của nhiều loại máy tính khác nhau.
- TCP/IP đã trở thành tiêu chuẩn thực tế cho kết nối liên mạng cũng như kết nối Internet toàn cầu.

1.1.6.2 NetBEUI

- Bộ giao thức nhỏ, nhanh và hiệu quả được cung cấp theo các sản phẩm của hãng IBM, cũng như sự hỗ trợ của Microsoft.
- Bất lợi chính của bộ giao thức này là không hỗ trợ định tuyến và sử dụng giới hạn ở mạng dựa vào Microsoft.

1.1.6.3 IPX/SPX

- Đây là bộ giao thức sử dụng trong mạng Novell.
- Ưu thế: nhỏ, nhanh và hiệu quả trên các mạng cục bộ đồng thời hỗ trợ khả năng định tuyến.

1.1.6.4 DECnet

- Đây là bộ giao thức độc quyền của hãng Digital Equipment Corporation.
- DECnet định nghĩa mô hình truyền thông qua mạng LAN, mạng MAN và WAN. Hỗ trợ khả năng định tuyến.

1.2 Bộ giao thức TCP/IP

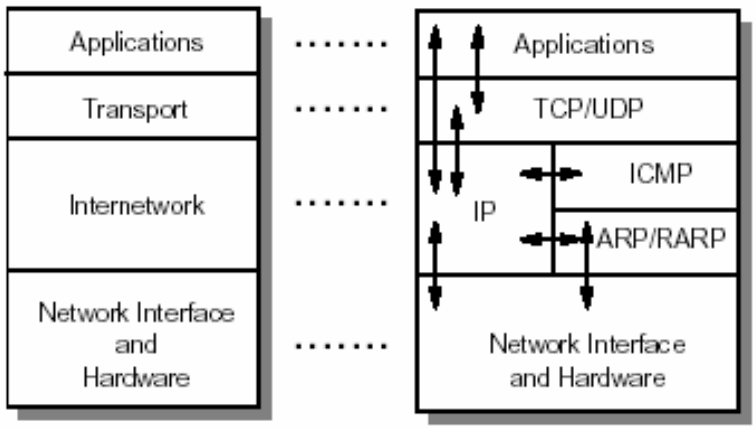
TCP/IP - Transmission Control Protocol/ Internet Protocol

1.2.1 Tổng quan về bộ giao thức TCP/IP

TCP/IP là bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau. Ngày nay, TCP/IP được sử dụng rộng rãi trong các mạng cục bộ cũng như trên mạng Internet toàn cầu.

TCP/IP được xem là giản lược của mô hình tham chiếu OSI với bốn tầng như sau:

- Tầng liên kết mạng (Network Access Layer)
- Tầng Internet (Internet Layer)
- Tầng giao vận (Host-to-Host Transport Layer)
- Tầng ứng dụng (Application Layer)



Hình 1-5: Kiến trúc TCP/IP

- **Tầng liên kết:**

Tầng liên kết (còn được gọi là tầng liên kết dữ liệu hay là tầng giao tiếp mạng) là tầng thấp nhất trong mô hình TCP/IP, bao gồm các thiết bị giao tiếp mạng và chương trình cung cấp các thông tin cần thiết để có thể hoạt động, truy nhập đường truyền vật lý qua thiết bị giao tiếp mạng đó.

- **Tầng Internet:**

Tầng Internet (còn gọi là tầng mạng) xử lý qua trình truyền gói tin trên mạng. Các giao thức của tầng này bao gồm: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Messages Protocol).

- **Tầng giao vận:**

Tầng giao vận phụ trách luồng dữ liệu giữa hai trạm thực hiện các ứng dụng của tầng trên. Tầng này có hai giao thức chính: TCP (Transmission Control Protocol) và UDP (User Datagram Protocol)

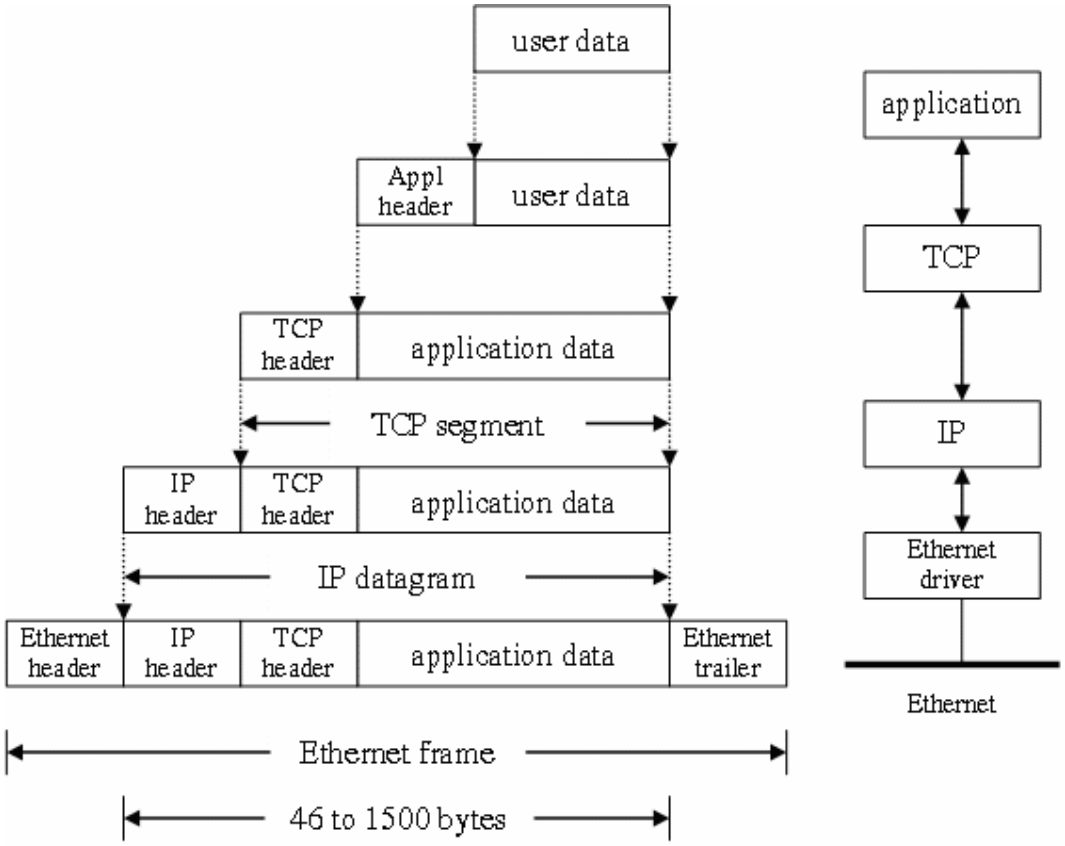
TCP cung cấp một luồng dữ liệu tin cậy giữa hai trạm, nó sử dụng các cơ chế như chia nhỏ các gói tin của tầng trên thành các gói tin có kích thước thích hợp cho tầng mạng bên dưới, báo nhận gói tin,đặt hạn chế thời gian time-out để đảm bảo bên nhận biết được các gói tin đã gửi đi. Do tầng này đảm bảo tính tin cậy, tầng trên sẽ không cần quan tâm đến nữa.

UDP cung cấp một dịch vụ đơn giản hơn cho tầng ứng dụng. Nó chỉ gửi các gói dữ liệu từ trạm này tới trạm kia mà không đảm bảo các gói tin đến được tới đích. Các cơ chế đảm bảo độ tin cậy cần được thực hiện bởi tầng trên.

- **Tầng ứng dụng:**

Tầng ứng dụng là tầng trên cùng của mô hình TCP/IP bao gồm các tiến trình và các ứng dụng cung cấp cho người sử dụng để truy cập mạng. Có rất nhiều ứng

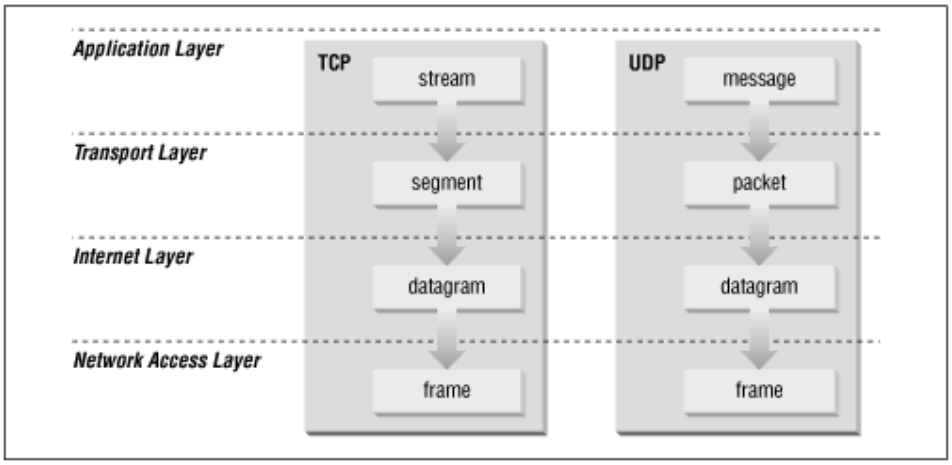
dụng được cung cấp trong tầng này, mà phổ biến là: Telnet: sử dụng trong việc truy cập mạng từ xa, FTP (File Transfer Protocol): dịch vụ truyền tệp, Email: dịch vụ thư tín điện tử, WWW (World Wide Web).



Hình 1-6: Quá trình đóng/mở gói dữ liệu trong TCP/IP

Cũng tương tự như trong mô hình OSI, khi truyền dữ liệu, quá trình tiến hành từ tầng trên xuống tầng dưới, qua mỗi tầng dữ liệu được thêm vào một thông tin điều khiển được gọi là phần header. Khi nhận dữ liệu thì quá trình xảy ra ngược lại, dữ liệu được truyền từ tầng dưới lên và qua mỗi tầng thì phần header tương ứng được lấy đi và khi đến tầng trên cùng thì dữ liệu không còn phần header nữa. Hình vẽ 1.7 cho ta thấy lược đồ dữ liệu qua các tầng. Trong hình vẽ này ta thấy tại các tầng khác nhau dữ liệu được mang những thuật ngữ khác nhau:

- Trong tầng ứng dụng dữ liệu là các luồng được gọi là stream.
- Trong tầng giao vận, đơn vị dữ liệu mà TCP gửi xuống tầng dưới gọi là TCP segment.
- Trong tầng mạng, dữ liệu mà IP gửi tới tầng dưới được gọi là IP datagram.
- Trong tầng liên kết, dữ liệu được truyền đi gọi là frame.



Hình 1-7: Cấu trúc dữ liệu trong TCP/IP

TCP/IP với OSI: mỗi tầng trong TCP/IP có thể là một hay nhiều tầng của OSI. Bảng sau chỉ rõ mối tương quan giữa các tầng trong mô hình TCP/IP với OSI

OSI	TCP/IP
Physical Layer và Data link Layer	Data link Layer
Network Layer	Internet Layer
Transport Layer	Transport Layer
Session Layer, Presentation Layer, Application Layer	Application Layer

Sự khác nhau giữa TCP/IP và OSI chỉ là:

- Tầng ứng dụng trong mô hình TCP/IP bao gồm luôn cả 3 tầng trên của mô hình OSI
- Tầng giao vận trong mô hình TCP/IP không phải luôn đảm bảo độ tin cậy của việc truyền tin như ở trong tầng giao vận của mô hình OSI mà cho phép thêm một lựa chọn khác là UDP

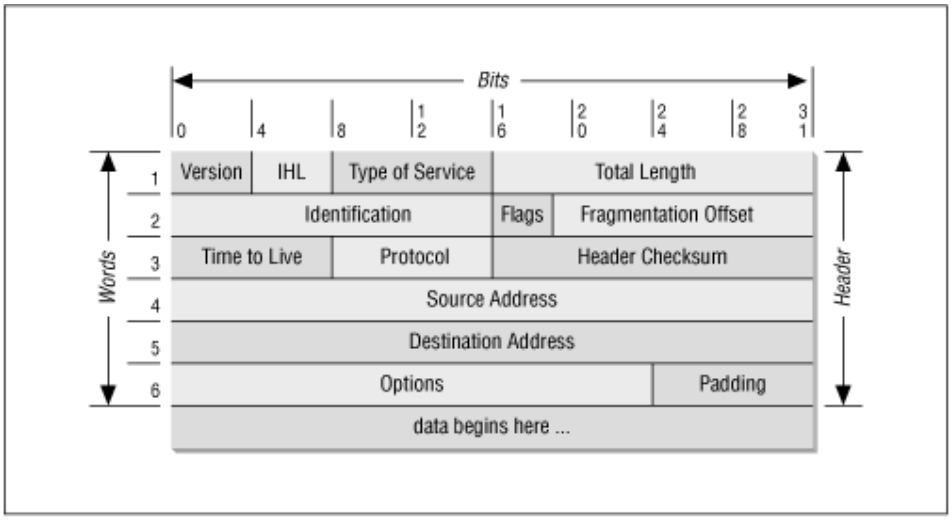
1.2.2 Một số giao thức cơ bản trong bộ giao thức TCP/IP

1.2.2.1 Giao thức liên mạng IP (Internet Protocol):

➢ **Giới thiệu chung**

Giao thức liên mạng IP là một trong những giao thức quan trọng nhất của bộ giao thức TCP/IP. Mục đích của giao thức liên mạng IP là cung cấp khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu. IP là giao thức cung cấp dịch vụ phân phát datagram theo kiểu không liên kết và không tin cậy nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu, không đảm bảo rằng IP

datagram sẽ tới đích và không duy trì bất kỳ thông tin nào về những datagram đã gửi đi. Khuôn dạng đơn vị dữ liệu dùng trong IP được thể hiện trên hình vẽ 1-7



Hình 1-8: Khuôn dạng dữ liệu trong IP

Ý nghĩa các tham số trong IP header:

- Version (4 bit): chỉ phiên bản (version) hiện hành của IP được cài đặt.
- IHL (4 bit): chỉ độ dài phần header tính theo đơn vị từ (word - 32 bit)
- Type of Service (8 bit): đặc tả tham số về yêu cầu dịch vụ
- Total length (16 bit): chỉ độ dài toàn bộ IP datagram tính theo byte. Dựa vào trường này và trường header length ta tính được vị trí bắt đầu của dữ liệu trong IP datagram.
- Indentification (16 bit): là trường định danh, cùng các tham số khác như địa chỉ nguồn (Source address) và địa chỉ đích (Destination address) để định danh duy nhất cho mỗi datagram được gửi đi bởi 1 trạm. Thông thường phần định danh (Indentification) được tăng thêm 1 khi 1 datagram được gửi đi.
- Flags (3 bit): các cờ, sử dụng trong khi phân đoạn các datagram.

0	1	2
0	DF	MF

Bit 0: reseved (chưa sử dụng, có giá trị 0)

bit 1: (DF) = 0 (May fragment)

= 1 (Don't fragment)

bit 2 : (MF) =0 (Last fragment)

=1 (More Fragment)

- Fragment Offset (13 bit): chỉ vị trí của đoạn phân mảnh (Fragment) trong datagram tính theo đơn vị 64 bit.
- TTL (8 bit): thiết lập thời gian tồn tại của datagram để tránh tình trạng datagram bị quẩn trên mạng. TTL thường có giá trị 32 hoặc 64 được giảm đi 1 khi dữ liệu đi qua mỗi router. Khi trường này bằng 0 datagram sẽ bị hủy bỏ và sẽ không báo lại cho trạm gửi.
- Protocol (8 bit): chỉ giao thức tầng trên kế tiếp
- Header checksum (16 bit): để kiểm soát lỗi cho vùng IP header.
- Source address (32 bit): địa chỉ IP trạm nguồn
- Destination address (32 bit): địa chỉ IP trạm đích
- Option (độ dài thay đổi): khai báo các tùy chọn do người gửi yêu cầu, thường là:
    - Độ an toàn và bảo mật,
    - Bảng ghi tuyến mà datagram đã đi qua được ghi trên đường truyền,
    - Time stamp,
    - Xác định danh sách địa chỉ IP mà datagram phải qua nhưng datagram không bắt buộc phải truyền qua router định trước,
    - Xác định tuyến trong đó các router mà IP datagram phải được đi qua.

➢ **Kiến trúc địa chỉ IP (IPv4)**

Địa chỉ IP (IPv4):

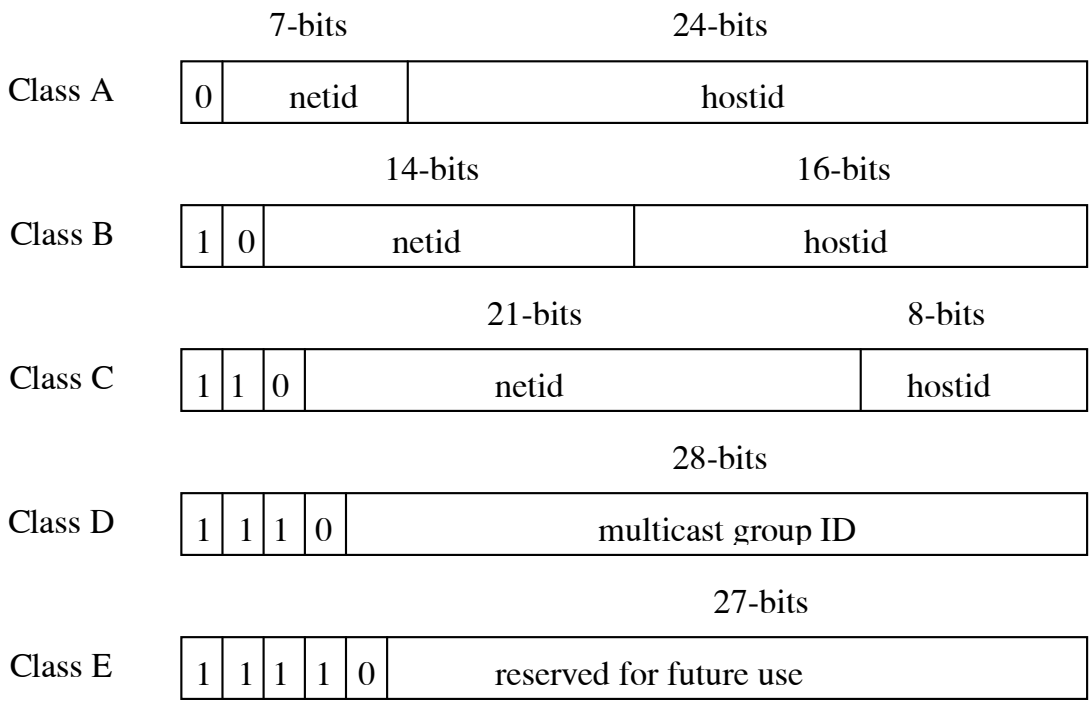
Địa chỉ IP (IPv4) có độ dài 32 bit và được tách thành 4 vùng, mỗi vùng (mỗi vùng 1 byte) thường được biểu diễn dưới dạng thập phân và được cách nhau bởi dấu chấm (.). Ví dụ: 203.162.7.92.

Địa chỉ IPv4 được chia thành 5 lớp A, B, C, D, E; trong đó 3 lớp địa chỉ A, B, C được dùng để cấp phát. Các lớp này được phân biệt bởi các bit đầu tiên trong địa chỉ.

Lớp A (0) cho phép định danh tới 126 mạng với tối đa 16 triệu trạm trên mỗi mạng. Lớp này thường được dùng cho các mạng có số trạm cực lớn (thường dành cho các công ty cung cấp dịch vụ lớn tại Mỹ) và rất khó được cấp.

Lớp B (10) cho phép định danh tới 16384 mạng với tối đa 65534 trạm trên mỗi mạng. Lớp địa chỉ này phù hợp với nhiều yêu cầu nên được cấp phát nhiều nên hiện nay đã trở nên khan hiếm.

Lớp C (110) cho phép định danh tới 2 triệu mạng với tối đa 254 trạm trên mỗi mạng. Lớp này được dùng cho các mạng có ít trạm.



Hình 1-9: Phân lớp địa chỉ IPv4

Lớp D (1110) dùng để gửi gói tin IP đến một nhóm các trạm trên mạng (còn được gọi là lớp địa chỉ multicast)

Lớp E (11110) dùng để dự phòng

Lớp	Khoảng địa chỉ
A	0.0.0.0 đến 127.255.255.255
B	128.0.0.0 đến 191.255.255.255
C	192.0.0.0 đến 223.255.255.255
D	224.0.0.0 đến 239.255.255.255
E	240.0.0.0 đến 247.255.255.255

Bảng các lớp địa chỉ Internet

Ngoài ra còn một số địa chỉ được quy định dùng riêng (private address). Các địa chỉ này chỉ có ý nghĩa trong mạng của từng tổ chức nhất định mà không được định tuyến trên Internet. Việc sử dụng các địa chỉ này không cần phải xin cấp phép.

Ví dụ: 192.168.0.0 – 192.168.255.255

Cách chuyển đổi địa chỉ IP từ dạng nhị phân sang thập phân:

Ví dụ:

Dạng Nhị phân				Dạng Thập phân
11001011	10100010	00000111	01011100	203.162.7.92

00001001	01000011	00100110	00000001	9.67.38.1

11001011.10100010.00000111.01011100 → 203.162.7.92

11001011

$2^7 + 2^6 + 2^3 + 2^1 + 2^0 = 128 + 64 + 8 + 2 + 1 = 203$

10100010

$2^7 + 2^5 + 2^1 = 128 + 32 + 2 = 162$

00000111

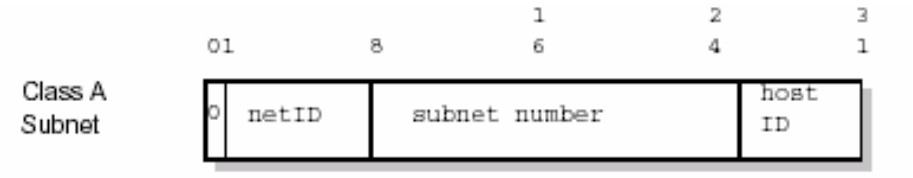
$2^2 + 2^1 + 2^0 = 4 + 2 + 1 = 7$

01011100

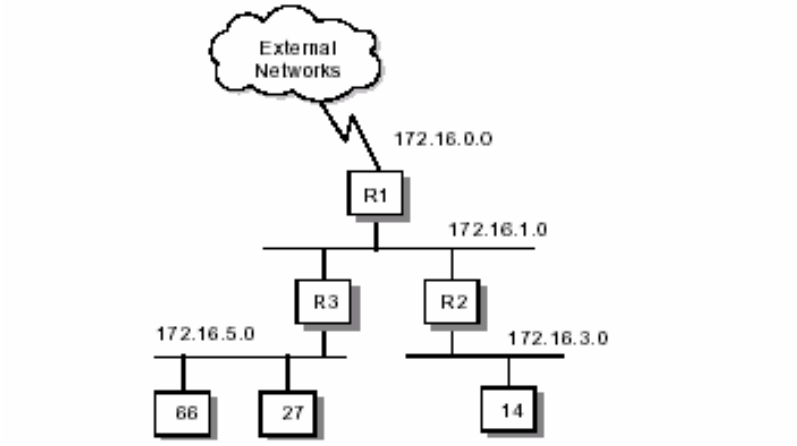
$2^6 + 2^4 + 2^3 + 2^2 = 64 + 16 + 8 + 4 = 92$

Địa chỉ mạng con:

Đối với các địa chỉ lớp A, B số trạm trong một mạng là quá lớn và trong thực tế thường không có một số lượng trạm lớn như vậy kết nối vào một mạng đơn lẻ. Địa chỉ mạng con cho phép chia một mạng lớn thành các mạng con nhỏ hơn. Người quản trị mạng có thể dùng một số bit đầu tiên của trường hostid trong địa chỉ IP để đặt địa chỉ mạng con. Chẳng hạn đối với một địa chỉ thuộc lớp A, việc chia địa chỉ mạng con có thể được thực hiện như sau:



Việc chia địa chỉ mạng con là hoàn toàn trong suốt đối với các router nằm bên ngoài mạng, nhưng nó là không trong suốt đối với các router nằm bên trong mạng.



Hình 1-10: Ví dụ minh họa cấu hình Subnet

Mặt nạ địa chỉ mạng con:

Bên cạnh địa chỉ IP, một trạm cũng cần được biết việc định dạng địa chỉ mạng con: bao nhiêu bit trong trường hostid được dùng cho phần địa chỉ mạng con (subnetid). Thông tin này được chỉ ra trong mặt nạ địa chỉ mạng con (subnet mask). Subnet mask cũng là một số 32 bit với các bit tương ứng với phần netid và subnetid được dặt bằng 1 còn các bit còn lại được đặt bằng 0.

Như vậy, địa chỉ thực của một trạm sẽ là hợp của địa chỉ IP và subnet mask.

Ví dụ với địa chỉ lớp C: 203.162.7.92, trong đó:

203.162.7 → Địa chỉ mạng

92 → Địa chỉ IP của trạm

Nếu dùng 3 bit đầu của trường hostid để đánh subnet → subnet mask sẽ là: 11111111.11111111.11111111.11100000 = 255.255.255.224

Địa chỉ của subnet:

11001011.10100010.00000111.01011100

11111111.11111111.11111111.111- - - - -

---------- AND Logic

11001011.10100010.00000111.010- - - - - = 203.162.7.64

(Subnet address)

Địa chỉ trạm: trạm thứ 28 trong Subnet 203.162.7.64

Trong thực tế subnet mask thường được viết kèm với địa chỉ IP theo dạng thu gọn sau: 203.162.7.92/27; trong đó 27 chính là số bit được đặt giá trị là 1 (gồm các bit thuộc địa chỉ mạng và các bit dùng cho Subnet). Như vậy ở đây ta có thể hiểu ngay được với subnet mask là 27 thì tương ứng với 11111111.11111111.11111111.111 - - - - -.

Các địa chỉ IP đặc biệt: có 7 loại địa chỉ IP đặc biệt được mô tả như trong bảng sau:

Địa chỉ IP			Vai trò		Mô tả
netID	subnetID	hostID	Địa chỉ nguồn	Địa chỉ đích	
0 0		0 hostID	có có	không không	Trạm hiện tại trong mạng hiện tại Trạm hostID trong mạng hiện tại
127		Bất kỳ	có	có	Địa chỉ phản hồi
1		1	không	có	Địa chỉ quảng bá giới hạn (không

					được chuyển tiếp)
netID		1	không	có	Địa chỉ quảng bá tới mạng netID
netID	subnetID	1	không	có	Địa chỉ quảng bá tới mạng con subnetID, netID
netID	1	1	không	có	Địa chỉ quảng bá tới mọi mạng con trong netID

Bảng các địa chỉ IP đặc biệt

Trong bảng trên, 0 nghĩa là tất cả các bit của trường đều bằng 0, còn 1 nghĩa là tất cả các bit của trường đều bằng 1.

- **Phân mảnh và hợp nhất các gói IP**

Phân mảnh dữ liệu là một trong những chức năng quan trọng của giao thức IP. Khi tầng IP nhận được IP datagram để gửi đi, IP sẽ so sánh kích thước của datagram với kích thước cực đại cho phép MTU (Maximum Transfer Unit), vì tầng dữ liệu qui định kích thước lớn nhất của Frame có thể truyền tải được, và sẽ phân mảnh nếu lớn hơn. Một IP datagram bị phân mảnh sẽ được ghép lại bởi tầng IP của trạm nhận với các thông tin từ phần header như identification, flag và fragment offset. Tuy nhiên nếu một phần của datagram bị mất trên đường truyền thì toàn bộ datagram phải được truyền lại.

- **Một số giao thức điều khiển**

  - Giao thức ICMP

    ICMP (Internet Control Message Protocol) là một giao thức của lớp IP, được dùng để trao đổi các thông tin điều khiển dòng số liệu, thông báo lỗi và các thông tin trạng thái khác của TCP/IP. Ví dụ:

    – Điều khiển dòng truyền (Flow Control): khi các gói dữ liệu đến quá nhanh, trạm đích hoặc một gateway ở giữa sẽ gửi một thông điệp ICMP trở lại nơi gửi, yêu cầu nơi gửi tạm thời dừng việc gửi dữ liệu.

    – Thông báo lỗi: trong trường hợp địa chỉ đích là không tới được thì hệ thống sẽ gửi một thông báo lỗi "Destination Unreachable".

    – Định hướng các tuyến đường: một gateway sẽ gửi một thông điệp ICMP "Redirect Router" để nói với một trạm là nên dùng gateway khác. Thông điệp này có thể chỉ được dùng khi mà trạm nguồn ở trên cùng một mạng với cả hai gateway.

    – Kiểm tra các trạm ở xa: một trạm có thể gửi một thông điệp ICMP "Echo" đi để biết được liệu một trạm ở xa có hoạt động hay không.

- Giao thức ARP

  ARP (Address Resolution Protocol) là giao thức giải (tra) địa chỉ để từ địa chỉ mạng xác định được địa chỉ liên kết dữ liệu (địa chỉ MAC). Ví dụ: khi IP gửi một gói dữ liệu cho một hệ thống khác trên cùng mạng vật lý Ethernet, IP cần biết địa chỉ Ethernet của hệ thống đích để tầng liên kết dữ liệu xây dựng khung. Thông thường , có thể xác định địa chỉ đó trong bảng địa chỉ IP – địa chỉ MAC ở mỗi hệ thống. Nếu không, có thể sử dụng ARP để làm việc này. Trạm làm việc gửi yêu cầu ARP (ARP_Request) đến máy phục vụ ARP Server, máy phục vụ ARP tìm trong bảng địa chỉ IP – MAC của mình và trả lời bằng ARP_Response cho trạm làm việc. Nếu không, máy phục vụ chuyển tiếp yêu cầu nhận được dưới dạng quảng bá cho tất cả các trạm làm việc trong mạng. Trạm nào có trùng địa chỉ IP được yêu cầu sẽ trả lời với địa chỉ MAC của mình.

- Giao thức RARP

  RARP (Reverse Address Resolution Protocol) là giao thức giải ngược (tra ngược) từ địa chỉ MAC để xác định IP. Quá trình này ngược lại với quá trình giải thuận địa chỉ IP – MAC mô tả ở trên.

➢ **Chọn tuyến (IP routing):**

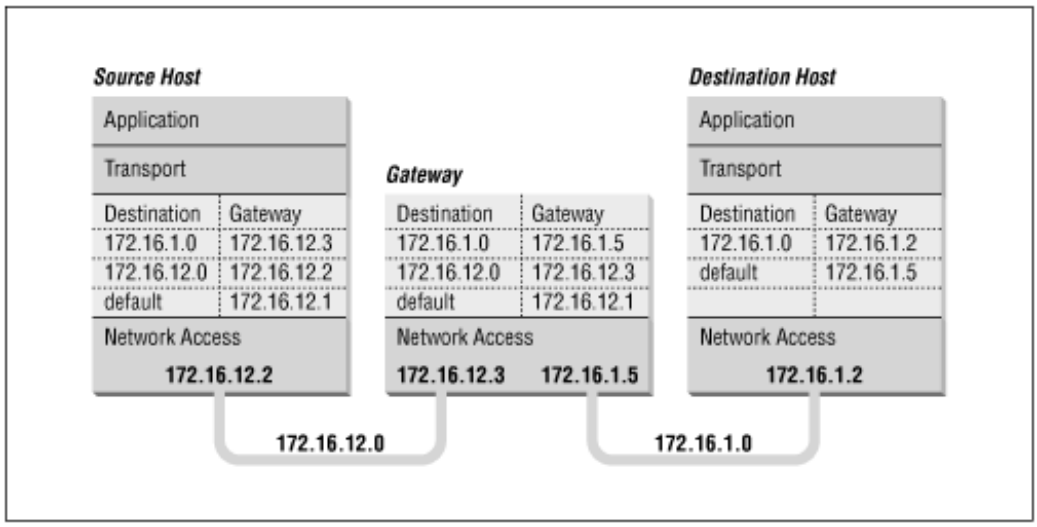
Bên cạnh việc cung cấp địa chỉ để chuyển phát các gói tin, chọn tuyến là một chức năng quan trọng của lớp IP.

Ta thấy rằng lớp IP nhận datagram từ TCP, UDP, ICMP hoặc IGMP để gửi đi hoặc nhận datagram từ giao tiếp mạng để chuyển tiếp. Lớp IP có một bảng định tuyến để truy cập mỗi khi nhận được một datagram để gửi đi. Khi một datagram được nhận từ tầng kết nối dữ liệu, đầu tiên IP sẽ kiểm tra xem địa chỉ IP đích là địa chỉ của chính nó hay một địa chỉ quảng bá, nếu đúng thì datagram sẽ được cấp phát cho giao thức đã được chỉ định trong protocol của IP header. Nếu datagram không được gửi tới địa chỉ IP này nó sẽ được chuyển tiếp trong trường hợp lớp IP được cấu hình đóng vai trò như môt router hoặc bị hủy bỏ trong trường hợp ngược lại.

IP duy trì một bảng chọn tuyến để truy nhập mỗi khi có gói tin cần chuyển tiếp. Mỗi mục trong bảng chọn tuyến gồm những thông tin sau:

- Địa chỉ IP đích: là địa chỉ đích cần tới, đó có thể là địa chỉ IP của một trạm hoặc địa chỉ IP của một mạng tùy thuộc vào cờ của đầu vào này.

- Địa chỉ IP của router kế tiếp: là địa chỉ của router được nối trực tiếp với mạng và ta có thể gửi datagram tới đó để cho router kế tiếp phân phát. Router kế tiếp không phải là đích nhưng nó có thể nhận lấy datagram được gửi tới và chuyển tiếp datagram này tới đích cuối cùng.
- Cờ: xác định địa chỉ IP của router kế tiếp là một địa chỉ một trạm hay là một mạng, router kế tiếp là một router thực hay là một trạm kết nối trực tiếp vào mạng.
- Giao tiếp mạng: xác định giao tiếp mạng nào mà datagram phải gửi qua đó để tới đích.



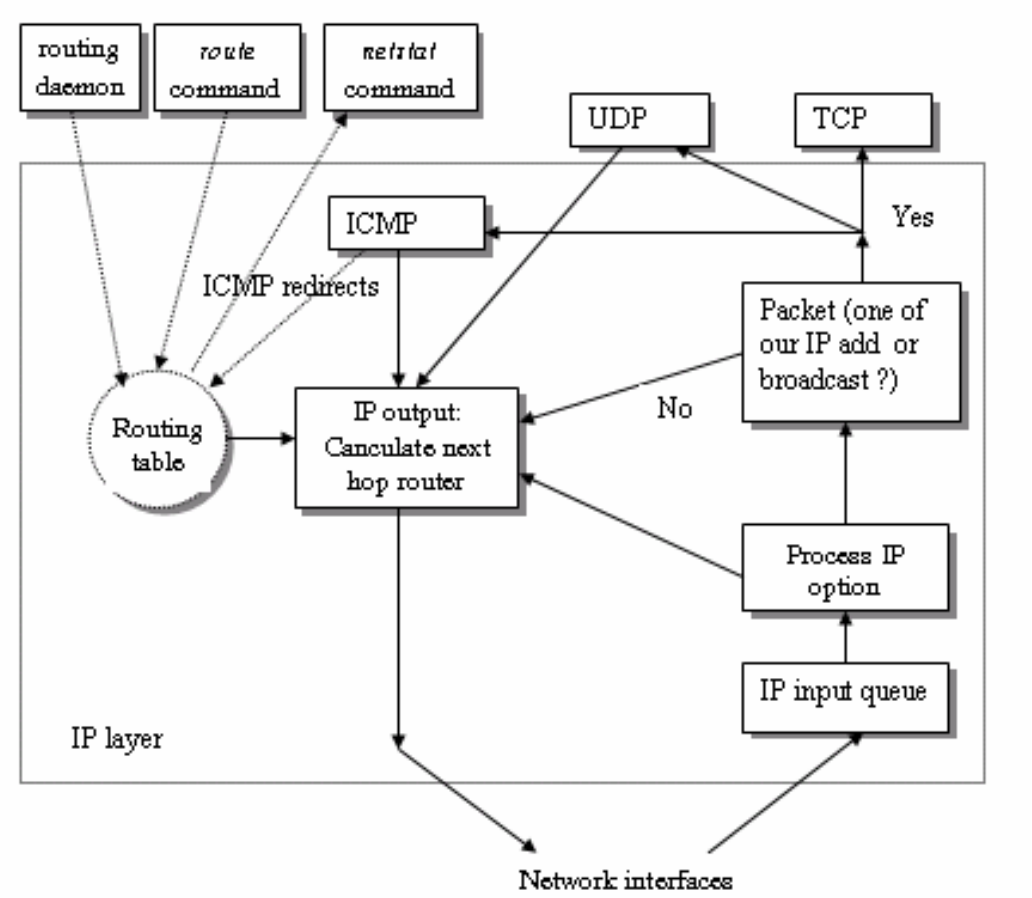
Hình 1-11: Chọn tuyến trong IP

Việc chọn tuyến của IP được thực hiện theo các trình tự sau:

- Tìm kiếm trong bảng chọn tuyến xem có mục nào khớp với địa chỉ đích (cả phần networkID và hostID). Nếu thấy thì sẽ gửi gói dữ liệu tới router kế tiếp hay giao tiếp mạng kết nối trực tiếp đã được chỉ định trong mục này.
- Tìm trong bảng chọn tuyến xem có mục nào được coi là mặc định (default). Nếu thấy thì gửi gói dữ liệu tới router kế tiếp đã được chỉ ra.

Nếu sau các bước trên mà datagram không được gửi đi thì trạm thực hiện việc chuyển tiếp gửi thông báo lỗi "host unreachable" hoặc "network unreachable" tới trạm tạo ra datagram này.

Khả năng xác định một tuyến tới một mạng mà không phải là tuyến tới một trạm là một đặc trưng cơ bản của việc chọn tuyến trong lớp giao thức IP. Điều này cho phép giảm kích thước của bảng chọn tuyến, cho phép router trên Internet chỉ có bảng chọn tuyến với hàng ngìn đầu vào thay vì hàng triệu đầu vào tới các trạm.



Hình 1-12: Quá trình xử lý thực hiện ở lớp IP

Ở đây ta cần phân biệt thêm về hai khái niệm: cơ chế chọn tuyến và chiến lược chọn tuyến. Cơ chế chọn tuyến là việc tìm kiếm trong bảng định tuyến và quyết định xem gói tin sẽ được gửi ra ngoài theo giao diện mạng nào. Cơ chế chọn tuyến được thực hiện bởi lớp IP. Chiến lược chọn tuyến là một tập hợp các luật qui định xem các tuyến nào sẽ được đưa vào bảng chọn tuyến. Chiến lược chọn tuyến được thực hiện bởi chương trình chọn tuyến (chẳng hạn routed). Chương trình chọn tuyến thực hiện việc cập nhật bảng chọn tuyến bằng cách giao tiếp với chương trình chọn tuyến của các trạm khác trong mạng. Việc giao tiếp này giữa các chương trình chọn tuyến tuân thủ thao một giao thức nhất định. Có thể tóm tắt việc chọn tuyến thực hiện ở lớp IP trong sơ đồ hình 1.12.

- **Giao thức liên mạng thế hệ mới (IPv6)**

Giao thức IPv4 đã được coi là nền tảng cho mạng Internet với những tính chất ưu việt của nó, tuy nhiên với sự bùng nổ về Internet giao thức IPv4 đã bộc lộ một số yếu điểm về tính năng, trong đó nổi bật là:

- Thiếu hụt về tính năng xác thực, an ninh của gói tin trên mạng. Khả năng mở rộng hạn chế.
- Thiếu hụt không gian địa chỉ. Với sự phát triển của mạng Internet, không gian địa chỉ IP có thể sử dụng thực sự là rất nhỏ do các địa chỉ lớp A được dành chủ yếu cho các công ty cung cấp dịch vụ lớn tại Mỹ và rất hạn chế trong việc cấp phát. Các địa chỉ lớp B nhanh chóng bị sử dụng hết do nó cung cấp số địa chỉ vừa phải. Hiện nay nhiều yêu cầu chỉ được đáp ứng bằng các địa chỉ lớp C với số địa chỉ rất hạn chế.
- Sự gia tăng số lượng các chỉ mục trong bảng định tuyến do cơ chế định tuyến không phân cấp dẫn đến yêu cầu nâng cấp các router và và định tuyến không hiệu quả.
- Ngày nay, với các nhu cầu kết nối vào mạng Internet của các dịch vụ khác như điện thoại di động, truyền hình số,… đòi hỏi giao thức IPv4 cần có các sửa đổi để đáp ứng các nhu cầu mới.

Trước những nhu cầu này, giao thức liên mạng thế hệ mới IPv6 đã ra đời nhằm thay thế cho IPv4, nhưng cho đến nay IPv6 vẫn chỉ mới chủ yếu là đang trong quá trình thử nghiệm và hoàn thiện. Trong khuôn khổ giáo trình cũng đề cập một cách tổng quát về giao thức liên mạng thế hệ mới IPv6.

Một số đặc điểm mới của IPv6:

- Khuôn dạng header mới: Header của IPv6 được thiết kế để giảm chi phí đến mức tối thiểu. Điều này đạt được bằng cách chuyển các trường lựa chọn sang các header mở rộng được đặt phía sau của IPv6 header. Khuôn dạng mới của IPv6 tạo ra sự xử lý hiệu quả hơn tại các router.
- Header của IPv4 và IPv6 không thể xử lý chung. Một trạm hay một router phải cài đặt cả IPv4 và IPv6 để có thể xử lý được cả hai khuôn dạng header này. Header của IPv6 chỉ có kích thước gấp 2 lần header của IPv4 mặc dù không gian địa chỉ của IPv6 lớn gấp 4 lần không gian địa chỉ IPv4.
- Không gian địa chỉ lớn: IPv6 có địa chỉ nguồn và đích dài 128 bit. Mặc dù 128 bit có thể tạo ra hơn 3.4x1038 tổ hợp, không gian địa chỉ của IPv6 được thiết kế cho phép phân bổ địa chỉ và mạng con từ trục xương sống Internet đến từng mạng con trong một tổ chức.
- Hiện tại chỉ một lượng nhỏ các địa chỉ hiện đang được phân bổ để sử dụng bởi các trạm, vẫn còn dư thừa rất nhiều địa chỉ sẵn sàng cho việc sử dụng trong tương lai.

- Hiệu quả, phân cấp địa chỉ hóa và hạ tầng định tuyến: Các địa chỉ toàn cục của IPv6 được thiết kế để tạo ra mọt hạ tầng định tuyến hiệu quả, phân cấp và có thể tổng quát hóa dựa trên sự phân cấp thường thấy của các nhà cung cấp dịch vụ (ISP) trên thực tế.
- Hỗ trợ chất lượng dịch vụ (QoS) tốt hơn: Các trường mới trong header của IPv6 định ra cách thức xử lý và định danh trên mạng. Giao thông trên mạng được định danh nhờ trường gán nhãn luồng (Flow Label) cho phép router có thể nhận ra và cung cấp các xử lý đặc biệt đối với các gói tin thuộc về một luồng nhất định, một chuẩn các gói tin giữa nguồn và đích. Do giao thông mạng được xác định trong header, các dịch vụ QoS có thể được thực hiện ngay cả khi phần dữ liệu được mã hóa theo IPSec.
- Khả năng mở rộng: IPv6 có thể dễ dàng mở rộng thêm các tính năng mới bằng việc thêm các header mới sau header IPv6.

- Kiến trúc địa chỉ trong IPv6:

  Không gian địa chỉ:

  - IPv6 sử dụng địa chỉ có độ dài lớn hơn IPv4 (128 bit so với 32 bit) do đó cung cấp không gian địa chỉ lớn hơn rất nhiều. Trong khi không gian địa chỉ 32 bit của IPv4 cho phép khoảng 4 tỷ địa chỉ, không gian địa chỉ của IPv6 có thể có khoảng 3.4x1038 địa chỉ. Số lượng điac hỉ này rất lớn, hỗ trợ khoảng 6.5x1023 địa chỉ trên mỗi mét vuông bề mặt trái đất. Địa chỉ IPv6 128 bit được chia thành các miền phân cấp theo trật tự trên Internet. Nó tạo ra nhiều mức phân cấp và linh hoạt trong địa chỉ hóa và định tuyến còn đang thiếu trong IPv4.
  - Không gian địa chỉ IPv6 được chia trên cơ sở các bit đầu trong địa chỉ. Trường có độ dài thay đổi bao gồm các bit đầu tiên trong địa chỉ gọi là tiền tố định dạng (Format Prefix) FP.
  - Ban đầu chỉ mới có 15% lượng địa chỉ được sử dụng, 85% còn lại để dùng trong tương lai.
  - Các tiền tố định dạng từ 001 đến 111, ngoại trừ kiểu địa chỉ multicast (1111 1111) đều bắt buộc có định danh giao diện theo khuôn dạng EUI-64.
  - Các địa chỉ dự trữ không lẫn với các địa chỉ chưa cấp phát. Chúng chiếm 1/256 không gian địa chỉ (FP = 0000 0000) và dùng cho các địa chỉ chưa chỉ định, địa chỉ quay vòng và các địa chỉ IPv6 có nhúng IPv4

  Cú pháp địa chỉ:

Các địa chỉ IPv6 dài 128 bit, khi viết mỗi nhóm 16 bit được biểu diễn thành một số nguyên không dấu dưới dạng hệ 16 và được phân tách bởi dấu hai chấm (:),

Ví dụ: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Trên thực tế địa chỉ IPv6 thường có nhiều số 0, ví dụ địa chỉ: 1080:0000:0000:0000:0008:0800:200C:417A. Do đó cơ chế nén địa chỉ được dùng để biểu diễn dễ dàng hơn các loại địa chỉ dạng này. Ta không cần viết các số 0 ở đầu mỗi nhóm, ví dụ 0 thay cho 0000, 20 thay cho 0020. Địa chỉ trong ví dụ trên sẽ trở thành 1080:0:0:0:8:800:200C:417A.

Hơn nữa ta có thể sử dụng ký hiệu :: để chỉ một chuỗi số 0. Địa chỉ trong ví dụ trên sẽ trở thành: 1080::8:800:200C:417A. Do địa chỉ IPv6 có độ dài cố định, ta có thể tính được số các bit 0 mà ký hiệu đó biểu diễn.

Tiền tố địa chỉ IPv6 được biểu diễn theo ký pháp CIDR như IPv4 như sau:

IPv6-address/prefix length

trong đó IPv6-address là bất kỳ kiểu biểu diễn nào, còn prefix length là độ dài tiền tố theo bit.

Ví dụ: biểu diễn mạng con có tiền tố 80 bit: 1080:0:0:0:8::/80.

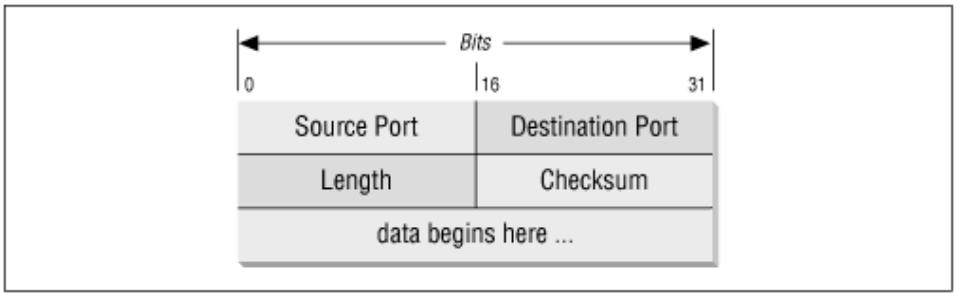
Với node address: 12AB:0:0:CD30:123:4567:89AB:CDEF,

prefix: 12AB:0:0:CD30::/60 có thể viết tắt thành

12AB:0:0:CD30:123:4567:89AB:CDEF/60

1.2.2.2 Giao thức UDP (User Datagram Protocol)

UDP là giao thức không liên kết, cung cấp dịch vụ giao vận không tin cậy được, sử dụng thay thế cho TCP trong tầng giao vận . Khác với TCP, UDP không có chức năng thiết lập và giải phóng liên kết, không có cơ chế báo nhận (ACK), không sắp xếp tuần tự các đơn vị dữ liệu (datagram) đến và có thể dẫn đến tình trạng mất hoặc trùng dữ liệu mà không hề có thông báo lỗi cho người gửi. Khuôn dạng của UDP datagram được mô tả như sau :



Hình 1-13: Khuôn dạng UDP datagram

- Số hiệu cổng nguồn (Source Port - 16 bit): số hiệu cổng nơi đã gửi datagram
- Số hiệu cổng đích (Destination Port - 16 bit): số hiệu cổng nơi datagram được chuyển tới
- Độ dài UDP (Length - 16 bit): độ dài tổng cổng kể cả phần header của gói UDP datagram.
- UDP Checksum (16 bit): dùng để kiểm soát lỗi, nếu phát hiện lỗi thì UDP datagram sẽ bị loại bỏ mà không có một thông báo nào trả lại cho trạm gửi.

UDP có chế độ gán và quản lý các số hiệu cổng (port number) để định danh duy nhất cho các ứng dụng chạy trên một trạm của mạng. Do có ít chức năng phức tạp nên UDP có xu thế hoạt động nhanh hơn so với TCP. Nó thường dùng cho các ứng dụng không đòi hỏi độ tin cậy cao trong giao vận.

1.2.2.3 Giao thức TCP (Transmission Control Protocol)

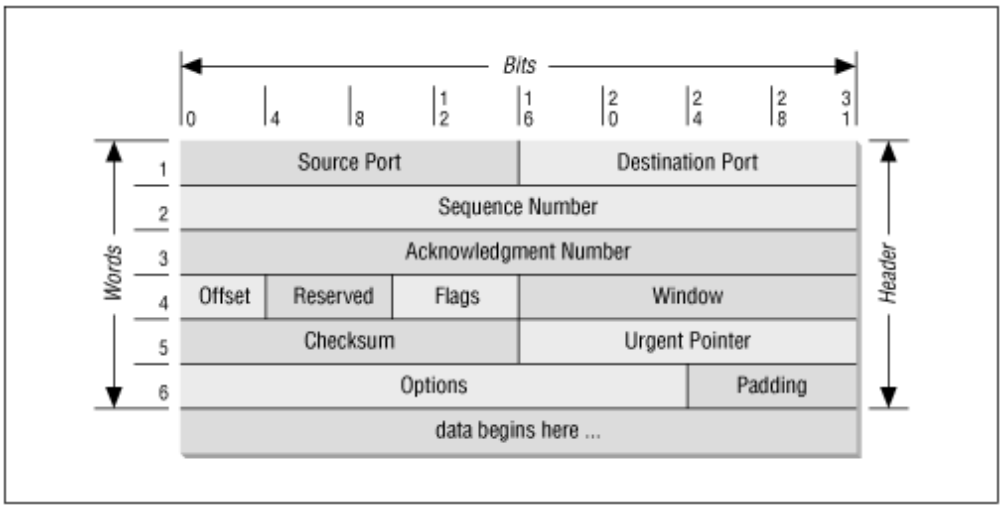
TCP và UDP là 2 giao thức ở tầng giao vận và cùng sử dụng giao thức IP trong tầng mạng. Nhưng không giống như UDP, TCP cung cấp dịch vụ liên kết tin cậy và có liên kết.

Có liên kết ở đây có nghĩa là 2 ứng dụng sử dụng TCP phải thiết lập liên kết với nhau trước khi trao đổi dữ liệu. Sự tin cậy trong dịch vụ được cung cấp bởi TCP được thể hiện như sau:

- Dữ liệu từ tầng ứng dụng gửi đến được được TCP chia thành các segment có kích thước phù hợp nhất để truyền đi .
- Khi TCP gửi 1 segment, nó duy trì một thời lượng để chờ phúc đáp từ trạm nhận. Nếu trong khoảng thời gian đó phúc đáp không tới được trạm gửi thì segment đó được truyền lại.
- Khi TCP trên trạm nhận nhận dữ liệu từ trạm gửi nó sẽ gửi tới trạm gửi 1 phúc đáp tuy nhiên phúc đáp không được gửi lại ngay lập tức mà thường trễ một khoảng thời gian .
- TCP duy trì giá trị tổng kiểm tra (checksum) trong phần Header của dữ liệu để nhận ra bất kỳ sự thay đổi nào trong quá trình truyền dẫn. Nếu 1 segment bị lỗi thì TCP ở phía trạm nhận sẽ loại bỏ và không phúc đáp lại để trạm gửi truyền lại segment bị lỗi đó.

Giống như IP datagram, TCP segment có thể tới đích một cách không tuần tự. Do vậy TCP ở trạm nhận sẽ sắp xếp lại dữ liệu và sau đó gửi lên tầng ứng dụng đảm bảo tính đúng đắn của dữ liệu.

Khi IP datagram bị trùng lặp TCP tại trạm nhận sẽ loại bỏ dữ liệu trùng lặp đó .



Hình 1-14: Khuôn dạng TCP segment

TCP cũng cung cấp khả năng điều khiển luồng. Mỗi đầu của liên kết TCP có vùng đệm (buffer) giới hạn do đó TCP tại trạm nhận chỉ cho phép trạm gửi truyền một lượng dữ liệu nhất định (nhỏ hơn không gian buffer còn lại). Điều này tránh xảy ra trường hợp trạm có tốc độ cao chiếm toàn bộ vùng đệm của trạm có tốc độ chậm hơn.

Khuôn dạng của TCP segment được mô tả trong hình 1.14

Các tham số trong khuôn dạng trên có ý nghĩa như sau:

- Source Port (16 bits) là số hiệu cổng của trạm nguồn .
- Destination Port (16 bits) là số hiệu cổng trạm đích .
- Sequence Number (32 bits) là số hiệu byte đầu tiên của segment trừ khi bit SYN được thiết lập. Nếu bit SYN được thiết lập thì sequence number là số hiệu tuần tự khởi đầu ISN (Initial Sequence Number) và byte dữ liệu đầu tiên là ISN + 1. Thông qua trường này TCP thực hiện việc quản lí từng byte truyền đi trên một kết nối TCP.
- Acknowledgment Number (32 bits). Số hiệu của segment tiếp theo mà trạm nguồn đang chờ để nhận và ngầm định báo nhận tốt các segment mà trạm đích đã gửi cho trạm nguồn .
- Header Length (4 bits). Số lượng từ (32 bits) trong TCP header, chỉ ra vị trí bắt đầu của vùng dữ liệu vì trường Option có độ dài thay đổi. Header length có giá trị từ 20 đến 60 byte .
- Reserved (6 bits). Dành để dùng trong tương lai .
- Control bits : các bit điều khiển

URG : xác đinh vùng con trỏ khẩn có hiệu lực.

ACK : vùng báo nhận ACK Number có hiệu lực.

PSH : chức năng PUSH.

RST : khởi động lại liên kết.

SYN : đồng bộ hoá các số hiệu tuần tự (Sequence number).

FIN : không còn dữ liệu từ trạm nguồn.

- Window size (16 bits) : cấp phát thẻ để kiểm soát luồng dữ liệu (cơ chế cửa sổ trượt). Đây chính là số lượng các byte dữ liệu bắt đầu từ byte được chỉ ra trong vùng ACK number mà trạm nguồn sẵn sàng nhận.
- Checksum (16 bits). Mã kiểm soát lỗi cho toàn bộ segment cả phần header và dữ liệu.
- Urgent Pointer (16 bits). Con trỏ trỏ tới số hiệu tuần tự của byte cuối cùng trong dòng dữ liệu khẩn cho phép bên nhận biết được độ dài của dữ liệu khẩn. Vùng này chỉ có hiệu lực khi bit URG được thiết lập.
- Option (độ dài thay đổi). Khai báo các tuỳ chọn của TCP trong đó thông thường là kích thước cực đại của 1 segment: MSS (Maximum Segment Size).
- TCP data (độ dài thay đổi). Chứa dữ liệu của tầng ứng dụng có độ dài ngầm định là 536 byte . Giá trị này có thể điều chỉnh được bằng cách khai báo trong vùng Option.

1.3 Giới thiệu một số các dịch vụ cơ bản trên mạng

1.3.1 Dịch vụ truy nhập từ xa Telnet

Telnet cho phép người sử dụng đăng nhập từ xa vào hệ thống từ một thiết bị đầu cuối nào đó trên mạng. Với Telnet người sử dụng hoàn toàn có thể làm việc với hệ thống từ xa như thể họ đang ngồi làm việc ngay trước màn hình của hệ thống. Kết nối Telnet là một kết nối TCP dùng để truyền dữ liệu với các thông tin điều khiển.

1.3.2 Dịch vụ truyền tệp (FTP)

Dịch vụ truyền tệp (FTP) là một dịch vụ cơ bản và phổ biến cho phép chuyển các tệp dữ liệu giữa các máy tính khác nhau trên mạng. FTP hỗ trợ tất cả các dạng tệp, trên thưc tế nó không quan tâm tới dạng tệp cho dù đó là tệp văn bản mã ASCII hay các tệp dữ liệu dạng nhị phân. Với cấu hình của máy phục vụ FTP, có thể qui định quyền truy nhập của người sử dụng với từng thư mục lưu trữ dữ liệu, tệp dữ

liệu cũng như giới hạn số lượng người sử dụng có khả năng cùng một lúc có thể truy nhập vào cùng một nơi lưu trữ dữ liệu.

1.3.3 Dịch vụ Gopher

Trước khi Web ra đời Gopher là dịch vụ rất được ưa chuộng. Gopher là một dịch vụ chuyển tệp tương tự như FTP, nhưng nó hỗ trợ người dùng trong việc cung cấp thông tin về tài nguyên. Client Gopher hiển thị một thực đơn, người dùng chỉ việc lựa chọn cái mà mình cần. Kết quả của việc lựa chọn được thể hiện ở một thực đơn khác.

Gopher bị giới hạn trong kiểu các dữ liệu. Nó chỉ hiển thị dữ liệu dưới dạng mã ASCII mặc dù có thể chuyển dữ liệu dạng nhị phân và hiển thị nó bằng một phần mềm khác.

1.3.4 Dịch vụ WAIS

WAIS (Wide Area Information Serves) là một dịch vụ tìm kiếm dữ liệu. WAIS thường xuyên bắt đầu việc tìm kiếm dữ liệu tại thư mục của máy chủ, nơi chứa toàn bộ danh mục của các máy phục vụ khác. Sau đó WAIS thực hiện tìm kiếm tại máy phục vụ thích hợp nhất. WAIS có thể thực hiện công việc của mình với nhiều loại dữ liệu khác nhau như văn bản ASCII, PostScript, GIF, TIFF, điện thư …

1.3.5 Dịch vụ World Wide Web

World Wide Web (WWW hay Web) là một dịch vụ tích hợp, sử dụng đơn giản và có hiệu quả nhất trên Internet. Web tích hợp cả FTP, WAIS, Gopher. Trình duyệt Web có thể cho phép truy nhập vào tất cả các dịch vụ trên.

Tài liệu WWW được viết bằng ngôn ngữ HTML (HyperText Markup Language) hay còn gọi là ngôn ngữ đánh dấu siêu văn bản. Siêu văn bản là văn bản bình thường cộng thêm một số lệnh định dạng. HTML có nhiều cách liên kết với các tài nguyên FTP, Gopher server, WAIS server và Web server. Web Server là máy phục vụ Web, đáp ứng các yêu cầu về truy nhập tài liệu HTML. Web Server trao đổi các tài liệu HTML bằng giao thức HTTP (HyperText Transfer Protocol) hay còn gọi là giao thức truyền siêu văn bản.

Trình duyệt Web (Web client) là chương trình để xem các tài liệu Web. Trình duyệt Web gửi các URL đến máy phục vụ Web sau đó nhận trang Web từ máy phục vụ Web dịch và hiển thị chúng. Khi giao tiếp với máy phục vụ Web thì trình duyệt Web sử dụng giao thức HTTP. Khi giao tiếp với một Gopher server thì trình duyệt Web hoạt động như một Gopher client và sử dụng giao thức gopher, khi

giao tiếp với một FTP server thì trình duyệt Web hoạt động như một FTP client và dùng giao thức FTP. Trình duyệt Web có thể thực hiện các công việc khác như ghi trang Web vào đĩa, gửi Email, tìm kiếm xâu ký tự trên trang Web, hiển thị tệp HTML nguồn của trang Web, v.v… Hiện nay có hai trình duyệt Web được sử dụng nhiều nhất là Internet Explorer và Netscape, ngoài ra còn một số trình duyệt khác như Opera, Mozila, …

1.3.6 Dịch vụ thư điện tử (E-Mail)

Dịch vụ thư điện tử (hay còn gọi là điện thư) là một dịch vụ thông dụng nhất trong mọi hệ thống mạng dù lớn hay nhỏ. Thư điện tử được sử dụng rộng rãi như một phương tiện giao tiếp hàng ngày trên mạng nhờ tính linh hoạt và phổ biến của nó. Từ các trao đổi thư tín thông thường, thông tin quảng cáo, tiếp thị, đến những công văn, báo cáo, hay kể cả những bản hợp đồng thương mại, chứng từ, … tất cả đều được trao đổi qua thư điện tử.

Một hệ thống điện thư được chia làm hai phần, MUA (Mail User Agent) và MTA (Message Transfer Agent). MUA thực chất là một chương trình làm nhiệm vụ tương tác trực tiếp với người dùng cuối, giúp họ nhận thông điệp, soạn thảo thông điệp, lưu các thông điệp và gửi thông điệp. Nhiệm vụ của MTA là định tuyến thông điệp và xử lý các thông điệp đến từ hệ thống của người dùng sao cho các thông điệp đó đến được đúng hệ thống đích.

- **Địa chỉ điện thư**

Hệ thống điện thư hoạt động cũng giống như một hệ thống thư bưu điện. Một thông điệp điện tử muốn đến được đích thì địa chỉ người nhận là một yếu tố không thể thiếu. Trong một hệ thống điện thư mỗi người có một địa chỉ thư. Từ địa chỉ thư sẽ xác định được thông tin của người sở hữu địa chỉ đó trong mạng. Nói chung, không có một qui tắc thống nhất cho việc đánh địa chỉ thư, bởi vì mỗi hệ thư lại có thể sử dụng một qui ước riêng về địa chỉ. Để giải quyết vấn đề này, người ta thường sử dụng hai khuôn dạng địa chỉ là địa chỉ miền (Domain-base address) và địa chỉ UUCP (UUCP address, được sử dụng nhiều trên hệ điều hành UNIX). Ngoài hai dạng địa chỉ trên, còn có một dạng địa chỉ nữa tạo thành bởi sự kết hợp của cả hai dạng địa chỉ trên, gọi là địa chỉ hỗn hợp.

Địa chỉ miền là dạng địa chỉ thông dụng nhất. Không gian địa chỉ miền có cấu trúc hình cây. Mỗi nút của cây có một nhãn duy nhất cũng như mỗi người dùng có một địa chỉ thư duy nhất. Các địa chỉ miền xác định địa chỉ đích tuyệt đối của người

nhận. Do đó, dạng địa chỉ này dễ sử dụng đối với người dùng: họ không cần biết đích xác đường đi của thông điệp như thế nào.

Địa chỉ tên miền có dạng như sau:

thông_tin_người_dùng@thông_tin_tên_miền

Phần "thông_tin_tên_miền" gồm có một xâu các nhãn cách nhau bởi một dấu chấm (".").

- **Cấu trúc của một thông điệp**

Một thông điệp điện tử gồm có những thành phần chính sau đây:

- Phong bì (Envelope): chứa các thông tin về địa chỉ người gửi thông điệp, địa chỉ người nhận thông điệp. MTA sẽ sử dụng những thông tin trên phong bì để định tuyến thông điệp.
- Đầu thông điệp (Header): chứa địa chỉ thư của người nhận. MUA sử dụng địa chỉ này để phân thông điệp về đúng hộp thư của người nhận.
- Thân thông điệp (Body): chứa nội dung của thông điệp.

Phần đầu thông điệp bao gồm những dòng chính sau:

- To: Địa chỉ của người nhận thông điệp.
- From: Địa chỉ của người gửi thông điệp.
- Subject: Mô tả ngắn gọn về nội dung của thông điệp.
- Date: Ngày và thời gian mà thông điệp bắt đầu được gửi.
- Received: Được thêm vào bởi mỗi MTA có mặt trên đường mà thông điệp đi qua để tới được đích (thông tin định tuyến).
- Cc: Các địa chỉ của người nhận thông điệp ngoài người nhận chính ở trường "To:".

1.4 Tóm tắt chương 1

Trong chương này giới thiệu các kiến thức và khái niệm cơ bản về hệ thống mạng như:

- Các kiến thức và khái niệm cơ bản về LAN/WAN,
- Các kiến thức và khái niệm cơ bản về mạng toàn cầu Internet,
- Các kiến thức tổng quan về mô hình OSI,
- Các kiến thức tổng quan về bộ giao thức TCP/IP, và đặc biệt giới thiệu sâu về giao thức liên mạng IP (IPv4), tạo cơ sở nền tảng cho các học viên trước khi đi vào phần thiết kế LAN/WAN trong các phần sau.

- Chương này cũng giới thiệu về giao thức liên mạng thế hệ mới IPv6, giúp cho học viên nắm bắt được các xu hướng mới trong việc phát triển các bộ giao thức mạng.
- Trong chương này cũng giới thiệu một số các dịch vụ cơ bản trên mạng đã và đang được ứng dụng rộng rãi.
- Trên cơ sở kiến thức của chương 1, phần tiếp theo của giáo trình sẽ đi sâu trình bày các kiến thức và các vấn đề liên quan khi thiết kế mạng LAN, mạng WAN.

2 Chương II - Mạng LAN và thiết kế mạng LAN

2.1 Kiến thức cơ bản về LAN

Mạng cục bộ (LAN) là hệ truyền thông tốc độ cao được thiết kế để kết nối các máy tính và các thiết bị xử lý dữ liệu khác cùng hoạt động với nhau trong một khu vực địa lý nhỏ như ở một tầng của toà nhà, hoặc trong một toà nhà.... Một số mạng LAN có thể kết nối lại với nhau trong một khu làm việc.

Các mạng LAN trở nên thông dụng vì nó cho phép những người sử dụng dùng chung những tài nguyên quan trọng như máy in mầu, ổ đĩa CD-ROM, các phần mềm ứng dụng và những thông tin cần thiết khác. Trước khi phát triển công nghệ LAN các máy tính là độc lập với nhau, bị hạn chế bởi số lượng các chương trình tiện ích, sau khi kết nối mạng rõ ràng hiệu quả của chúng tăng lên gấp bội.

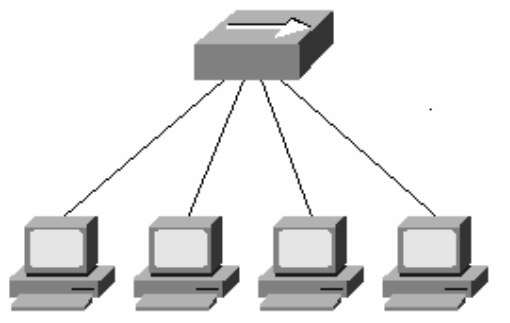
2.1.1 Cấu trúc tôpô của mạng

Cấu trúc tôpô (network topology) của LAN là kiến trúc hình học thể hiện cách bố trí các đường cáp, sắp xếp các máy tính để kết nối thành mạng hoàn chỉnh. Hầu hết các mạng LAN ngày nay đều được thiết kế để hoạt động dựa trên một cấu trúc mạng định trước. Điển hình và sử dụng nhiều nhất là các cấu trúc: dạng hình sao, dạng hình tuyến, dạng vòng cùng với những cấu trúc kết hợp của chúng.

2.1.1.1 Mạng dạng hình sao (Star topology).

Mạng dạng hình sao bao gồm một bộ kết nối trung tâm và các nút . Các nút này là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Bộ kết nối trung tâm của mạng điều phối mọi hoạt động trong mạng.

Mạng dạng hình sao cho phép nối các máy tính vào một bộ tập trung (Hub) bằng cáp, giải pháp này cho phép nối trực tiếp máy tính với Hub không cần thông qua trục bus, tránh được các yếu tố gây ngưng trệ mạng.



Hình 2-1: Cấu trúc mạng hình sao

Mô hình kết nối hình sao ngày nay đã trở lên hết sức phổ biến. Với việc sử dụng các bộ tập trung hoặc chuyển mạch, cấu trúc hình sao có thể được mở rộng bằng cách tổ chức nhiều mức phân cấp, do vậy dễ dàng trong việc quản lý và vận hành.

Các ưu điểm của mạng hình sao:

- Hoạt động theo nguyên lý nối song song nên nếu có một thiết bị nào đó ở một nút thông tin bị hỏng thì mạng vẫn hoạt động bình thường.
- Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.
- Mạng có thể dễ dàng mở rộng hoặc thu hẹp.

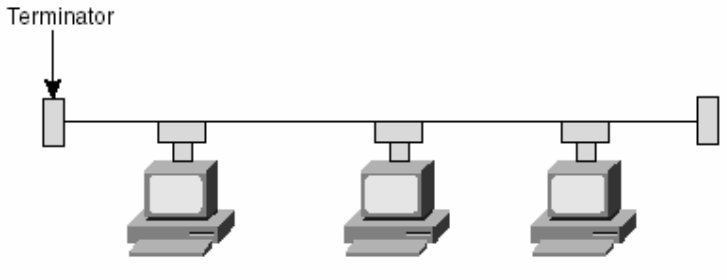
Những nhược điểm mạng dạng hình sao:

- Khả năng mở rộng mạng hoàn toàn phụ thuộc vào khả năng của trung tâm.
- Khi trung tâm có sự cố thì toàn mạng ngừng hoạt động.
- Mạng yêu cầu nối độc lập riêng rẽ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm rất hạn chế (100 m).

2.1.1.2 Mạng hình tuyến (Bus Topology).

Thực hiện theo cách bố trí hành lang, các máy tính và các thiết bị khác - các nút, đều được nối về với nhau trên một trục đường dây cáp chính để chuyển tải tín hiệu. Tất cả các nút đều sử dụng chung đường dây cáp chính này.

Phía hai đầu dây cáp được bịt bởi một thiết bị gọi là terminator. Các tín hiệu và dữ liệu khi truyền đi dây cáp đều mang theo địa chỉ của nơi đến.



Hình 2-2: Cấu trúc mạng hình tuyến

Ưu điểm: Loại hình mạng này dùng dây cáp ít nhất, dễ lắp đặt, giá thành rẻ.

Nhược điểm:

- Sự ùn tắc giao thông khi di chuyển dữ liệu với lưu lượng lớn.
- Khi có sự hỏng hóc ở đoạn nào đó thì rất khó phát hiện, một sự ngừng trên đường dây để sửa chữa sẽ ngừng toàn bộ hệ thống.

Cấu trúc này ngày nay ít được sử dụng.

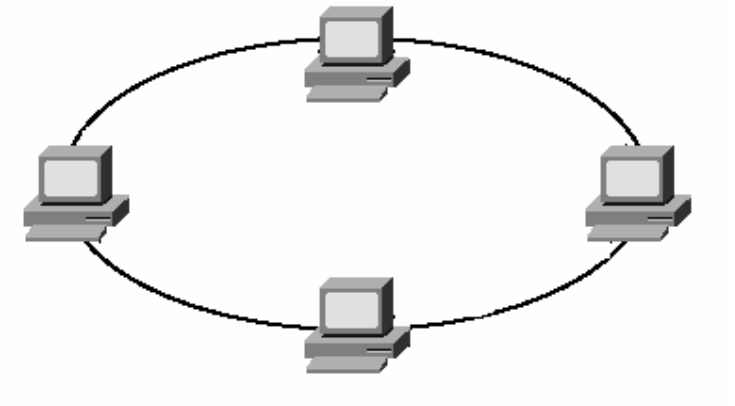
2.1.1.3 Mạng dạng vòng (Ring Topology).

Mạng dạng này, bố trí theo dạng xoay vòng, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút truyền tín hiệu cho nhau mỗi thời điểm chỉ được một nút mà thôi. Dữ liệu truyền đi phải có kèm theo địa chỉ cụ thể của mỗi trạm tiếp nhận.

Ưu điểm:

- Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên
- Mỗi trạm có thể đạt được tốc độ tối đa khi truy nhập.

Nhược điểm: Đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.



Hình 2-3: Cấu trúc mạng dạng vòng

2.1.1.4 Mạng dạng kết hợp.

Kết hợp hình sao và tuyến (*star/Bus Topology*): Cấu hình mạng dạng này có bộ phận tách tín hiệu (*spitter*) giữ vai trò thiết bị trung tâm, hệ thống dây cáp mạng có thể chọn hoặc *Ring Topology* hoặc *Linear Bus Topology*. Lợi điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở cách xa nhau, ARCNET là mạng dạng kết hợp *Star/Bus Topology*. Cấu hình dạng này đưa lại sự uyển chuyển trong việc bố trí đường dây tương thích dễ dàng đối với bất cứ toà nhà nào.

Kết hợp hình sao và vòng *(Star/Ring Topology)*. Cấu hình dạng kết hợp *Star/Ring Topology*, có một "thẻ bài" liên lạc (*Token*) được chuyển vòng quanh một cái HUB trung tâm. Mỗi trạm làm việc (*workstation*) được nối với HUB - là cầu nối giữa các trạm làm việc và để tăng khoảng cách cần thiết.

2.1.2 Các phương thức truy nhập đường truyền

Khi được cài đặt vào trong 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:

2.1.2.1 Giao thức CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Giao thức này 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 rỗi (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 và thông báo tới các trạm khác gây ra xung đột (Collision Detection), 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 xẩy ra với số lượng lớn dẫn đến làm chậm tốc độ truyền tin của hệ thống.

Giao thức này còn được trình bày chi tiết thêm trong phần công Ethernet.

2.1.2.2 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 rỗi). 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 xoay 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 rỗi. 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 xẩy 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 dừng 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.

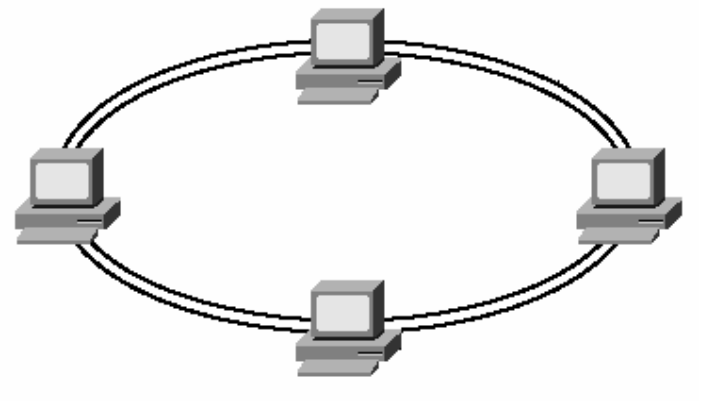
Việc truyền thẻ bài sẽ không thực hiện được nếu việc xoay vòng bị đứt đoạn. Giao thức phải chứa các thủ tục kiểm tra thẻ bài để cho phép khôi phục lại thẻ bài bị mất hoặc thay thế trạng thái của thẻ bài và cung cấp các phương tiện để sửa đổi logic (thêm vào, bớt đi hoặc định lại trật tự của các trạm).

2.1.2.3 Giao thức FDDI.

FDDI 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 trục 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.



Hình 2-4: Cấu trúc mạng dạng vòng của FDDI

2.1.3 Các loại đường truyền và các chuẩn của chúng

- **Chuẩn Viện công nghệ điện và điện tử (IEEE)**

Tiêu chuẩn IEEE LAN được phát triển dựa vào uỷ ban IEEE 802.

- Tiêu chuẩn IEEE 802.3 liên quan tới mạng CSMA/CD bao gồm cả 2 phiên bản băng tần cơ bản và băng tần mở rộng.
- Tiêu chuẩn IEEE 802.4 liên quan tới sự phương thức truyền thẻ bài trên mạng hình tuyến (Token Bus)
- IEEE 802.5 liên quan đến truyền thẻ bài trên mạng dạng vòng (Token Ring).

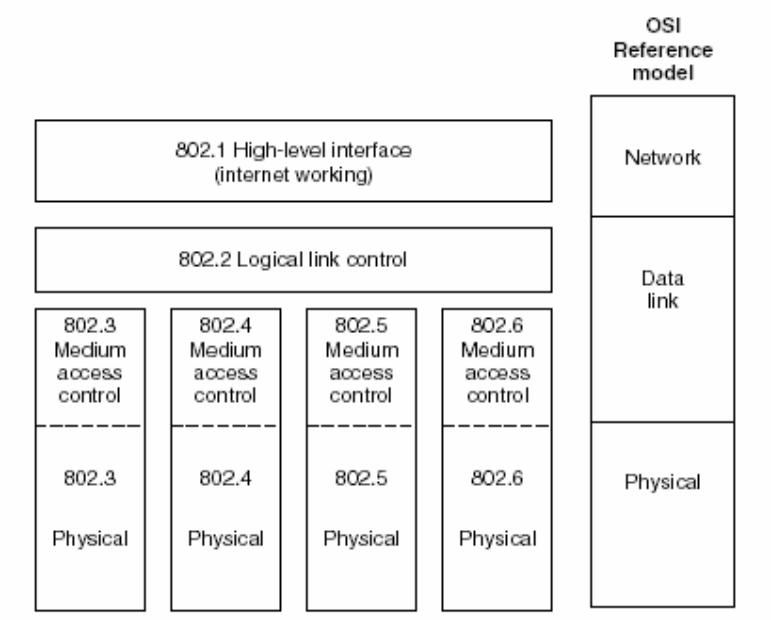
Theo chuẩn 802 thì tầng liên kết dữ liệu chia thành 2 mức con: mức con điều khiển logic LLC (Logical Link Control Sublayer) và mức con điều khiển xâm nhập mạng MAC (Media Access Control Sublayer). Mức con LLC giữ vai trò tổ chức dữ liệu, tổ chức thông tin để truyền và nhận. Mức con MAC chỉ làm nhiệm vụ điều khiển việc xâm nhập mạng. Thủ tục mức con LLC không bị ảnh hưởng khi sử dụng các đường truyền dẫn khác nhau, nhờ vậy mà linh hoạt hơn trong khai thác.

Chuẩn 802.2 ở mức con LLC tương đương với chuẩn HDLC của ISO hoặc X.25 của CCITT.

Chuẩn 802.3 xác định phương pháp thâm nhập mạng tức thời có khả năng phát hiện lỗi chồng chéo thông tin CSMA/CD. Phương pháp CSMA/CD được đưa ra từ năm 1993 nhằm mục đích nâng cao hiệu quả mạng. Theo chuẩn này các mức được ghép nối với nhau thông qua các bộ ghép nối.

Chuẩn 802.4 thực chất là phương pháp thâm nhập mạng theo kiểu phát tín hiệu thăm dò token qua các trạm và đường truyền bus.

Chuẩn 802.5 dùng cho mạng dạng xoay vòng và trên cơ sở dùng tín hiệu thăm dò token. Mỗi trạm khi nhận được tín hiệu thăm dò token thì tiếp nhận token và bắt đầu quá trình truyền thông tin dưới dạng các khung tín hiệu. Các khung có cấu trúc tương tự như của chuẩn 802.4. Phương pháp xâm nhập mạng này quy định nhiều mức ưu tiên khác nhau cho toàn mạng và cho mỗi trạm, việc quy định này vừa cho người thiết kế vừa do người sử dụng tự quy định.



Hình 2-5: Mối quan hệ giữa các chuẩn IEEE và mô hình OSI

- **Chuẩn uỷ ban tư vấn quốc tế về điện báo và điện thoại(CCITT)**

Đây là những khuyến nghị về tiêu chuẩn hóa hoạt động và mẫu mã modem (truyền qua mạng điện thoại)

Một số chuẩn: V22, V28, V35...

X series bao gồm các tiêu chuẩn OSI.

Chuẩn cáp và chuẩn giao tiếp EIA.

Các tiêu chuẩn EIA dành cho giao diện nối tiếp giữa modem và máy tính.

- RS-232
- RS-449
- RS-422

2.1.4 Hệ thống cáp mạng dùng cho LAN.

2.1.4.1 Cáp xoắn

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

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

Cáp có bọc kim loại (STP): Lớp bọc bên ngoài có tác dụng chống nhiễu điện từ, có loại có một đôi giây xoắn vào nhau và có loại có nhiều đôi giây xoắn với nhau.

Cáp không bọc kim loại (UTP): Tính tương tự như STP nhưng kém hơn về khả năng chống nhiễu và suy hao vì không có vỏ bọc.

STP và UTP có các loại (Category - Cat) thường dùng:

- Loại 1 & 2 (Cat 1 & Cat 2): Thường dùng cho truyền thoại và những đường truyền tốc độ thấp (nhỏ hơn 4Mb/s).
- Loại 3 (Cat 3): tốc độ truyền dữ liệu khoảng 16 Mb/s , nó là chuẩn cho hầu hết các mạng điện thoại.
- Loại 4 (Cat 4): Thích hợp cho đường truyền 20Mb/s.
- Loại 5 (Cat 5): Thích hợp cho đường truyền 100Mb/s.
- Loại 6 (Cat 6): Thích hợp cho đường truyền 300Mb/s.

Đây là loại cáp rẻ, dễ cài đặt tuy nhiên nó dễ bị ảnh hưởng của môi trường.

2.1.4.2 Cáp đồng trục

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

Cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác (ví dụ như cáp xoắn đôi) do ít bị ảnh hưởng của môi trường. Các mạng cục bộ sử dụng cáp đồng trục có thể có kích thước trong phạm vi vài ngàn mét, cáp đồng trục được sử dụng nhiều trong các mạng dạng đường thẳng. Hai loại cáp thường được sử dụng là cáp đồng trục mỏng và cáp đồng trục dày trong đường kính cáp đồng trục mỏng là 0,25 inch, cáp đồng trục dày là 0,5 inch. Cả hai loại cáp đều làm việc ở cùng tốc độ nhưng cáp đồng trục mỏng có độ hao suy tín hiệu lớn hơn

Hiện nay có cáp đồng trục sau:

- RG -58,50 ohm: dùng cho mạng Thin Ethernet

– RG -59,75 ohm: dùng cho truyền hình cáp

Các mạng cục bộ thường sử dụng cáp đồng trục có dải thông từ 2,5 - 10 Mb/s, cáp đồng trục có độ suy hao ít hơn so với các loại cáp đồng khác vì nó có lớp vỏ bọc bên ngoài, độ dài thông thường của một đoạn cáp nối trong mạng là 200m, thường sử dụng cho dạng Bus.

2.1.4.3 Cáp sợi quang (Fiber - Optic Cable)

Cáp sợi quang bao gồm một dây dẫn trung tâm (là một hoặc một bó sợi thủy tinh có thể truyền dẫn tín hiệu quang) được bọc một lớp vỏ bọc có tác dụng phản xạ các tín hiệu trở lại để giảm sự mất mát tín hiệu. Bên ngoài cùng là lớp vỏ plastic để bảo vệ cáp. Như vậy cáp sợi quang không truyền dẫn các tín hiệu điện mà chỉ truyền các tín hiệu quang (các tín hiệu dữ liệu phải được chuyển đổi thành các tín hiệu quang và khi nhận chúng sẽ lại được chuyển đổi trở lại thành tín hiệu điện).

Cáp quang có đường kính từ 8.3 - 100 micron, Do đường kính lõi sợi thuỷ tinh có kích thước rất nhỏ nên rất khó khăn cho việc đấu nối, nó cần công nghệ đặc biệt với kỹ thuật cao đòi hỏi chi phí cao.

Dải thông của cáp quang có thể lên tới hàng Gbps và cho phép khoảng cách đi cáp khá xa do độ suy hao tín hiệu trên cáp rất thấp. Ngoài ra, vì cáp sợi quang không dùng tín hiệu điện từ để truyền dữ liệu nên nó hoàn toàn không bị ảnh hưởng của nhiễu điện từ và tín hiệu truyền không thể bị phát hiện và thu trộm bởi các thiết bị điện tử của người khác.

Chỉ trừ nhược điểm khó lắp đặt và giá thành còn cao , nhìn chung cáp quang thích hợp cho mọi mạng hiện nay và sau này.

Các loại cáp	Cáp xoắn cặp	Cáp đồng trục mỏng	Cáp đồng trục dày	Cáp quang
Chi tiết	Bằng đồng, có 4 cặp dây (loại 3, 4, 5)	Bằng đồng, 2 dây, đường kính 5mm	Bằng đồng, 2 dây, đường kính 10mm	Thủy tinh, 2 sợi
Chiều dài đoạn tối đa	100m	185m	500m	1000m
Số đầu nối tối đa trên 1 đoạn	2	30	100	2
Chạy 10 Mbit/s	Được	Được	Được	Được

Chạy 100 Mbit/s	Được	Không	Không	Được
Chống nhiễu	Tốt	Tốt	Rất tốt	Hoàn toàn
Bảo mật	Trung bình	Trung bình	Trung bình	Hoàn toàn
Độ tin cậy	Tốt	Trung bình	Tốt	Tốt
Lắp đặt	Dễ dàng	Trung bình	Khó	Khó
Khắc phục lỗi	Tốt	Dở	Dở	Tốt
Quản lý	Dễ dàng	Khó	Khó	Trung bình
Chi phí cho 1 trạm	Rất thấp	Thấp	Trung bình	Cao

2.1.4.4 Hệ thống cáp có cấu trúc theo chuẩn TIA/EIA 568

Vào giữa những năm 1980, TIA và EIA bắt đầu phát triển phương pháp đi cáp cho các toà nhà, với ý định phát triển một hệ đi dây giống nhau, hỗ trợ các sản phẩm và môi trường của các nhà cung cấp thiết bị khác nhau. Năm 1991, TIA và EIA đưa ra chuẩn 568 Commercial Building Telecommunication Cabling Standard. Từ đó chuẩn này tiếp tục phát triển phù hợp với các công nghệ truyền dẫn mới, hiện nay nó mang tên TIA/EIA 568 B.

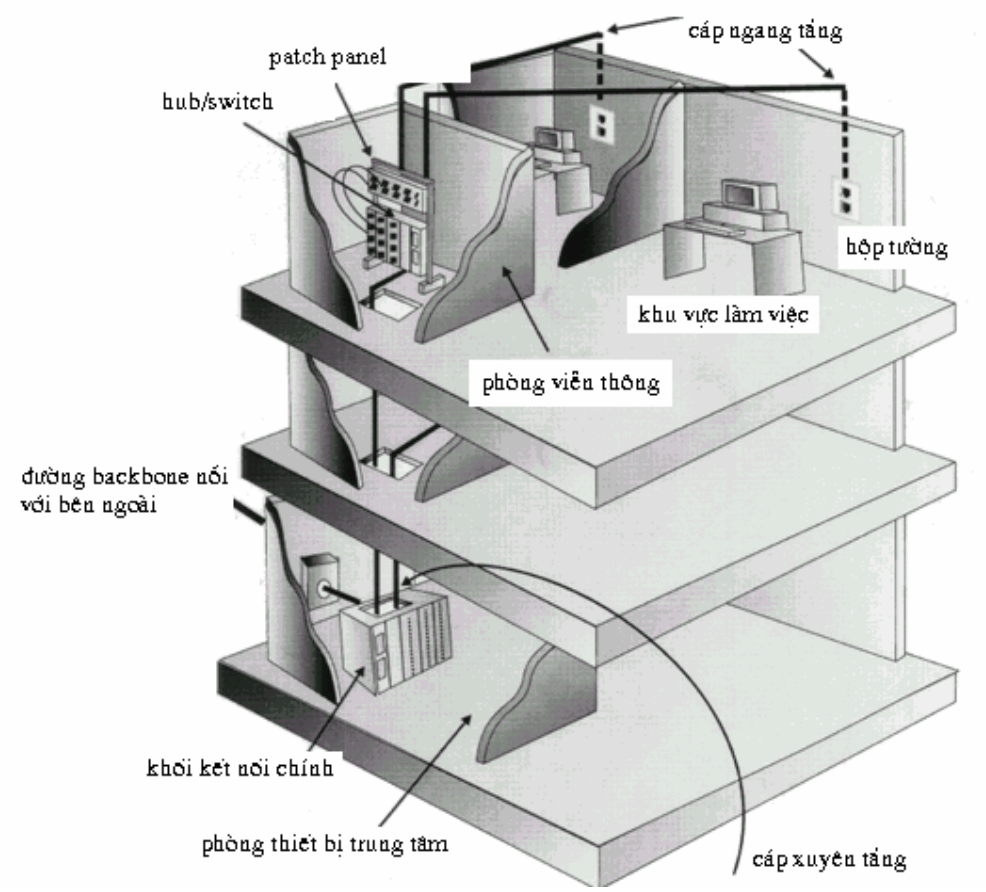
TIA/EIA xác định một loạt các chuẩn liên quan đến đi cáp mạng:

- TIA/EIA-568-A Xác định chuẩn cho hệ đi cáp cho các toà nhà thương mại hỗ trợ mạng dữ liệu, thoại và video.
- TIA/EIA-569 Xác định cách xây dựng đường dẫn và không gian cho các môi trường viễn thông.
- TIA/EIA-606 Xác định hướng dẫn về thiết kế cho việc điều cơ sở hạ tầng viễn thông.
- TIA/EIA-607 Xác định các yêu cầu về nền và xây ghép cho cáp và thiết bị viễn thông.

Chuẩn cáp có cấu trúc của TIA/EIA là các đặc tả quốc tế để xác định cách thiết kế, xây dựng và quản lý hệ cáp có cấu trúc. Chuẩn nầy xác định mạng cấu trúc hình sao. Theo tài liệu TIA/EIA-568B, chuẩn nối dây được thiết kế để cung cấp các đặc tính và chức năng sau:

- Hệ nối dây viễn thông cùng loại cho các toà nhà thương mại
- Xác định môi trường truyền thông, cấu trúc tôpô, các điểm kết nối, điểm đầu cuối, và sự quản lý.
- Hỗ trợ các sản phẩm, các phương tiện của các nhà cung cấp khác nhau.
- Định hướng việc thiết kế tương lai cho các sản phẩm viễn thông cho các doanh nghiệp thương mại.
- Khả năng lập kế hoạch và cài đặt kết nối viễn thông cho toà nhà thương mại mà không cần có trước kiến thức về sản phẩm sử dụng để đi dây.
- Điểm cuối cùng có lợi cho người dùng vì nó chuẩn hóa việc đi dây và cài đặt, mở ra thị trường cho các sản phẩm và dịch vụ cạnh tranh trong các lĩnh vực về đi cáp, thiết kế, cài đặt, và quản trị.

Hình sau minh hoạ cấu trúc hệ thống cáp trong một toà nhà cụ thể:



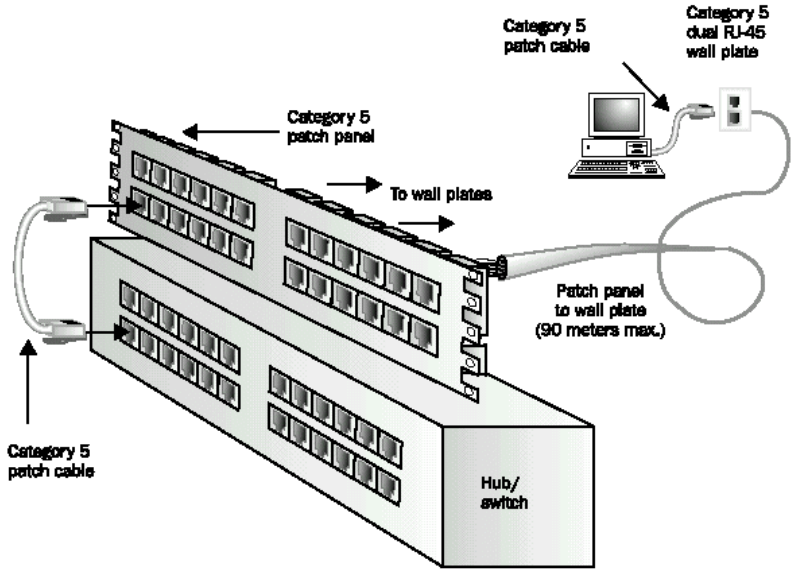
Hình 2-6: Sơ đồ các thành phần hệ thống cáp trong toà nhà

Các thành phần của hệ thống cáp gồm có:

- Hệ cáp khu vực làm việc (work area wiring) - Gồm các hộp tường, cáp, và các đầu kết nối (connector) cần thiết để nối các thiết bị trong vùng làm việc (máy tính, máy in,...) qua hệ cáp ngang tầng đến phòng viễn thông.
- Hệ cáp ngang tầng (horizontal wiring) - Chạy từ mỗi máy trạm đến phòng viễn thông. Khoảng cách dài nhất theo chiều ngang từ phòng viễn thông đến hộp tường là 90 mét, không phụ thuộc vào loại môi trường. Được phép dùng thêm 10 m cho các bó cáp ở phòng viễn thông và tại máy trạm.
- Hệ cáp xuyên tầng (vertical wiring) - Kết nối các phòng viễn với phòng thiết bị trung tâm của toà nhà.
- Hệ cáp backbone - Kết nối toà nhà với các toà nhà khác.

Ta có thể thay các phòng viễn thông và các phòng thiết bị trung tâm bởi các tủ đựng thiết bị nhưng vẫn cần tuân thủ kiến trúc phân cấp dựa trên tôpô hình sao của chuẩn này.

Hình sau đây minh hoạ rõ hơn kết nối máy tính với hub/switch thông qua hệ thống cáp ngang.



Hình 2-7: Kết nối từ máy tính tới hub/switch

2.1.4.5 Các yêu cầu cho một hệ thống cáp

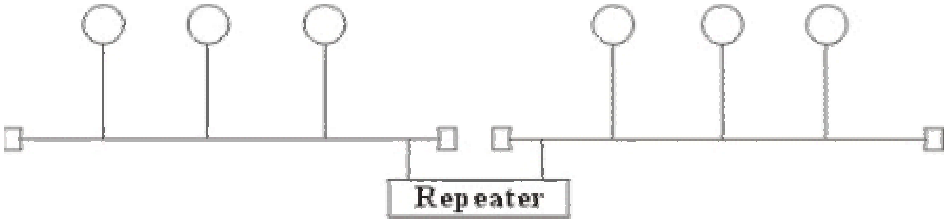
- An toàn, thẩm mỹ: tất cả các dây mạng phải được bao bọc cẩn thận, cách xa các nguồn điện, các máy có khả năng phát sóng để tránh trường hợp bị nhiễu. Các đầu nối phải đảm bảo chất lượng, tránh tình trạng hệ thống mạng bị chập chờn.

– Đúng chuẩn: hệ thống cáp phải thực hiện đúng chuẩn, đảm bảo cho khả năng nâng cấp sau này cũng như dễ dàng cho việc kết nối các thiết bị khác nhau của các nhà sản xuất khác nhau. Tiêu chuẩn quốc tế dùng cho các hệ thống mạng hiện nay là EIA/TIA 568B.
– Tiết kiệm và "linh hoạt" (flexible): hệ thống cáp phải được thiết kế sao cho kinh tế nhất, dễ dàng trong việc di chuyển các trạm làm việc và có khả năng mở rộng sau này.

2.1.5 Các thiết bị dùng để kết nối LAN.

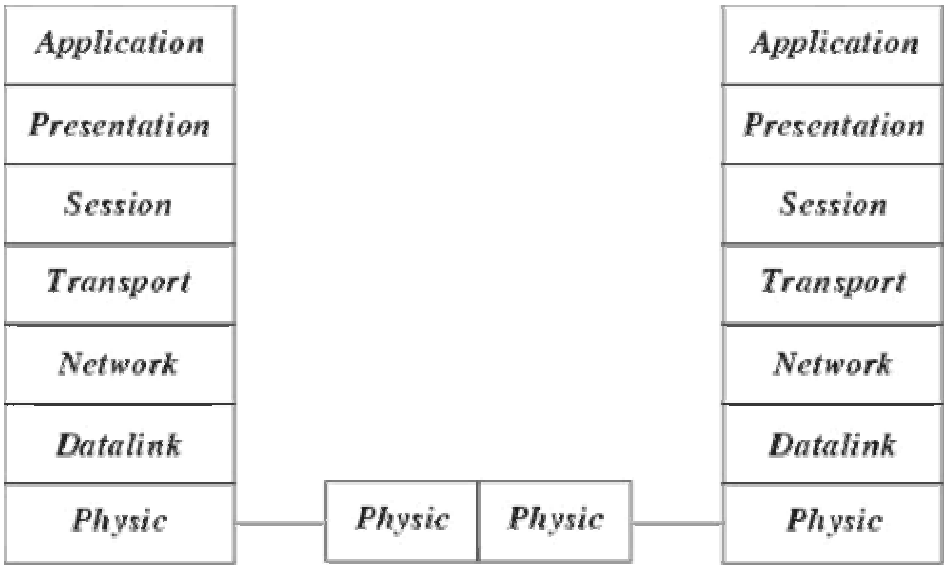
2.1.5.1 Bộ lặp tín hiệu (Repeater)

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 OSI. Khi Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.



Hình 2-8: Mô hình liên kết mạng sử dụng Repeater

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



Hình 2-9: 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 trục 50 thì khoảng cách tối đa là 2.8 km, khoảng cách đó không thể kéo thêm cho dù sử dụng thêm Repeater.
- Repeater điện quang liên kết với một đầu cáp quang và một đầu là cáp điện, nó chuyển một tín hiệu điện từ cáp điện ra tín hiệu quang để phát trên cáp quang và ngược lại. Việc sử dụng Repeater điện quang cũng làm tăng thêm chiều dài của mạng.

Việc sử dụng Repeater không thay đổi nội dung các tín hiện đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông (như hai mạng Ethernet hay hai mạng Token ring) và không thể nối hai mạng có giao thức truyền thông khác nhau. Thêm nữa Repeater không làm thay đổi khối lượng chuyển vận trên mạng nên việc sử dụng không tính toán nó trên mạng lớn sẽ hạn chế hiệu năng của mạng. Khi lưa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ chuyển vận phù hợp với tốc độ của mạng.

2.1.5.2 Bộ tập trung (Hub)

Hub là một trong những yếu tố quan trọng nhất của LAN, đây là điểm kết nối dây trung tâm của mạng, tất cả các trạm trên mạng LAN được kết nối thông qua Hub. Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng hình sao.

Một hub thông thường có nhiều cổng nối với người sử dụng để gắn máy tính và các thiết bị ngoại vi. Mỗi cổng hỗ trợ một bộ kết nối dùng cặp dây xoắn 10BASET từ mỗi trạm của mạng.

Khi tín hiệu được truyền từ một trạm tới hub, nó được lặp lại trên khắp các cổng khác của. Các hub thông minh có thể định dạng, kiểm tra, cho phép hoặc không cho phép bởi người điều hành mạng từ trung tâm quản lý hub.

Nếu phân loại theo phần cứng thì có 3 loại hub:

- Hub đơn (stand alone hub)

- Hub modun (Modular hub) rất phổ biến cho các hệ thống mạng vì nó có thể dễ dàng mở rộng và luôn có chức năng quản lý, modular có từ 4 đến 14 khe cắm, có thể lắp thêm các modun Ethernet 10BASET.
- Hub phân tầng (Stackable hub) là lý tưởng cho những cơ quan muốn đầu tư tối thiểu ban đầu nhưng lại có kế hoạch phát triển LAN sau này.

Nếu phân loại theo khả năng ta có 2 loại:

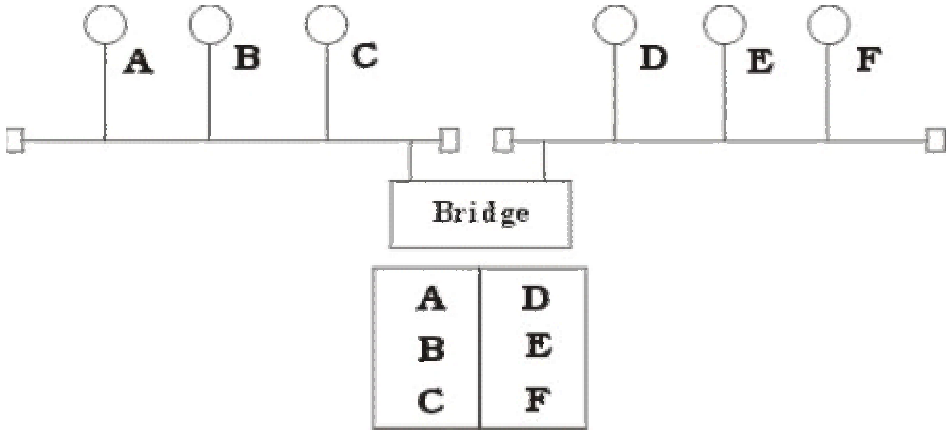
- Hub bị động (Passive Hub) : Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng.
- Hub chủ động (Active Hub) : Hub chủ động có các linh kiện điện tử có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Qúa trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động.

Về cơ bản, trong mạng Ethernet, hub hoạt động như một repeater có nhiều cổng.

2.1.5.3 Cầu (Bridge)

Bridge là một thiết bị có xử lý 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 nên không như bộ tiếp sức phải phát lại tất cả những gì nó nhận được thì cầu nối đọc được các gói tin 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 gói tin Bridge chọn lọc và chỉ chuyển những gói tin 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.

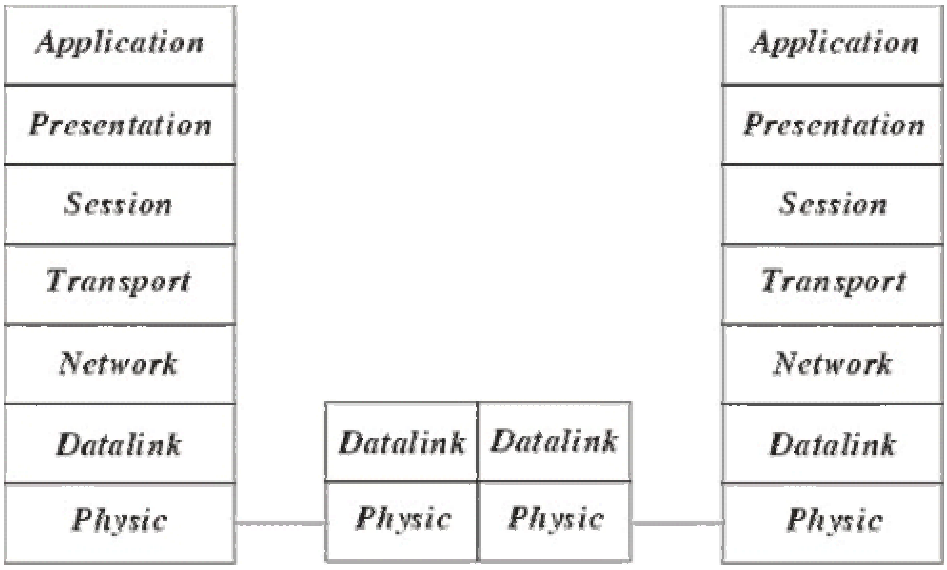


Hình 2-10: Hoạt động của cầu nối

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 gói tin nó nhận được bằng cách đọc địa chỉ của nơi gửi và nhận và dựa trên bảng địa chỉ phía nhận được gói tin nó quyết định gửi gói tin hay không và bổ xung bảng địa chỉ.

Khi đọc địa chỉ nơi gửi Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu không có thì Bridge tự động bổ xung bảng địa chỉ (cơ chế đó được gọi là tự học của cầu nối).

Khi đọc địa chỉ nơi nhận Bridge kiểm tra xem trong bảng địa chỉ của phần mạng nhận được gói tin có địa chỉ đó hay không, nếu có thì Bridge sẽ cho rằng đó là gói tin nội bộ thuộc phần mạng mà gói tin đến nên không chuyển gói tin đó đi, nếu ngược lại thì Bridge mới chuyển sang phía bên kia. Ở đây chúng ta thấy một trạm không cần thiết chuyển thông tin trên toàn mạng mà chỉ trên phần mạng có trạm nhận mà thôi.



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 gói tin 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 gói tin/giây trong đó thể hiện khả năng của Bridge chuyển các gói tin từ mạng này sang mạng khác.

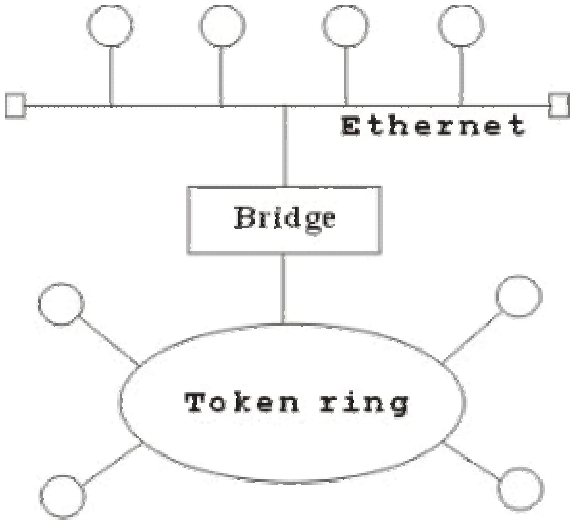
Hiện nay có hai loại Bridge đang được sử dụng là Bridge vận chuyển và Bridge biên dịch. Bridge vận chuyển dùng để nối hai mạng cục bộ cùng sử dụng một giao thức truyền thông của tầng liên kết dữ liệu, tuy nhiên mỗi mạng có thể sử dụng loại dây nối khác nhau. Bridge vận chuyển không có khả năng thay đổi cấu trúc các gói tin mà nó nhận được mà chỉ quan tâm tới việc xem xét và chuyển vận gói tin đó đi.

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

Ví dụ : Bridge biên dịch nối một mạng Ethernet và một mạng Token ring. Khi đó Cầu nối thực hiện như một nút token ring trên mạng Token ring và một nút Enthernet trên mạng Ethernet. Cầu nối có thể chuyền một gói tin theo chuẩn đang sử dụng trên mạng Enthernet sang chuẩn đang sử dụng trên mạng Token ring.

Tuy nhiên chú ý ở đây cầu nối không thể chia một gói tin ra làm nhiều gói tin cho nên phải hạn chế kích thước tối đa các gói tin phù hợp với cả hai mạng. Ví dụ như kích thước tối đa của gói tin trên mạng Ethernet là 1500 bytes và trên mạng Token

ring là 6000 bytes do vậy nếu một trạm trên mạng token ring gửi một gói tin cho trạm trên mạng Ethernet với kích thước lớn hơn 1500 bytes thì khi qua cầu nối số lượng byte dư sẽ bị chặt bỏ.



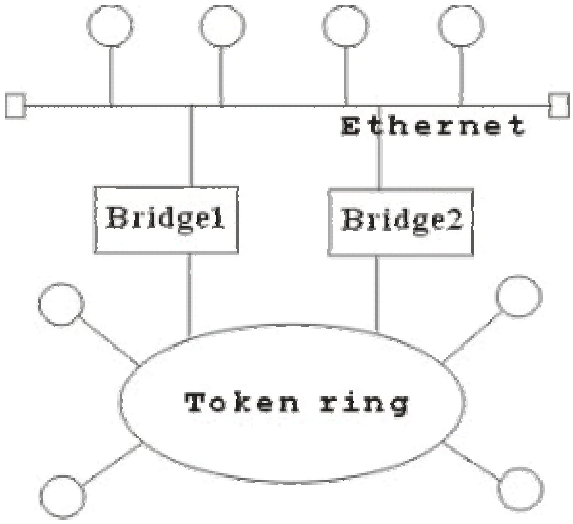
Hình 2-12: Bridge biên dịch

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 sử lý gói tin đã phát lại gói tin trên phần mạng còn lại nên tín hiệu tốt hơn bộ 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 gói tin trong nội bộ tùng 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 gói tin của nhửng địa chỉ xác định. Ví dụ : cho phép gói tin của máy A, B qua Bridge 1, gói tin của máy C, D qua Bridge 2.



Hình 2-13: Liên kết mạng sử dụng 2 Bridge

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 cắïm 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.

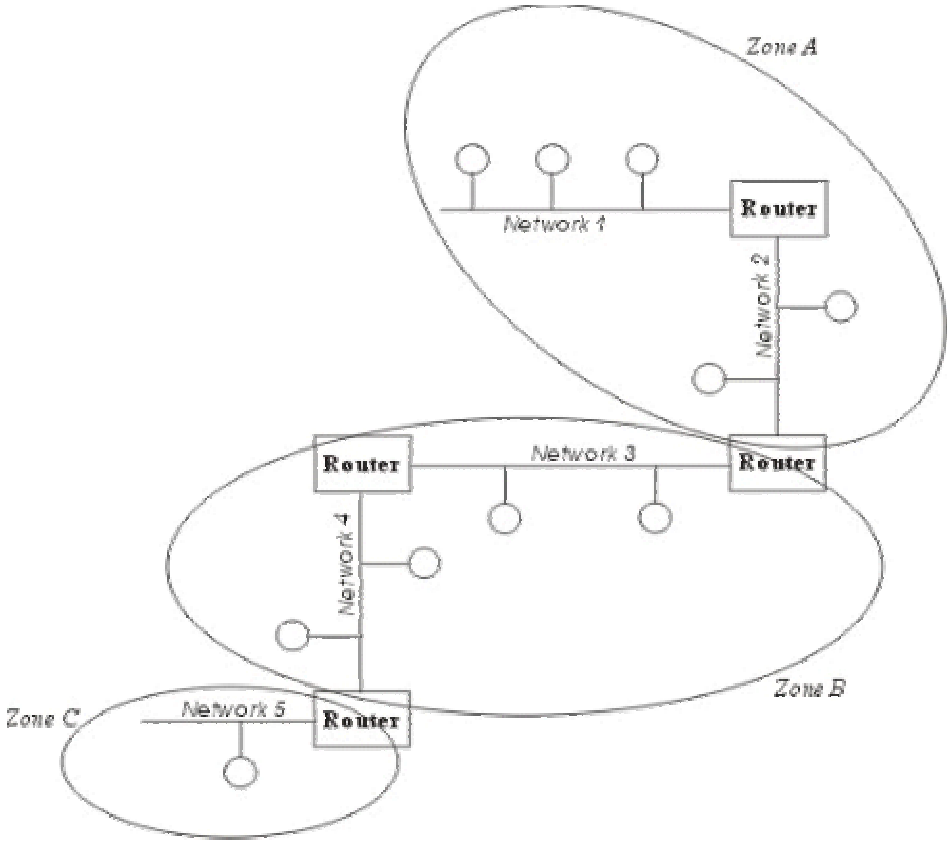
2.1.5.4 Bộ chuyển mạch (Switch)

Bộ chuyển mạch là sự tiến hoá của cầu, nhưng có nhiều cổng và dùng các mạch tích hợp nhanh để giảm độ trễ của việc chuyển khung dữ liệu.

Switch giữa bảng địa chỉ MAC của mỗi cổng và thực hiện giao thức Spanning-Tree. Switch cũng hoạt động ở tầng data link và trong suốt với các giao thức ở tầng trên.

2.1.5.5 Bộ định tuyến(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.



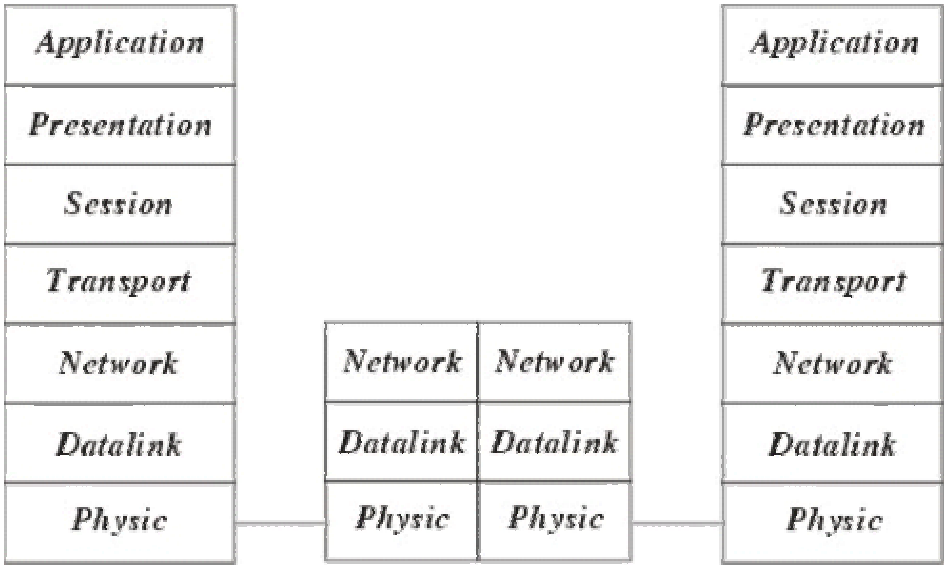
Hình 2-14: Hoạt động của Router

Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong gói tin đó phải chứa các thông tin khác về đích đến) và khi gói tin đến Router thì Router mới xử lý và gửi tiếp.

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

Người ta phân chia Router thành hai loại là Router có phụ thuộc giao thức (The protocol 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 truyền trên mạng).

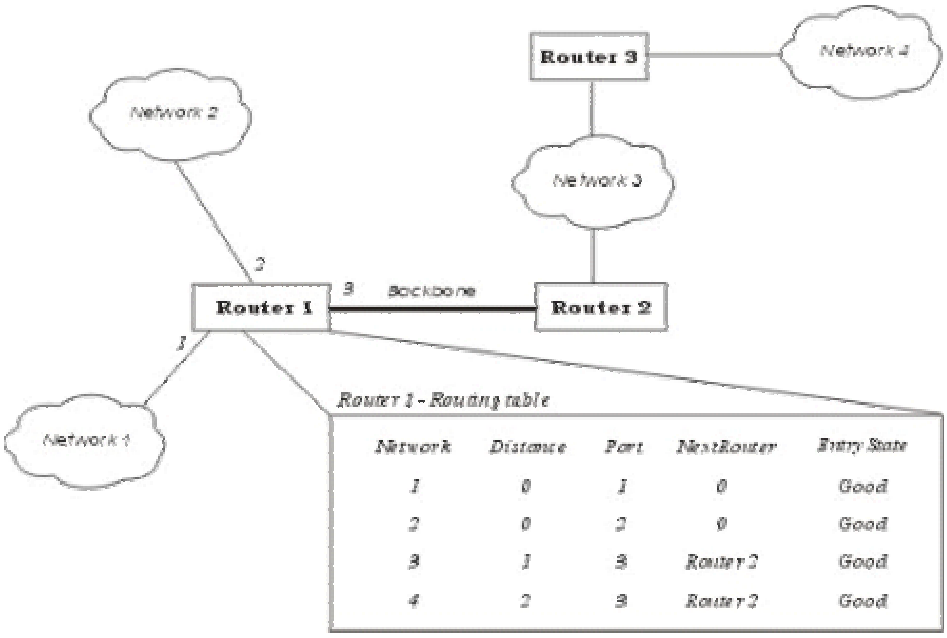


Hình 2-15: Hoạt động của Router trong mô hình OSI

Để ngăn chặn việc mất mát số liệu Router còn nhận biết được đường nào có thể chuyển vận và ngừng chuyển vận khi đường bị tắc.
Các lý do sử dụng Router :

- Router có các phần mềm lọc ưu việt hơn là Bridge do các gói tin muốn đi qua Router cần phải gửi trực tiếp đến nó nên giảm được số lượng gói tin qua nó. Router thường được sử dụng trong khi nối các mạng thông qua các đường dây thuê bao đắt tiền do nó không truyền dư lên đường truyền.
- Router có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.
- Router có thể xác định được đường đi an toàn và tốt nhất trong mạng nên độ an toàn của thông tin được đảm bảo hơn.

Trong một mạng phức hợp khi các gói tin luân chuyển các đường có thể gây nên tình trạng tắc nghẽn của mạng thì các Router có thể được cài đặt các phương thức nhằm tránh được tắc nghẽn.



Hình 2-16: Ví dụ về bảng định tuyến của Router

Các phương thức hoạt động của Router: Đó là phương thức mà một Router có thể nối với các Router khác để qua đó chia sẻ thông tin về mạng hiện co. 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 : mỗi Router luôn luôn truyền đi thông tin về bảng chỉ đường của mình trên mạng, thông qua đó các Router khác sẽ cập nhật lên bảng chỉ đường của mình.
- Phương thức trạng thái tĩnh : Router chỉ truyền các thông báo khi có phát hiện có sự thay đổi trong mạng vàchỉ khi đó các Routerkhác ù cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

Một số giao thức hoạt động chính của Router

- RIP(Routing Information Protocol) được phát triển bởi Xerox Network system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.

- NLSP (Netware Link Service Protocol) được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương thức véctơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng chỉ đường giảm đi..
- OSPF (Open Shortest Path First) là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...
- IS-IS (Open System Interconnection Intermediate System to Intermediate System) là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...

2.1.5.6 Bộ chuyển mạch có định tuyến (Layer 3 switch)

Switch L3 có thể chạy giao thức định tuyến ở tầng mạng, tầng 3 của mô hình 7 tầng OSI. Switch L3 có thể có các cổng WAN để nối các LAN ở khoảng cách xa. Thực chất nó được bổ sung thêm tính năng của router.

2.1.6 Các hệ điều hành mạng

- **Hệ điều hành mạng UNIX:**

Đây là hệ điều hành do các nhà khoa học xây dựng và được dùng rất phổ biến trong giới khoa học, giáo dục. Hệ điều hành mạng UNIX là hệ điều hành đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt.

Nhược điểm của nó là hiện nay có nhiều *Version* khác nhau, không thống nhất gây khó khăn cho người sử dụng. Ngoài ra hệ điều hành này khá phức tạp lại đòi hỏi cấu hình máy mạnh (trước đây chạy trên máy *mini*, gần đây có SCO UNIX chạy trên máy vi tính với cấu hình mạnh).

- **Hệ điều hành mạng Windows NT:**

Đây là hệ điều hành của hãng *Microsoft*, cũng là hệ điều hành đa nhiệm, đa người sử dụng. Đặc điểm của nó là tương đối dễ sử dụng, hỗ trợ mạnh cho phần mềm WINDOWS.

Do hãng *Microsoft* là hãng phần mềm lớn nhất thế giới hiện nay, hệ điều hành này có khả năng sẽ được ngày càng phổ biến rộng rãi. Ngoài ra, *Windows* NT có thể liên kết tốt với máy chủ *Novell Netware*. Tuy nhiên, để chạy có hiệu quả, *Windows* NT cũng đòi hỏi cấu hình máy tương đối mạnh.

- **Hệ điều hành mạng NetWare của Novell:**

Đây là hệ điều hành phổ biến nhất hiện nay ở nước ta và trên thế giới trong thời gian cuối, nó có thể dùng cho các mạng nhỏ (khoảng từ 5-25 máy tính) và cũng có thể dùng cho các mạng lớn gồm hàng trăm máy tính.

Trong những năm qua, *Novell* đã cho ra nhiều phiên bản của *Netware*: Netware 2.2, 3.11. 4.0 và hiện có 4.1. *Netware* là một hệ điều hành mạng cục bộ dùng cho các máy vi tính theo chuẩn của IBM hay các máy tính *Apple Macintosh*, chạy hệ điều hành MS-DOS hoặc OS/2.

- **Hệ điều hành mạng Linux:**

Linux là hệ điều hành phát triển từ Unix - 32 bit xử lý đa nhiệm, đa người dùng.

Hệ điều hành này là miễn phí và quan trọng là mã nguồn mở. Linux là một sản phẩm do người sử dụng tự phát triển, có nghĩa là nhiều thành phần của nó được người sử dụng trên khắp thế giới phát triển lấy để tự chạy hệ điều hành cho mục đích riêng của mình.

Hệ thống gốc được phát triển bởi Linux Torvalds. Ngày nay nó đã được phát triển khá tốt và được đánh giá cao, hoạt động hiệu quả với các ứng dụng mạng.

Các hệ điều hành khác nhau thuộc họ Linux được xây dựng với giao diện đồ hoạ gần gũi với người sử dụng. Một số hệ điều hành phổ biến như : RedHat Linux, SuSe, ManDrake, VietKey Linux...

Với việc cung cấp mã nguồn mở miễn phí, Linux đưa ra một giải pháp rẻ tiền cho các doanh nghiệp, công ty và các chính phủ. Hiện nay cộng đồng mã nguồn mở đang rất phát triển, thúc đẩy Linux thâm nhập sâu thêm vào đời sống.

2.2 Công nghệ Ethernet

2.2.1 Giới thiệu chung về Ethernet

Ngày nay, Ethernet đã trở thành công nghệ mạng cục bộ được sử dụng rộng rãi. Sau 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 và tiện dụng.

Ngày 22 tháng 5 năm 1973, Robert Metcalfe thuộc Trung tâm Nghiên cứu Palto 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 lazer. 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 10Mbps 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).

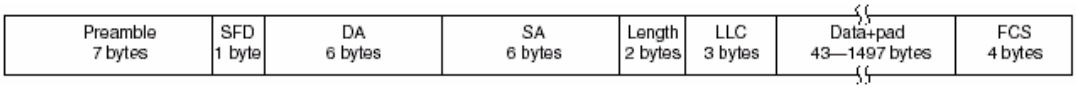
Uỷ ban 802.3 của IEEE đã lấy DIX Ethernet làm nền tảng để phát triển. Năm 1985, chuẩn 802.3 đầu tiên đã ra đời với tên **IEEE 802.3 Carrier Sense Multiple Access with Collition Detection (CSMA/CD) Access Method vesus Physical Layer Specification.** Mặc dù không sử dụng tên Ethernet nhưng hầu hết mọi 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.

2.2.2 Các đặc tính chung của Ethernet

2.2.2.1 Cấu trúc khung tin Ethernet

Các chuẩn Ethernet đều hoạt động ở tầng Data Link trong mô hình 7 lớp OSI vì thế đơn vị dữ liệu mà các trạm trao đổi với nhau là các khung (frame). Cấu trúc khung Ethernet như sau:



Hình 2-17: Cấu trúc khung tin Ethernet

Các trường quan trọng trong phần mào đầu sẽ được mô tả dưới đây:

- preamble: trường này đánh dấu sự xuất hiện của khung bit, nó luôn mang giá trị 10101010. Từ nhóm bit này, phía nhận có thể tạo ra xung đồng hồ 10 Mhz.
- SFD (start frame delimiter): trường này mới thực sự xác định sự bắt đầu của 1 khung. Nó luôn mang giá trị 10101011.
- Các trường Destination và Source: mang địa chỉ vật lý của các trạm nhận và gửi khung, xác định khung được gửi từ đâu và sẽ được gửi tới đâu.
- LEN: giá trị của trường nói lên độ lớn của phần dữ liệu mà khung mang theo.
- FCS mang CRC (cyclic redundancy checksum): phía gửi sẽ tính toán trường này trước khi truyền khung. Phía nhận tính toán lại CRC này theo

cách tương tự. Nếu hai kết quả trùng nhau, khung được xem là nhận đúng, ngược lại khung coi như là lỗi và bị loại bỏ.

2.2.2.2 Cấu trúc địa chỉ Ethernet

Mỗi giao tiếp mạng Ethernet được định danh duy nhất bởi 48 bit địa chỉ (6 octet). Đây là địa chỉ được ấn định khi sản xuất thiết bị, gọi là địa chỉ MAC (Media Access Control Address).

Địa chỉ MAC được biểu diễn bởi các chữ số hexa (hệ cơ số 16). Ví dụ :

00:60:97:8F:4F:86 hoặc 00-60-97-8F-4F-86.

Khuôn dạng địa chỉ MAC được chia làm 2 phần:

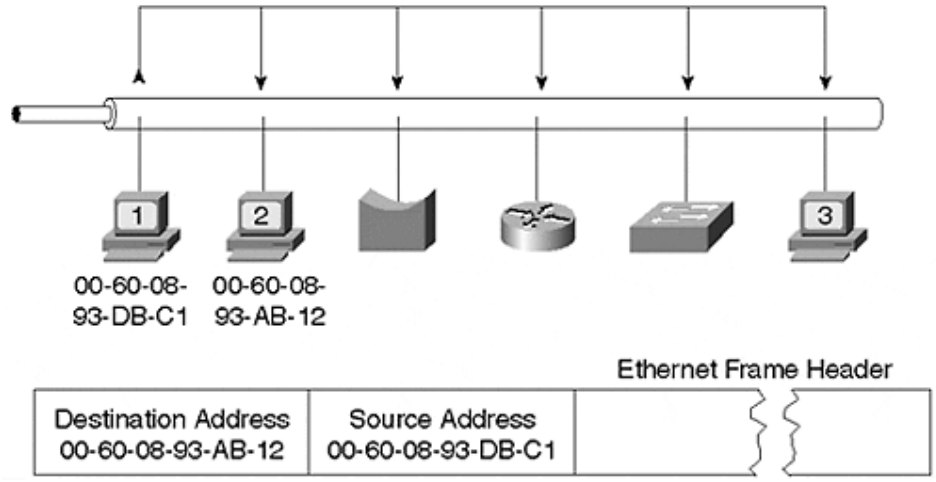
- 3 octet đầu xác định hãng sản xuất, chịu sự quản lý của tổ chức IEEE.
- 3 octet sau do nhà sản xuất ấn định.

Kết hợp ta sẽ có một địa chỉ MAC duy nhất cho một giao tiếp mạng Ethernet. Địa chỉ MAC được sử dụng làm địa chỉ nguồn và địa chỉ đích trong khung Ethernet.

2.2.2.3 Các loại khung Ethernet

- Các khung unicast

Giả sử trạm 1 cần truyền khung tới trạm 2 (trên hình vẽ ...)



Khung Ethernet do trạm 1 tạo ra có địa chỉ:

MAC nguồn: 00-60-08-93-DB-C1

MAC đích: 00-60-08-93-AB-12

Đây là khung unicast. Khung này được truyền tới một trạm xác định.

+ Tất cả các trạm trong phân đoạn mạng trên sẽ đều nhận được khung này nhưng:

+ Chỉ có trạm 2 thấy địa chỉ MAC đích của khung trùng với địa chỉ MAC của giao tiếp mạng của mình nên tiếp tục xử lý các thông tin khác trong khung.

+ Các trạm khác sau khi so sánh địa chỉ sẽ bỏ qua không tiếp tục xử lý khung nữa.

- Các khung broadcast

Các khung broadcast có địa chỉ MAC đích là FF-FF-FF-FF-FF-FF (48 bit 1). Khi nhận được các khung này, mặc dù không trùng với địa chỉ MAC của giao tiếp mạng của mình nhưng các trạm đều phải nhận khung và tiếp tục xử lý.

Giao thức ARP sử dụng các khung broadcast này để tìm địa chỉ MAC tương ứng với một địa chỉ IP cho trước.

Một số giao thức định tuyến cũng sử dụng các khung broadcast để các router trao đổi bảng định tuyến.

- Các khung multicast

Trạm nguồn gửi khung tới một số trạm nhất định chứ không phải là tất cả. Địa chỉ MAC đích của khung là địa chỉ đặc biệt mà chỉ các trạm trong cùng nhóm mới chấp nhận các khung gửi tới địa chỉ này.

Note: Địa chỉ MAC nguồn của khung luôn là địa chỉ MAC của giao tiếp mạng tạo ra khung. Trong khi đó địa chỉ MAC đích của khung thì phụ thuộc vào một trong ba loại khung nêu trên.

2.2.2.4 Hoạt động của Ethernet

Phương thức điều khiển truy nhập CSMA/CD quy định hoạt động của hệ thống Ethernet.

Một số khái niệm cơ bản liên quan đến quá trình truyền khung Ethernet:

- Khi tín hiệu đang được truyền trên kênh truyền, kênh truyền lúc này bận và ta gọi trạng thái này là có sóng mang – carrier.
- Khi đường truyền rỗi: không có sóng mang – absence carrier.
- Nếu hai trạm cùng truyền khung đồng thời thì chúng sẽ phát hiện ra sự xung đột và phải thực hiện lại quá trình truyền khung.
- Khoảng thời gian để một giao tiếp mạng khôi phục lại sau mỗi lần nhận khung được gọi là khoảng trống liên khung (interframe gap) – ký hiệu IFG. Giá trị của IFG bằng 96 lần thời gian của một bit.

  Ethernet 10Mb/s: IFG = 9,6 us

  Ethernet 100Mb/s: IFG = 960 ns

  Ethernet 1000Mb/s: IFG = 96 ns

Cách thức truyền khung và phát hiện xung đột diễn ra như sau:

+ 1. Khi phát hiện đường truyền rỗi, máy trạm sẽ đợi thêm một khoảng thời gian bằng IFG, sau đó nó thực hiện ngay việc truyền khung. Nếu truyền nhiều khung thì giữa các khung phải cách nhau khoảng IFG.

+ 2. Trong trường hợp đường truyền bận, máy trạm sẽ tiếp tục lắng nghe đường truyền cho đến khi đường truyền rỗi thì thực hiện lại 1.

+ 3. Trường hợp khi quá trình truyền khung đang diễn ra thì máy trạm phát hiện thấy sự xung đột, máy trạm sẽ phải tiếp tục truyền 32 bit dữ liệu. Nếu sự xung đột được phát hiện ngay khi mới bắt đầu truyền khung thì máy trạm sẽ phải truyền hết trường preamble và thêm 32 bit nữa , việc truyền nốt các bit này (ta xem như là các bit báo hiệu tắc nghẽn) đảm bảo tín hiệu sẽ tồn tại trên đường truyền đủ lâu cho phép các trạm khác (trong các trạm gây ra xung đột) nhận ra được sự xung đột và xử lý :

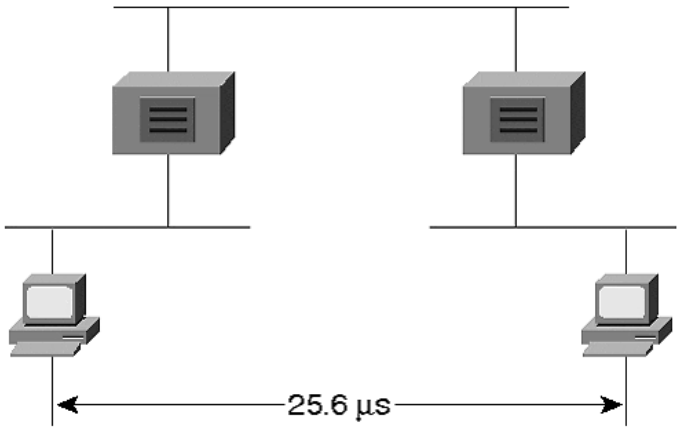
- Sau khi truyền hết các bit báo hiệu tắc nghẽn, máy trạm sẽ đợi trong một khoảng thời gian ngẫu nhiên hy vọng sau đó sẽ không gặp xung đột và thực hiện lại việc truyền khung như bước 1.
- Trong lần truyền khung tiếp theo này mà vẫn gặp xung đột, máy trạm buộc phải đợi thêm lần nữa với khoảng thời gian ngẫu nhiên nhưng dài hơn.

+ 4. Khi một trạm truyền thành công 512 bit (không tính trường preamble), ta xem như kênh truyền đã bị chiếm. Điều này cũng có nghĩa là không thể có xung đột xảy ra nữa. Khoảng thời gian ứng với thời gian của 512 bit được gọi là slotTime. Đây là tham số quan trọng quyết định nhiều tới việc thiết kế.

Do bản chất cùng chia sẻ kênh truyền, tại một thời điểm chỉ có một trạm được phép truyền khung. Càng có nhiều trạm trong phân đoạn mạng thì sự xung đột càng xảy ra nhiều, khi đó tốc độ truyền bị giảm xuống.

Sự xung đột là hiện tượng xảy ra bình thường trong hoạt động của mạng Ethernet (từ xung đột dễ gây hiểu nhầm là mạng bị sự cố hay là hoạt động sai, hỏng hóc).

Khái niệm slotTime



Hình 2-18: Hai trạm hai phía xa nhất trong mạng Ethernet 10Mb/s

Trong ví dụ này, trạm 1 và trạm 2 được xem như hai trạm ở hai phía xa nhất của mạng. Trạm 1 truyền khung tới trạm 2, ngay trước khi khung này tới trạm 2, trạm 2 cũng quyết định truyền khung (vì nó thấy đường truyền rỗi).

Để mạng Ethernet hoạt động đúng, mỗi máy trạm phải phát hiện và thông báo sự xung đột tới trạm xa nhất trong mạng trước khi một trạm nguồn hoàn thành việc truyền khung.

Khung Ethernet kích cỡ nhỏ nhất là 512 bit (64 octet), do đó khoảng thời gian nhỏ nhất để phát hiện và thông báo xung đột là 512 lần thời gian một bit.

Ethernet 10Mb/s : slot Time = 51,2 us

Ethernet 100Mb/s : slot Time = 5,12 us

Ethernet 1000Mb/s : slot Time = 512 ns

Trường hợp vi phạm thời gian slotTime, mạng Ethernet sẽ hoạt động không đúng nữa. Mỗi lần truyền khung, máy trạm sẽ lưu khung cần truyền trong bộ đệm cho đến khi nó truyền thành công. Giả sử mạng không đáp ứng đúng tham số slotTime. Trạm 1 truyền 512 bit thành công không hề bị xung đột, lúc này khung được xem là truyền thành công và bị xoá khỏi bộ đệm. Do sự phát hiện xung đột bị trễ, trạm 1 lúc này muốn truyền lại khung cũng không được nữa vì khung đã bị xoá khỏi bộ đệm rồi. Mạng sẽ không hoạt động đúng.

Một mạng Ethernet được thiết kế đúng phải thoả mãn điều kiện sau:

“ Thời gian trễ tổng cộng lớn nhất để truyền khung Ethernet từ trạm này tới trạm khác trên mạng phải nhỏ hơn một nửa slotTime”.

Thời gian trễ tổng cộng nói tới ở đây bao gồm trễ qua các thành phần truyền khung: trễ truyền tín hiệu trên cáp nối, trễ qua bộ repeater. Thời gian trễ của từng thành phần phụ thuộc vào đặc tính riêng của chúng. Các nhà sản xuất thiết bị ghi

rõ và khi thiết kế cần lựa chọn và tính toán để thoả mãn điều kiện hoạt động đúng của mạng Ethernet.

2.2.3 Các loại mạng Ethernet

IEEE đã phát triển chuẩn Ethernet trên nhiều công nghệ truyền dẫn khác nhau vì thế có nhiều loại mạng Ethernet. Mỗi loại mạng được mô tả dựa theo ba yếu tố: tốc độ, phương thức tín hiệu sử dụng và đặc tính đường truyền vật lý.

Các hệ thống Ethernet 10Mb/s :

- 10Base5. Đây là tiêu chuẩn Ethernet đầu tiên, dựa trên cáp đồng trục loại dày. Tốc độ đạt được 10 Mb/s, sử dụng băng tần cơ sở, chiều dài cáp tối đa cho 1 phân đoạn mạng là 500m.
- 10Base2. Có tên khác là "thin Ethernet" , dựa trên hệ thống cáp đồng trục mỏng với tốc độ 10 Mb/s, chiều dài cáp tối đa của phân đoạn là 185 m (IEEE làm tròn thành 200m).
- 10BaseT. Chữ T là viết tắt của "twisted": cáp xoắn cặp. 10BaseT hoạt động tốc độ 10 Mb/s dựa trên hệ thống cáp xoắn cặp Cat 3 trở lên.
- 10BaseF. F là viết tắt của Fiber Optic (sợi quang). Đây là chuẩn Ethernet dùng cho sợi quang hoạt động ở tốc độ 10 Mb/s , ra đời năm 1993.

Các hệ thống Ethernet 100 Mb/s – Ethernet cao tốc (Fast Ethernet)

- 100BaseT. Chuẩn Ethernet hoạt động với tốc độ 100 Mb/s trên cả cắp xoắn cặp lẫn cáp sợi quang.
- 100BaseX. Chữ X nói lên đặc tính mã hóa đường truyền của hệ thống này (sử dụng phương pháp mã hoá 4B/5B của chuẩn FDDI). Bao gồm 2 chuẩn 100BaseFX và 100BaseTX
    - 100BaseFX. Tốc độ 100Mb/s, sử dụng cáp sợi quang đa mode.
    - 100BaseTX. Tốc độ 100Mb/s, sử dụng cắp xoắn cặp.
- 100BaseT2 và 100BaseT4. Các chuẩn này sử dụng 2 cặp và 4 cặp cáp xoắn cặp Cat 3 trở lên tuy nhiên hiện nay hai chuẩn này ít được sử dụng.

Các hệ thống Giga Ethernet

- 1000BaseX. Chữ X nói lên đặc tính mã hoá đường truyền (chuẩn này dựa trên kiểu mã hoá 8B/10B dùng trong hệ thống kết nối tốc độ cao Fibre Channel được phát triển bởi ANSI). Chuẩn 1000BaseX gồm 3 loại:
    - 1000Base-SX: tốc độ 1000 Mb/s, sử dụng sợi quang với sóng ngắn.

- 1000Base-LX: tốc độ 1000 Mb/s, sử dụng sợi quang với sóng dài.
- 1000Base-CX: tốc độ 1000 Mb/s, sử dụng cáp đồng.

- 1000BaseT. Hoạt động ở tốc độ Giga bit, băng tần cơ sở trên cáp xoắn cặp Cat 5 trở lên. Sử dụng kiểu mã hoá đường truyền riêng để đạt được tốc độ cao trên loại cáp này.

2.3 Các kỹ thuật chuyển mạch trong LAN.

2.3.1 Phân đoạn mạng trong LAN

2.3.1.1 Mục đích của phân đoạn mạng

Mục đích là phân chia băng thông hợp lý đáp ứng nhu cầu của các ứng dụng trong mạng. Đồng thời tận dụng hiệu quả nhất băng thông đang có. Để thực hiện tốt điều này cần hiểu rõ khái niệm: miền xung đột (collition domain) và miền quảng bá (broadcast domain)

- **Miền xung đột (còn được gọi là miền băng thông – bandwidth domain)**

Như đã mô tả trong hoạt động của Ethernet, hiện tượng xung đột xảy ra khi hai trạm trong cùng một phân đoạn mạng đồng thời truyền khung. Miền xung đột được định nghĩa là vùng mạng mà trong đó các khung phát ra có thể gây xung đột với nhau. Càng nhiều trạm trong cùng một miền xung đột thì sẽ làm tăng sự xung đột và làm giảm tốc độ truyền, vì thế mà miền xung đột còn có thể gọi là miền băng thông (các trạm trong cùng miền này sẽ chia sẻ băng thông của miền).

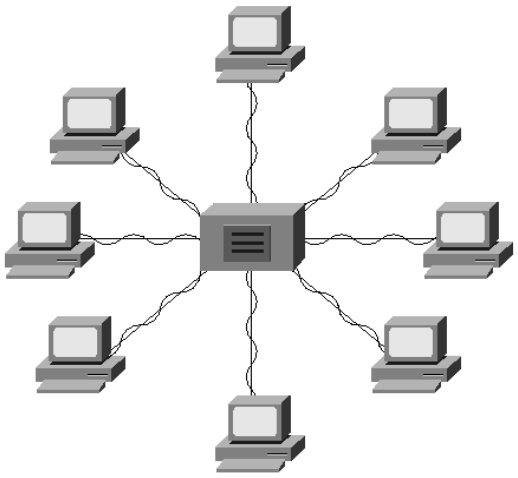
- **Miền quảng bá (broadcast domain)**

Miền quảng bá được định nghĩa là tập hợp các thiết bị mà trong đó khi một thiết bị phát đi một khung quảng bá (khung broadcast) thì tất cả các thiết bị còn lại đều nhận được.

Khi sử dụng các thiết bị kết nối khác nhau, ta sẽ phân chia mạng thành các miền xung đột và miền quảng bá khác nhau.

2.3.1.2 Phân đoạn mạng bằng Repeater

Thực chất repeater không phân đoạn mạng mà chỉ mở rộng đoạn mạng về mặt vật lý. Nói chính xác, repeater cho phép mở rộng miền xung đột.



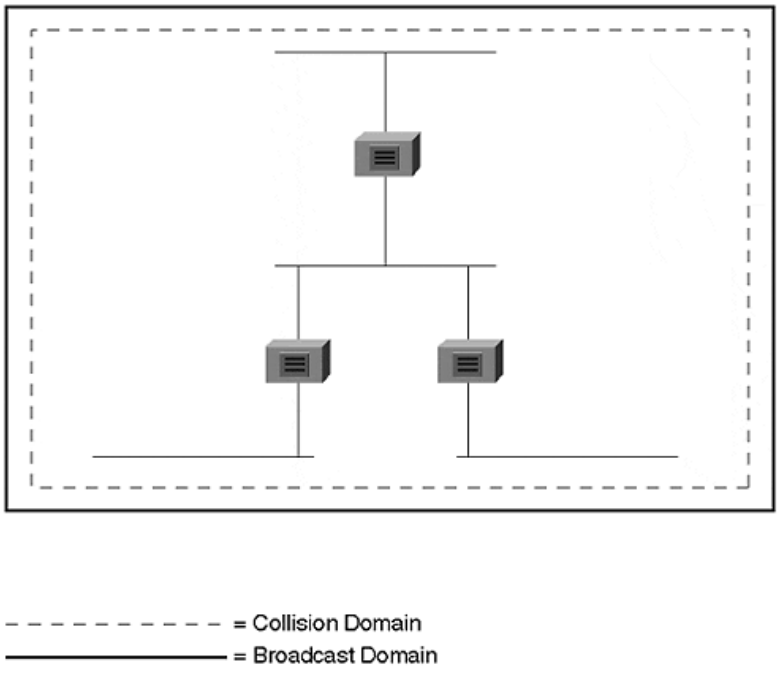
Hình 2-19: Kết nối mạng Ethernet 10BaseT sử dụng Hub

Hệ thống 10BaseT sử dụng hub như là một bộ repeater nhiều cổng. Các máy trạm cùng nối tới một hub sẽ thuộc cùng một miền xung đột.

Giả sử 8 trạm nối cùng một hub 10BaseT tốc độ 10Mb/s, vì tại một thời điểm chỉ có một trạm được truyền khung nên băng thông trung bình mỗi trạm có được là:

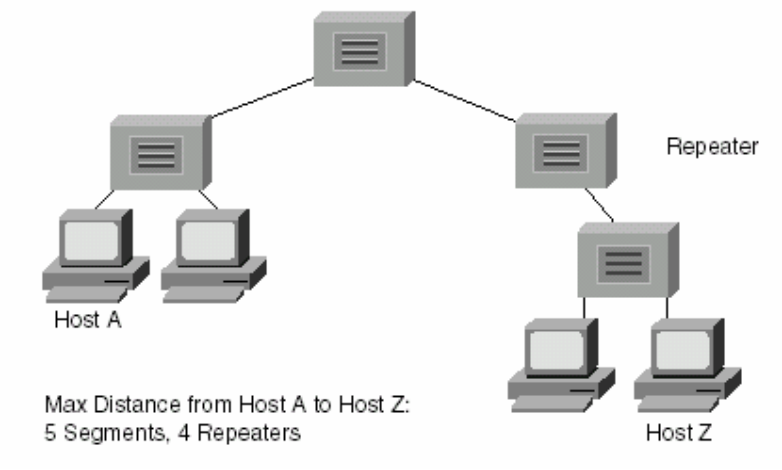
10 Mb/s : 8 trạm = 1,25 Mbps / 1 trạm.

Hình sau minh hoạ miền xung đột và miền quảng bá khi sử dụng repeater:



Hình 2-20: Miền xung đột và miền quảng bá khi phân đoạn mạng bằng Repeater

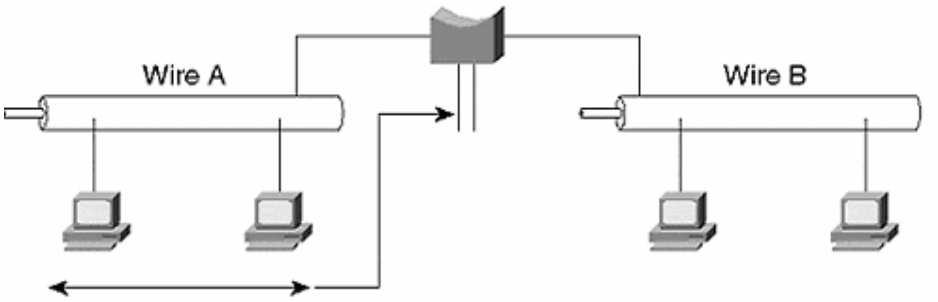
Một điều cần chú ý khi sử dụng repeater để mở rộng mạng, thì khoảng cách xa nhất giữa 2 máy trạm sẽ bị hạn chế. Trong hoạt động của Ethernet, trong cùng miền xung đột, giá trị slotTime sẽ quy định việc kết nối các thiết bị. Việc sử dụng nhiều repeater làm tăng giá trị trễ truyền khung vượt quá giá trị cho phép gây ra hoạt động không đúng trong mạng.



Hình 2-21: Luật 5-4-3 quy định việc sử dụng Repeater để liên kết mạng

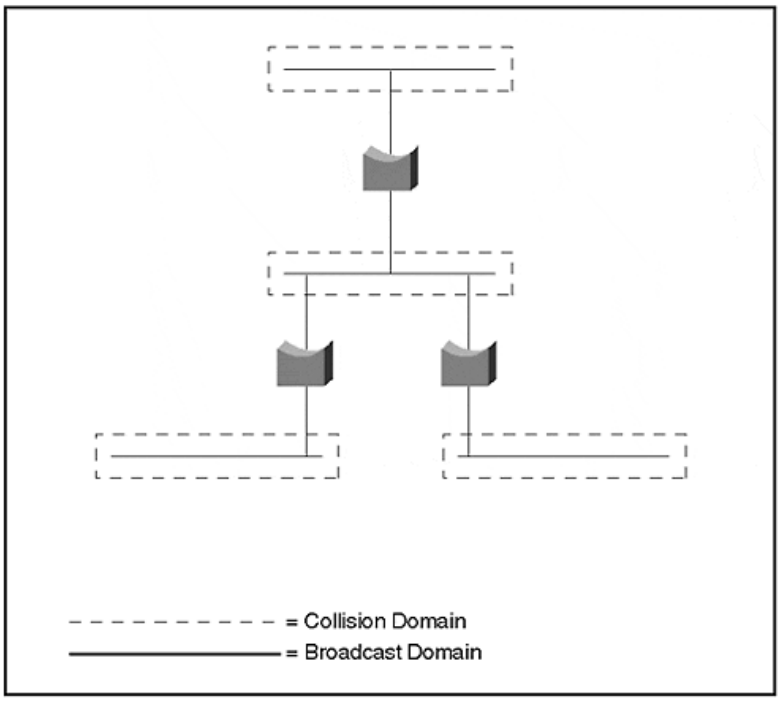
2.3.1.3 Phân đoạn mạng bằng cầu nối

Cầu nối hoạt động ở tầng 2 trong mô hình OSI, nó có khả năng kiểm tra phần địa chỉ MAC trong khung, và dựa vào địa chỉ nguồn, đích, nó sẽ đưa ra quyết định đẩy khung này tới đâu. Quan trọng là qua đó ta có thể liên kết các miền xung đột với nhau trong cùng một miền quảng bá mà các miền xung đột này vẫn độc lập với nhau.



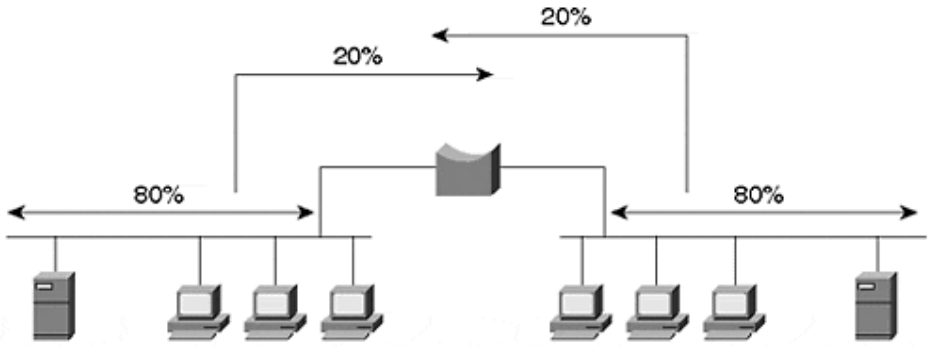
Hình 2-22: Việc truyền khung tin diễn ra phía A không xuất hiện bên phía B

Khác với trường hợp sử dụng repeater ở trên, băng thông lúc này chỉ bị chia sẻ trong từng miền xung đột, mỗi máy trạm được sử dụng nhiều băng thông hơn.
Lợi ích khác của việc sử dụng cầu là ta có hai miền xung đột riêng biệt nên mỗi miền có riêng giá trị slotTime do vậy có thể mở rộng tối đa cho từng miền.



Hình 2-23: Miền xung đột và miền quảng bá khi sử dụng Bridge

Tuy nhiên việc sử dụng cầu cũng bị giới hạn bởi quy tắc 80/20.
Theo quy tắc này, cầu chỉ hoạt động hiệu quả khi chỉ có 20 % tải của phân đoạn đi qua cầu , 80% là tải trong nội bộ phân đoạn.



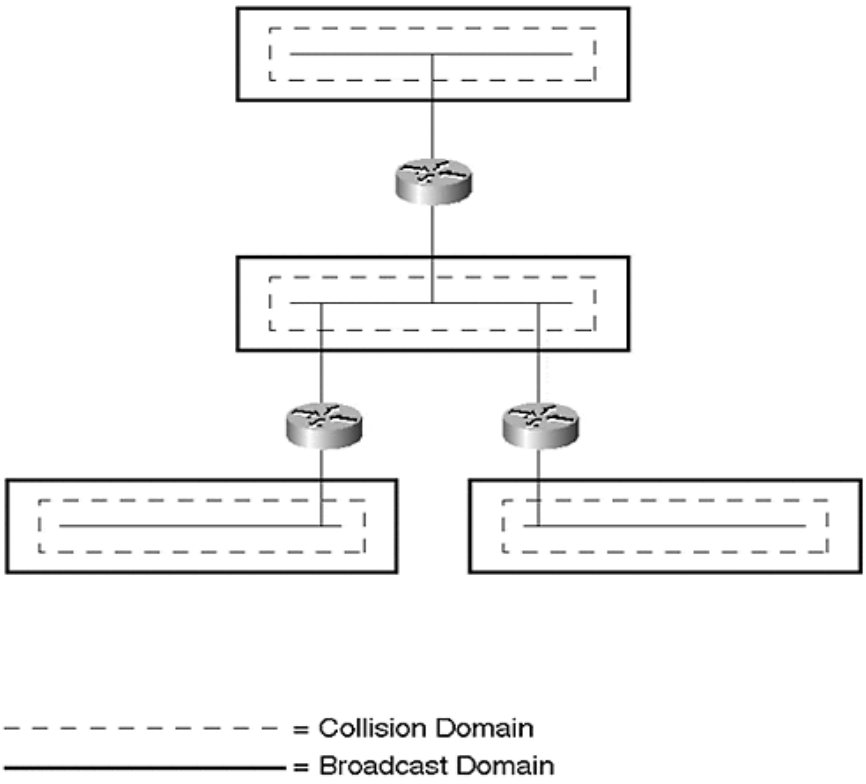
Hình 2-24: Quy tắc 80/20 đối với việc sử dụng Bridge

Trường hợp ngược lại với quy tắc này, hai phân đoạn kết nối bởi cầu có thể xem như cùng một phân đoạn mạng, không được lợi gì về băng thông.

2.3.1.4 Phân đoạn mạng bằng router

Router hoạt động ở tầng 3 trong mô hình OSI, nó có khả năng kiểm tra header của gói IP nên đưa ra quyết định. Đơn vị dữ liệu mà các bộ định tuyến thao tác là các gói IP (các bộ chuyển mạch và cầu nối thao tác với các khung tin).

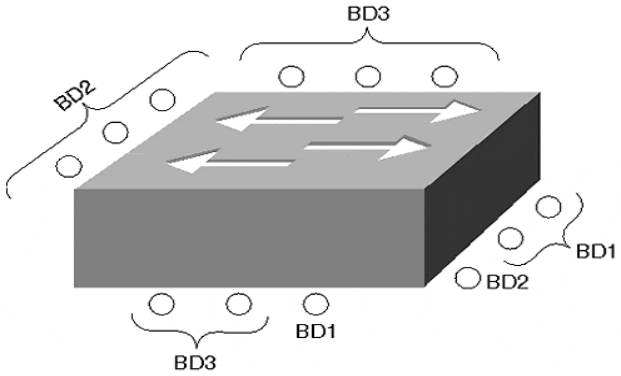
Bộ định tuyến đồng thời tạo ra các miền xung đột và miền quảng bá riêng biệt.



Hình 2-25: Phân đoạn mạng bằng Router

2.3.1.5 Phân đoạn mạng bằng bộ chuyển mạch

Bộ chuyển mạch là một thiết bị phức tạp nhiều cổng cho phép cấu hình theo nhiều cách khác nhau. Có thể cấu hình để nó trở thành nhiều cầu ảo như sau:



Hình 2-26: Có thể cấu hình bộ chuyển mạch thành nhiều cầu ảo

Bảng tổng kết thực hiện phân đoạn mạng bằng các thiết bị kết nối khác nhau:

Thiết bị	Miền xung đột	Miền quảng bá
Repeater	Một	Một
Bridge	Nhiều	Một
Router	Nhiều	Nhiều
Switch	Nhiều	Một hoặc nhiều

2.3.2 Các chế độ chuyển mạch trong LAN

Như phần trên đã trình bày, bộ chuyển mạch cung cấp khả năng tương tự như cầu nối, nhưng có khả năng thích ứng tốt hơn trong trường hợp phải mở rộng quy mô, cũng như trong trường hợp phải cải thiện hiệu suất vận hành của toàn mạng.

Bộ chuyển kết nối nhiều đoạn mạng hoặc thiết bị thực hiện chức năng của nó bằng cách xây dựng và duy trì một cơ sở dữ liệu lưu danh sách các cổng và các phân đoạn mạng kết nối tới. Khi một khung tin gửi tới, bộ chuyển mạch sẽ kiểm tra địa chỉ đích có trong khung tin, sau đó tìm số cổng tương ứng trong cơ sở dữ liệu để gửi khung tin tới đúng cổng.

Cách thức nhận và chuyển khung tin cho ta hai chế độ chuyển mạch:

- Chuyển mạch lưu-và-chuyển (store- and- forward switching)
- Chuyển mạch ngay (cut-through switching)

2.3.2.1 Chuyển mạch lưu-và-chuyển (store- and- forward switching)

Các bộ chuyển mạch lưu và chuyển hoạt động như cầu nối.

Trước hết, khi có khung tin gửi tới, bộ chuyển mạch sẽ nhận toàn bộ khung tin, kiểm tra tính toàn vẹn dữ liệu của khung tin, sau đó mới chuyển tiếp khung tin tới cổng cần chuyển.

Khung tin trước hết phải được lưu lại để kiểm tra tính toàn vẹn do đó sẽ có một độ trễ nhất định từ khi dữ liệu được nhận tới khi dữ liệu được chuyển đi.

Với chế độ chuyển mạch này, các khung tin đảm bảo tính toàn vẹn mới được chuyển mạch, các khung tin lỗi sẽ không được chuyển từ phân đoạn mạng này sang phân đoạn mạng khác.

2.3.2.2 Chuyển mạch ngay (cut-through switching)

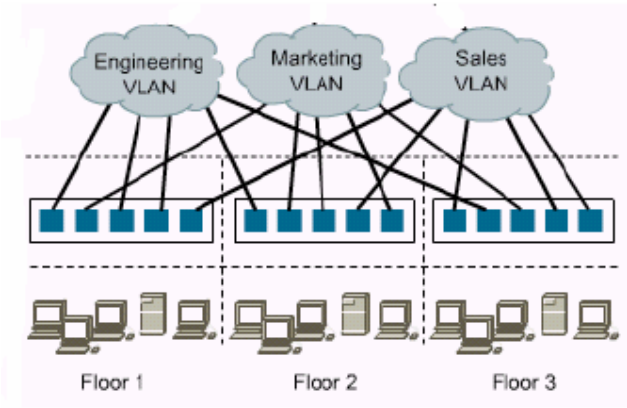
Các bộ chuyển mạch ngay hoạt động nhanh hơn so với các bộ chuyển mạch lưu-và-chuyển. Bộ chuyển mạch đọc địa chỉ đích ở phần đầu khung tin rồi chuyển ngay khung tin tới cổng tương ứng mà không cần kiểm tra tính toàn vẹn.

Khung tin được chuyển ngay thậm chí trước khi bộ chuyển mạch nhận đủ dòng bit dữ liệu. Khung tin đi ra khỏi bộ chuyển mạch trước khi nó được nhận đủ.

Các bộ chuyển mạch đời mới có khả năng giám sát các cổng của nó và quyết định sẽ sử dụng phương pháp nào thích hợp nhất. Chúng có thể tự động chuyển từ phương pháp chuyển ngay sang phương pháp lưu-và-chuyển nếu số lỗi trên cổng vượt quá một ngưỡng xác định.

2.3.3 Mạng LAN ảo (VLAN)

Như trong phần phân đoạn mạng đã trình bày, cầu nối và bộ chuyển mạch có thể tách mỗi cổng của chúng là một miền xung đột riêng nhưng tất cả đều thuộc cùng một miền quảng bá. Cách duy nhất để chia tách các miền quảng bá khác nhau là sử dụng các bộ định tuyến.



Hình 2-27: Mạng LAN ảo theo chức năng các phòng ban

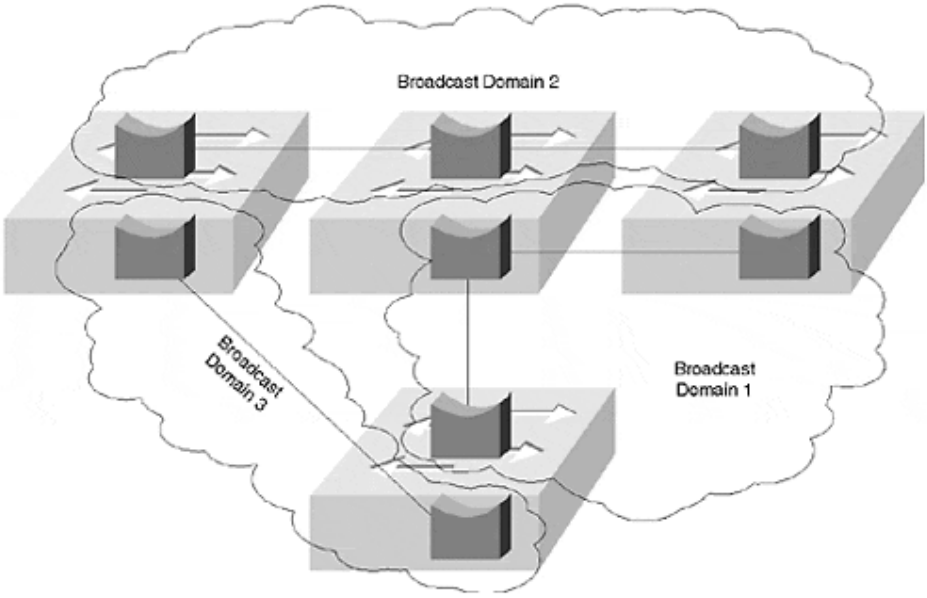
Tuy nhiên trong phần này chúng ta nói tới khả năng khác của các bộ chuyển mạch hiện đại, chúng có thể lọc các khung tin quảng bá và chỉ gửi chúng tới miền quảng bá xác định. Sử dụng các bộ chuyển mạch để kết hợp các thiết bị thành các vùng quảng bá logic sẽ tạo ra các mạng LAN ảo (VLAN).

2.3.3.1 Tạo mạng LAN ảo với một bộ chuyển mạch

Mỗi mạng LAN ảo và các thành viên của nó được xác định bởi một nhóm các cổng trên bộ chuyển mạch. Mỗi cổng của bộ chuyển mạch thuộc về một mạng LAN ảo nào đó, do đó các thiết bị gắn với cổng này sẽ thuộc về mạng LAN ảo này. Các khung tin quảng bá chỉ được phát tới các cổng thuộc cùng một mạng LAN ảo. Một thiết bị có thể chuyển từ LAN ảo sang LAN ảo khác bằng cách kết nối tới cổng khác của bộ chuyển mạch. Một thiết bị khi thay đổi vị trí địa lý vẫn thuộc về LAN ảo cũ nếu nó vẫn duy trì kết nối tới một trong các cổng thuộc về LAN ảo này.

2.3.3.2 Tạo mạng LAN ảo với nhiều bộ chuyển mạch

Trong thực tế, việc sử dụng nhiều bộ chuyển mạch để xây dựng các mạng LAN ảo được thực hiện nhiều hơn.



Hình 2-28: Cấu hình các bộ chuyển mạch tạo thành các miền quảng bá cho các mạng LAN ảo

Để thực hiện mạng LAN ảo bằng nhiều bộ chuyển mạch, một số định danh đặc biệt – VLAN ID được gán cho các khung tin, số này xác định mạng LAN ảo mà khung tin cần chuyển tới.

Giả sử một máy trạm A gửi khung tin tới máy trạm B thuộc cùng LAN ảo với mình (nhưng không cùng thuộc một bộ chuyển mạch). Bộ chuyển mạch mà máy A nối trực tiếp tới sẽ gán thêm vào khung tin chỉ số VLAN ID và chuyển nó tới bộ chuyển mạch kế tiếp.

Mỗi bộ chuyển mạch sẽ sử dụng VLAN ID để định tuyến khung tin, nó sẽ đọc VLAN ID và chuyển tiếp khung tin cho bộ chuyển mạch thích hợp. Khi khung tin tới bộ chuyển mạch cuối cùng, bộ chuyển mạch này nhận ra đích tới nối trực tiếp tới một trong các cổng của mình. Nó sẽ loại bỏ phần đầu chứa chỉ số VLAN ID rồi gửi khung tới đúng cổng. Khung tin khi tới trạm đích sẽ được khôi phục nguyên dạng ban đầu.

2.3.3.3 Cách xây dựng mạng LAN ảo

Để tạo ra mạng LAN ảo, cần phải xác định nhóm logic. Nhóm các máy tính (thiết bị) trong mạng LAN ảo thường được tổ chức theo hai mô hình:

- Mô hình nhóm làm việc.

Theo mô hình này, các thành viên trong mạng LAN ảo là các máy tính cùng thực hiện một chức năng, người sử dụng trong cùng một nhóm công việc. Các mạng LAN ảo thường được chia theo các phòng ban, ví dụ Phòng kế toán, phòng Bán hàng, Phòng nghiên cứu... Các tài nguyên khác chung của mạng sẽ thuộc về một hoặc nhiều mạng LAN ảo.

- Mô hình dịch vụ.

Theo mô hình này, các mạng LAN ảo được phân chia theo loại hình dịch vụ cụ thể. Ví dụ, tất cả các máy tính cần truy nhập tới dịch vụ đặc thù nào đó sẽ là thành viện của cùng một mạng LAN ảo. Các máy tính có thể là thành viên của nhiều mạng LAN ảo khác nhau tuỳ thuộc vào các dịch vụ mà nó cần truy nhập tới.

2.3.3.4 Ưu điểm và nhược điểm của mạng LAN ảo

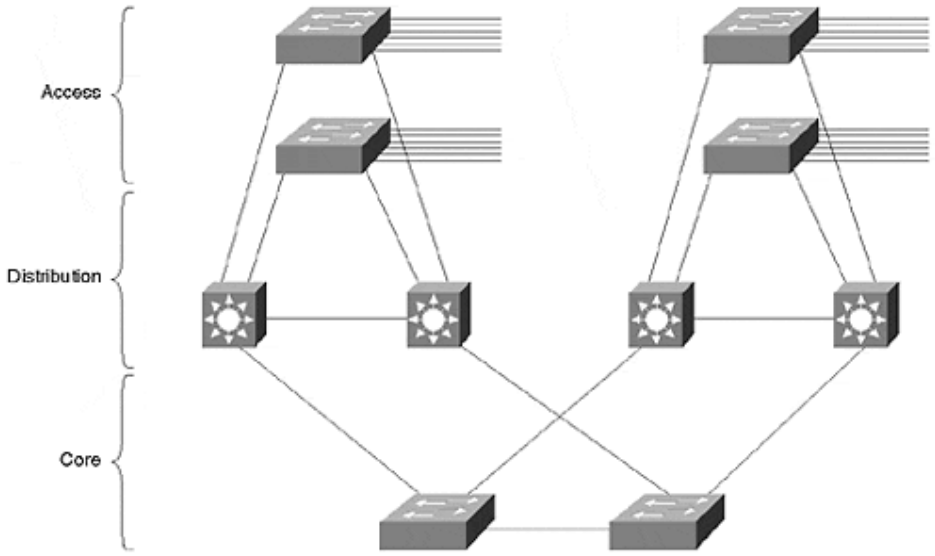
- Ưu điểm:
  - Có thể tạo ra mạng LAN ảo, tạo ra các nhóm làm việc không phụ thuộc vào vị trí của thiết bị, chẳng hạn, những người thuộc cùng nhóm nghiên cứu không cần ngồi cùng một phòng hay cùng một tầng trong toà nhà mà vẫn là các thành viên trong một mạng LAN ảo.
  - Có thể dễ dàng di chuyển thiết bị từ mạng LAN ảo này sang mạng LAN ảo khác.
  - Mạng LAN ảo cho phép kiểm soát kiểm soát các miền quảng bá và kiếm soát tính bảo mật.
  - Ưu điểm khác là bằng việc sử dụng các bộ chuyển mạch thay cho các bộ định tuyến, hiệu năng làm việc đạt được cao hơn, giá thành rẻ hơn, khả năng quản trị tốt hơn.
- Nhược điểm:

Hiện nay, chuẩn chính thức cho VLAN (Uỷ ban IEEE 802.1q đang soạn thảo) chưa được phê chuẩn mặc dù chuẩn này được hỗ trợ bởi nhiều nhà cung cấp. Do đó các thiết lập và cấu hình VLAN phụ thuộc vào nhà sản xuất thiết bị.

2.4 Thiết kế mạng LAN.

2.4.1 Mô hình cơ bản.

2.4.1.1 Mô hình phân cấp (Hierarchical models)



Hình 2-29: Mô hình phân cấp

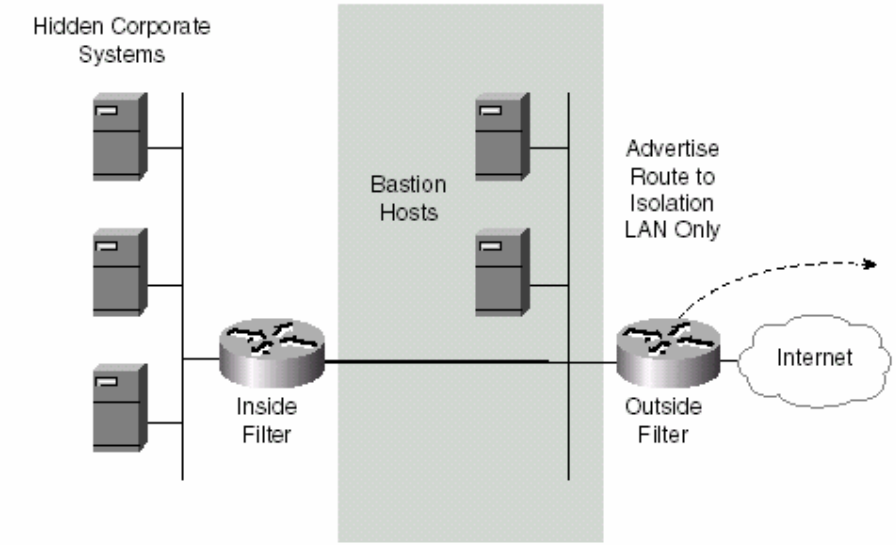
- **Cấu trúc**
  - Lớp lõi (Core Layer): Đây là trục xương sống của mạng(backbone) thường dùng các bộ chuyển mạch có tốc độ cao(high-speed switching), thường có các đặc tính như độ tin cậy cao, có công suất dư thừa, có khả năng tự khắc phục lỗi, có khả năng thích nghi cao, đáp ứng nhanh, dễ quản lý, có khả năng lọc gói, hay lọc các tiến trình đang truyền trong mạng.
  - Lớp phân tán (Distribution Layer) Lớp phân tán là gianh giới giữa lớp truy nhập và lớp lõi của mạng. lớp phân tán thực hiện các chức năng như đảm bảo gửi dữ liệu đến từng phân đoạn mạng, đảm bảo an ninh-an toàn, phân đoạn mạng theo nhóm công tác, chia miền Broadcast/multicast, định tuyến giữa các LAN ảo (VLAN), chuyển môi trường truyền dẫn, định tuyến giữa các miền, tạo biên giới giữa các miền trong định tuyến tĩnh và động, thực hiện các bộ lọc gói(theo địa chỉ, theo số hiệu cổng,...), thực hiện các cơ chế đảm bảo chất lượng dịch vụ QoS.
  - Lớp truy nhập(Access Layer) Lớp truy nhập cung cấp các khả năng truy nhập cho người dùng cục bộ hay từ xa truy nhập vào mạng. Thường được thực hiện bằng các bộ chuyển mạch(switch) trong môi trường campus, hay các công nghệ WAN.

➢ **Đánh giá mô hình**

- Giá thành thấp
- dễ cài đặt
- dễ mở rộng
- dễ cô lập lỗi.

2.4.1.2 Mô hình an ninh-an toàn(Secure models).

Hệ thống tường lửa 3 phần (Three-Part Firewall System), đặc biệt quan trọng trong thiết kế WAN, chúng tôi sẽ trình bày trong chương 3. Ở đây, chúng tôi chỉ nêu một số khía cạnh chung nhất cấu trúc của mô hình sử dụng trong thiết kế mạng LAN.



Hình 2-30: Mô hình tường lửa 3 phần

- LAN cô lập làm vùng đệm giữa mạng công tác với mạng bên ngoài(LAN cô lập được gọi là khu phi quân sự hay vùng DMZ)
- Thiết bị định tuyến trong có cài đặt bộ lọc gói được đặt giữa DMZ và mạng công tác.
- Thiết bị định tuyến ngoài có cài đặt bộ lọc gói được đặt giữa DMZ và mạng ngoài.

2.4.2 Các yêu cầu thiết kế

Các yêu cầu thiết kế của LAN về mặt cấu trúc cũng tương tự như thiết kế WAN, ở đây chúng tôi chỉ nêu đề mục bao gồm các yêu cầu:

- Yêu cầu kỹ thuật.
- Yêu cầu về hiệu năng.

- Yêu cầu về ứng dụng.
- Yêu cầu về quản lý mạng.
- Yêu cầu về an ninh-an toàn mạng.
- Yêu cầu 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.

2.4.3 Các bước thiết kế.

- **Phân tích yêu cầu**
  - Số lượng nút mạng (rất lớn trên 1000 nút, vừa trên 100 nút và nhỏ dưới 10 nút). Trên cơ sở số lượng nút mạng, chúng ta có phương thức phân cấp, chọn kỹ thuật chuyển mạch, và chọn thiết bị chuyển mạch.
  - Dựa vào mô hình phòng ban để phân đoạn vật lý đảm bảo hai yêu cầu an ninh và đảm bảo chất lượng dịch vụ.
  - Dựa vào mô hình topo lựa chọn công nghệ đi cáp.
  - Dự báo các yêu cầu mở rộng.
- **Lựa chọn phần cứng (thiết bị, cáp, công nghệ kết nối,...)**

Dựa trên các phân tích yêu cầu và kinh phí dự kiến cho việc triển khai, chúng ta sẽ lựa chọn nhà cung cấp thiết bị tốt nhất như là Cisco, Nortel, 3COM, Intel ...

- **Lựa chọn phần mềm**
  - Lựa chọn hệ điều hành Unix (AIX, OSF, HP, Solaris, ...), Linux , Windows dựa trên yêu cầu về xử lý số lượng giao dịch, đáp ứng thời gian thực, kinh phí, an ninh an toàn.
  - Lựa chọn các công cụ phát triển phần mềm ứng dụng như các phần mềm quản trị cơ sở dữ liệu (Oracle, Informix, SQL, Lotusnote, ...), các phần mềm portal như Websphere, ...
  - Lựa chọn các phần mềm mạng như thư điện tử (Sendmail, PostOffice, Netscape, ...), Web server (Apache, IIS, ...),
  - Lựa chọn các phần mềm đảm bảo an ninh an toàn mạng như phần mềm tường lửa (PIX, Checkpoint, Netfilter, ...), phần mềm chống virut (VirusWall, NAV, ...), phần mềm chống đột nhập và phần mềm quét lỗ hổng an ninh trên mạng.
- **Đánh giá khả năng**

- Dựa vào thông tin đã được xác minh của các hãng có uy tín trên thế giới.
- Thực hiện thử nghiệm và kiểm tra trong phòng thí nghiệm của các chuyên gia.
- Đánh giá trên mô hình thử nghiệm.

➢ **Tính toán giá thành**

Giá thành thấp đảm bảo các chỉ tiêu kỹ thuật, các yêu cầu của ứng dụng, tính khả mở của hệ thống.

➢ **Triển khai pilot.**

Triển khai ở quy mô nhỏ nhưng vẫn minh họa được toàn bộ các yêu cầu về kỹ thuật, yêu cầu về ứng dụng làm cơ sở cho việc đánh giá khả năng và giá thành của mạng trước khi triển khai trên diện rộng.

2.5 Một số mạng LAN mẫu.

2.5.1 Xây dựng mạng LAN quy mô một toà nhà

Xây dựng LAN trong tòa nhà điều hành không lớn, phục vụ cho công tác nghiên cứu và giảng dạy.

2.5.1.1 Hệ thống mạng bao gồm:

- Hệ thống các thiết bị chuyển mạch (switch, switch có chức năng định tuyến – layer 3 switch) cung cấp nền tảng mạng cho các máy tính có thể trao đổi thông tin với nhau. Do toàn bộ phân mạng xây dựng tập trung trong 1 toà nhà nên hệ thống cáp truyền dẫn sẽ sử dụng bao gồm các cáp đồng tiêu chuẩn UTP CAT5 và cáp quang đa mode. Công nghệ mạng cục bộ sẽ sử dụng là Ethernet/ FastEthernet/GigabitEthernet tương ứng tốc độ 10/100/100Mbps chạy trên cáp UTP hoặc cáp quang.
- Các máy chủ dịch vụ như cơ sở dữ liệu quản lý, giảng dạy, truyền thông…
- Các máy tính phục vụ cho công tác nghiên cứu khoa học : Cung cấp các thông tin cho sinh viên, giáo viên, và cung cấp công cụ làm việc cho các cán bộ giảng dạy, các bộ môn, khoa.
- Các máy tính phục vụ riêng cho công tác quản lý hành chính nhằm thực hiện mục tiêu tin học hoá quản lý hành chính.

2.5.1.2 Phân tích yêu cầu:

- Mạng máy tính này là LAN Campus Network có băng thông rộng đủ để khai thác hiệu quả các ứng dụng, cơ sở dữ liệu đặc trưng của tổ chức cũng như đáp ứng khả năng chạy các ứng dụng đa phương tiện (hình ảnh, âm thanh) phục vụ cho công tác giảng dạy từ xa.
- Như vậy, mạng này sẽ được xây dựng trên nền tảng công nghệ truyền dẫn tốc độ cao Ethernet/FastEthernet/GigabitEthernet và hệ thống cáp mạng xoắn UTP CAT5 và cáp quang đa mode.
- Mạng cần có độ ổn định cao và khả năng dự phòng để đảm bảo chất lượng cho việc truy cập các ứng dụng dữ liệu quan trọng cũng như đào tạo từ xa : hình ảnh, âm thanh... Như vậy, hệ thống cáp mạng phải có khả năng dự phòng 1:1 cho các kết nối switch-switch cũng như đảm bảo khả năng sửa chữa, cách ly sự cố dễ dàng.
- Mạng có khả năng cung cấp việc giảng dạy từ xa trong phạm vi tổ chức nên các ứng dụng phải đáp ứng thời gian thực.
- Hệ thống cáp mạng cần được thiết kể đảm bảo đáp ứng các yêu cầu về kết nối tốc độ cao và khả năng dự phòng cũng như mở rộng lên các công nghệ mới.
- Mạng cần đảm bảo an ninh an toàn cho toàn bộ các thiết bị nội bộ trước các truy nhập trái phép ở mạng ngoài cũng như từ các truy nhập gián tiếp có mục đích phá hoại hệ thống nên cần có tường lửa.
- LAN này được cấu thành bởi các switch chuyển mạch tốc độ cao hạn chế tối thiểu xung đột dữ liệu truyền tải (non-blocking). Các switch có khả năng tạo các LAN ảo phân đoạn mạng thành các phần nhỏ hơn cho từng phòng ban. LAN ảo là công nghệ dùng trong mạng nội bộ cho phép sử dụng cùng một nền tảng mạng nội bộ vật lý bao gồm nhiều switch được phân chia về mặt logic theo các cổng trên switch thành các phân mạng nhỏ khác nhau và độc lập hoạt động. Như vậy, ngay trong mạng LAN tại toà nhà điều hành ta có thể thực hiện phân chia thành các phân mạng nhỏ hơn nữa cho các khoa, phòng ban…Máy tính trong 1 phân mạng chia nhỏ thuộc về một broadcasting domain và các phân mạng này phải liên hệ với nhau qua bộ định tuyến router. Ngoài ra, mạng điều hành cũng áp dụng công nghệ định tuyến mới khiến việc liên kết giữa các phân mạng LAN của các văn phòng, khoa có thể thực hiện bằng những liên kết tốc độ cao trong các switch có

tính năng định tuyến (Layer 3) thay cho mô hình định tuyến truyền thống sử dụng bộ định tuyến router

- Việc phân chia các phân mạng LAN ảo cho phép các Phòng ban tổ chức có các phân mạng máy tính độc lập để tiện cho việc phát triển các ứng dụng nội bộ cũng như tăng cường tính bảo mật giữa các phân mạng máy tính của các phòng ban khác nhau. Tuy nhiên, LAN ảo cũng cho phép quản lý tập trung toàn bộ hệ thống mạng máy tính nhất là hệ thống máy chủ thay vì phát triển rất nhiều phân mạng một cách riêng rẽ. Điều này tạo ra môi trường làm việc tập trung cho người quản trị cũng như cắt giảm các chi phí do tập hợp được các thiết bị mạng lưới và máy chủ dich vụ hoạt động 24/24 vào một số phòng có điều kiện hạ tầng đầy đủ (điện nguồn ổn định, điều hoà hoạt động tốt) thay vì nằm rải rác trên các phòng ban khác nhau. Công nghệ mạng LAN ảo giải quyết đồng thời được hai bài toán về quản trị tập trung và riêng rẽ cho mạng máy tính của tổ chức.
- Mạng đảm bảo khả năng định tuyến trao đổi thông tin giữa các phân mạng LAN ảo khác nhau, cho phép các phân mạng khác nhau có thể kết nối đến nhau thông qua môi trường mạng dùng chung. Tuy nhiên, do phân cách các mạng LAN bằng switch có tính năng định tuyến (hay còn gọi là switch có chức năng Layer 3) nên các gói tin broadcasting trên toàn mạng được hạn chế it đi và làm cho băng thông của mạng dược sử dụng hiệu quả hơn so với trường hợp toàn bộ mạng của Trường xây dựng thành một mạng LAN không phân cấp (flat network). Ngoài ra, khi sử dụng chức năng định tuyến cho phép người quản trị mạng được phép định nghĩa các luật hạn chế hay cho phép các phân mạng được kết nối với nhau bằng các bộ lọc (access-list) tăng cường tính bảo mật cho các phân mạng quan trọng cũng như khả năng quản trị hệ thống dễ dàng hơn.

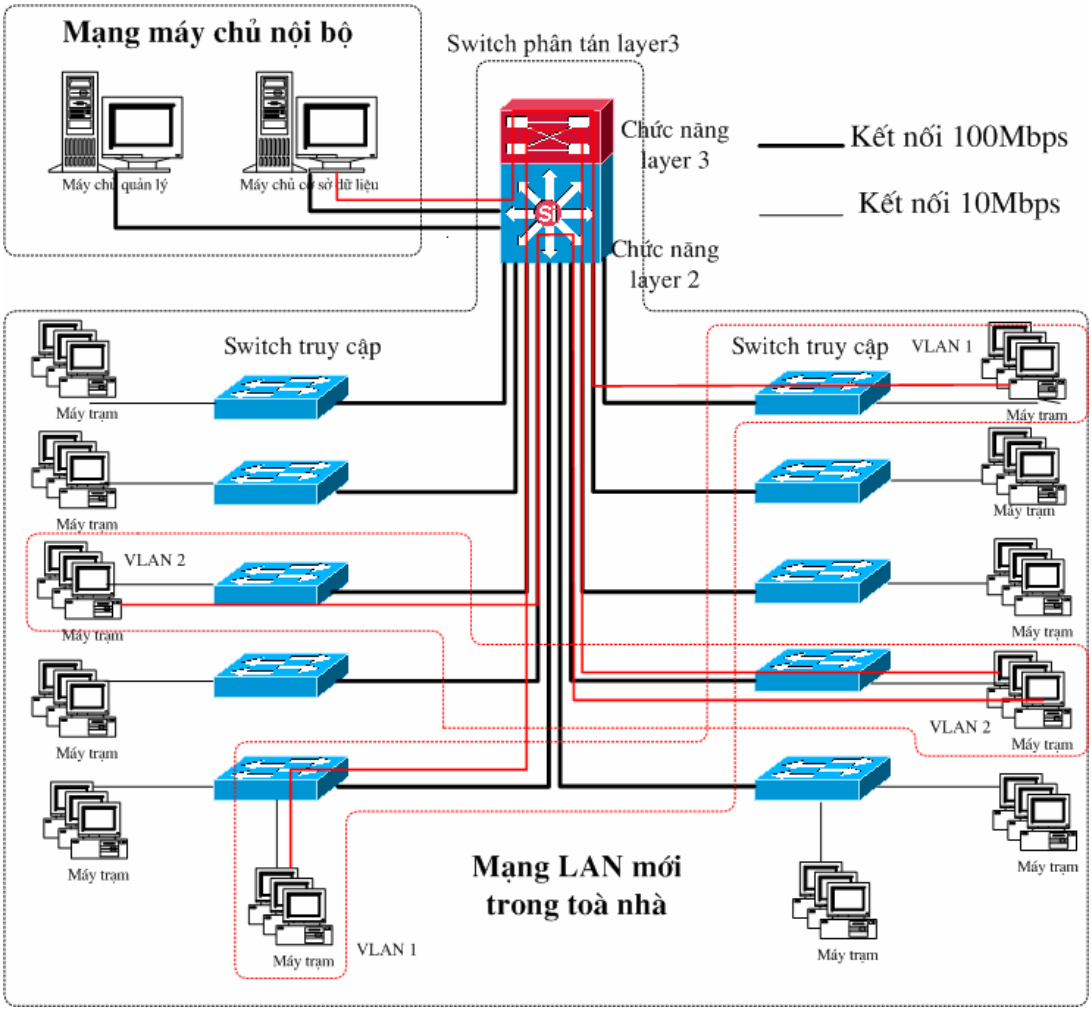
2.5.1.3 Thiết kế hệ thống

Hệ thống chuyển mạch và định tuyến trung tâm cho LAN

- Hệ thống chuyển mạch chính bao gồm các switch có khả năng xử lý tốc độ cao có cấu trúc phân thành 2 lớp là lớp phân tán (distribution) và lớp cung cấp truy nhập (access) cho các đầu cuối máy tính. Switch phân tán là switch tốc độ cao, băng thông lớn có khả năng xử lý đến hàng trăm triệu bít/giây. Switch phân phối còn có có chức năng định tuyến cho các phân

mạng LAN ảo khác nhau thiết lập trên mạng và tăng cường bảo mật cho các phân mạng riêng rẽ. Switch truy cập làm nhiệm vụ cung cấp cổng truy nhập cho các đầu cuối máy tính và tích hợp cổng truy cập với mật độ cao. Các kết nối giữa switch truy cập và switch phân phối là các kết nối truyền tải dữ liệu qua lại cho các LAN ảo nên phải có tốc độ cao 100/1000Mbps. Các switch truy cập cung cấp các cổng truy cập cho máy tính mạng có tốc độ thấp hơn nên cần có cổng 10/100Mbps

- Hệ thống switch phân phối theo cấu hình chuẩn sẽ bao gồm 2 switch có cấu hình mạnh đáp ứng được nhu cầu chuyển mạch dữ liệu tốc độ cao và tập trung lưu lượng đến từ các access switch. Switch phân phối cũng đảm nhận chức năng định tuyến. Cấu hình 2 switch phân phối cho phép mạng lưới có độ dự phòng cao (dự phòng nóng 1:1) tuy nhiên trong trường hợp quy mô mạng ban đầu không lớn và kinh phí hạn chế vẫn có thể triển khai mạng với 1 switch phân phối đáp ứng được yêu cầu hoạt động. Tổ chức hoàn toàn có khả năng nâng cấp lên 2 switch phân phối trong tương lai do thiết kế mạng cáp đảm bảo yêu cầu trên.
- Hệ thống các switch truy cập cung cấp cho các máy tính đường kết nối vào mạng dữ liệu. Do phần lớn các giao tiếp mạng cho máy tính đầu cuối cũng như server hiện tại có băng thông 10/100Mbps nên các switch truy cập cũng sử dụng công nghệ 10/100 BaseTX FastEthernet và đáp ứng được mục tiêu cung cấp số lượng cổng truy nhập lớn để cho phép mở rộng số lượng người truy cập mạng trong tương lai. Các switch truy cập sẽ kết nối với switch phân phối để tập trung lưu lượng và thông qua switch phân phối với làm tác vụ tập trung và lưu chuyển qua lại lưu lượng dữ liệu sẽ giúp cho các máy tính nằm trên các switch khác nhau có thể liên lạc được với nhau. Các đường kết nối giữa switch truy cập và switch phân phối còn được gọi là các kết nối lên (up-link) và sử dụng công nghệ FastEthernet 100 BaseTX có băng thông 100Mbps. Trong tương lai, khi cần nâng cấp các kết nối uplink thì có thể sử dụng thay thế công nghệ 1000BaseT với tốc độ Gigabit



Hình 2-31: Mô hình thiết kế

– Trong cấu hình vẽ mạng máy tính cục bộ toà nhà điều hành có 1 switch phân phối có chức năng định tuyến (layer 3 switch). Switch này có tác dụng chuyển lưu lượng qua lại giữa các switch truy cập và một nhiệm vụ rất quan trọng là định tuyến giữa các LAN ảo. Bất kỳ một switch truy cập nào được kết nối đến switch phân phối bằng đường kết nối uplink 100Mbps và kết nối này đảm bảo cung cấp băng thông cho toàn bộ các máy tính kết nối đến switch truy cập. Switch phân phối sử dụng ở đây là thiết bị có nhiều cổng truy nhập 100Mbps . Các switch truy cập cung cấp 24 cổng 10/100 Mbps đảm bảo băng thông này cho từng máy trạm. Toàn bộ toàn nhà sẽ có 14 switch truy cập cung cấp số cổng tối đa cho khoảng 336 máy tính . Nếu số lượng máy tính trong toàn bộ toàn nhà phát triển lên, các switch truy cập có thể cắm xếp trồng để cung cấp số lượng cổng truy cập nhiều hơn hoặc các phòng ban có thể cắm switch mở rộng để cung cấp

thêm số cổng truy nhập. Tuy nhiên, việc cắm thêm switch mở rộng cần tuân thủ nguyên tắc về việc xây dựng mạng tránh tình trạng cắm thiết bị mạng (HUB, switch) mở rộng tràn lan và làm giảm đáng kể tố độ truy cập các máy tính của phân mạng ở xa khi tập trung nhiều lưu lượng tải năng vào 1 switch truy cập và làm quá tải băng thông uplink từ switch đó lên switch phân phối.

- Các switch truy cập được chia ra thành hai nhóm (gọi là closet) với mỗi nhóm 07 switch được đặt tại 2 phòng bao gồm 1 phòng thông tin và 1 phòng Trung tâm điều hành mạng trên tầng 3. Trung tâm điều hành mạng cũng là nơi đặt các máy chủ nội bộ và switch phân phối. Từ các phòng này có các phiến đấu cáp UTP và cáp được đưa đến các máy tính đặt rải rác trên nhiều phòng. Mỗi một nhóm switch do đó cung cấp truy cập cho một nửa của toà nhà .Thiết kế này cho phép các switch truy cập cung cấp được đủ số cổng cho các thiết bị máy tính của các khoa, phòng ban thoả mãn điều kiện dây cáp từ mỗi máy tính tới switch không vượt quá 100m, Đây là giới hạn độ dài vật lý khi sử dụng cáp mạng xoắn UTP CAT5 hoặc CAT5 với công nghệ 10/100FastEthernet. Mỗi một switch truy cập có 1 đường kết nối uplink lên switch.
- Khi xây dựng các mạng LAN ảo, kỹ thuật cho phép gán 1 cổng trên một switch bất kỳ vào một phân mạng LAN riêng rẽ. Khi đó, mặc dù sử dụng chung một hệ thống switch, chỉ có các máy tính trong cùng một phân mạng LAN mới có thể nhận được các gói tin gửi qua lại cho nhau. Có được điều đó là do switch sẽ kiểm tra thông tin về phân mạng LAN với mỗi một khung tin và chỉ gửi đến các máy tính trong cùng phân mạng. Các kết nối uplink sẽ là các kết nối trunking cho phép mọi thông tin LAN ảo được đi qua. Chính vì chỉ sử dụng trong 1 môi trường mạng vật lý nên các phân mạng LAN phân chia logic như ở đây goi là các LAN ảo. Trong hình vẽ trên có miêu tả hoạt động của các phân mạng LAN ảo. Ví dụ : thông tin giữa các máy tính trong phân mạng LAN 1 sẽ không được nhận bởi các máy tính trong phân mạng LAN 2 hoặc phân mạng máy chủ nội bộ. Nếu muốn đi từ phân mạng LAN 1 sang phân mạng LAN 2 cần đi qua bộ định tuyến của switch phân phối. Tương tự vấn đề với việc trao đổi thông tin giữa mạng LAN 1 với mạng máy chủ dịch vụ.

- Mạng máy chủ dịch vụ nội bộ tách rời trong một phân mạng LAN cho phép bảo mật tốt hơn và quản trị tập trung. Ví dụ : Khi có một phòng ban nào đó không cần truy nhập đến máy chủ dịch vụ nội bộ thì switch phân phối sẽ ngăn cản không cho liên lạc giữa phân mạng LAN đó với phân mạng LAN dành cho các máy chủ nội bộ và người quản trị có khả năng cho phép hoạt động qua lại giữa các LAN hoặc siết chặt an ninh, hạn chế truy cập với các phân mạng quan trọng. Nhờ các ưu thế về công nghệ giúp giảm bớt gánh nặng quản trị của người quản trị mạng và tạo ra được cơ hội phát triển mạnh mạng lưới.
- Trong trường hợp các khoa, phòng, ban cần phát triển ứng dụng đặc thù cho nội bộ khoa mình cũng có thể đặt máy chủ tập trung tại Trung tâm điều hành mạng và sử dụng công nghệ mạng LAN ảo để định nghĩa máy chủ kết nối trong phân mạng nhỏ dành cho khoa, phòng, ban đó. Như thế sẽ đảm bảo quản lý thiết bị chung nhưng vẫn mềm dẻo trong việc phân chia cấp độ quản trị một cách tương đối độc lập và riêng rẽ.
- Có thể xây dựng một phân mạng trung tâm máy tính tại khu máy chủ trung tâm để tạo điều kiên thuận lợi cho các cán bộ, giáo viên có thiết bị máy tính để thực hiện truy cập mạng lấy thông tin trong trường hợp cần thiết.
- Khi mạng phát triển, để tăng cường độ tin cậy của mạng lưới và mở rộng năng lực mạng, sẽ sử dụng 2 switch phân phối và mỗi switch truy cập được kết nối đến 02 switch phân phối bằng 02 đường uplink. Các switch phân phối cũng sẽ được kết nối với nhau theo một thủ tục cho phép thay thế lẫn nhau hoạt động của chức năng định tuyến trên các switch.

Hệ thống cáp

Hệ thống cáp được chia thành 02 phần. Mỗi phần phụ trách cung cấp truy nhập cho các máy tính nằm trong một nửa toà nhà. Do các switch trong một closet đặt cùng với switch phân phối tại Trung tâm điều hành mạng tầng 3 và các switch trong closet còn lại đặt trong 1 phòng đặt thiết bị trên cùng tầng 3 nên các cáp nối uplink từ các switch trong closet thứ hai sang switch phân phối sử dụng cáp UTP 25 đôi. Các cáp uplink từ các switch trong closet 1 do nằm cùng với switch phân phối sẽ là cáp nhảy 4 đôi. Tại các phòng đặt các thiết bị switch sẽ có các patch panel AMP với 24 cổng RJ-45/1 patch panel để tập trung đấu nối cho cáp mạng.

Cáp UTP nối giữa máy tính và switch truy cập là cáp 4 đôi kéo thẳng từ các patch panel AMP tại một trong 2 phòng đặt thiết bị switch đến các outlet riêng rẽ đặt gắn trên tường phòng gần nơi đặt các máy tính của người sử dụng. Do dây cáp có 4 đôi nên có thể sử dụng 2 đôi thừa làm dây dự phòng.

Quản lý và cấp phát địa chỉ IP

Mạng máy tính thư viện là mạng máy tính dùng riêng, do vậy sẽ được đánh địa chỉ IP trong dải địa chỉ IP dùng cho mạng dùng riêng quy định tại RFC1918 (Bao gồm các địa chỉ từ 10.0.0.0 đến 10.255.255.255, 172.16.0.0 đến 172.31.255.255 và địa chỉ 192.168.0.0 đến 192.168.255.255). Số lượng máy tính cho 1 segment mạng đông nhất được tính bằng một phần 4 số lượng máy tính dự tính sẽ có trong toàn nhà (Khoảng vài chục máy tính). Như vậy, có thể gán cho 2 segment máy tính bằng các phân lớp class C địa chỉ IP từ class C 192.168.0.0 đến 192.168.255.0

Hệ thống các máy chủ sẽ nằm trong phân mạng riêng và có địa chỉ IP gán trong phân lớp địa chỉ 172.18.0.0. Để có thể truy cập ra Internet, một số các máy chủ cần có tính năng che dấu địa chỉ như Firewall hay Proxy và các máy chủ này cần có địa chỉ IP thật. Các máy tính bên trong mạng sử dụng địa chỉ của các máy chủ khi kết nối ra Internet . Nếu các máy chủ cần cung cấp thông tin cho người dùng Internet thì cần phải đánh lại địa chỉ IP cho các máy chủ này là địa chỉ do IANA cung cấp.

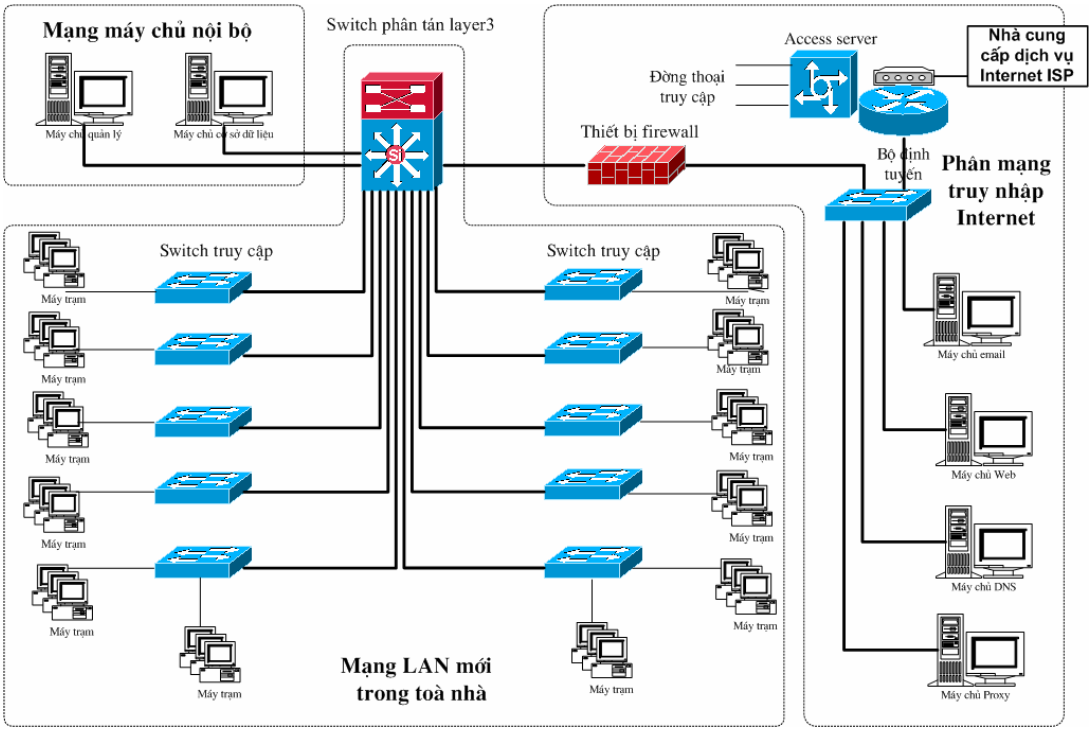
Để kết nối với các phân mạng máy tính của trường và mạng quốc gia, cần tuân thủ một qui định đánh địa chỉ chặt chẽ để khỏi sử dụng trùng vùng địa chỉ mạng dùng riêng. Có thể sử dụng các kỹ thuật chuyển đổi địa chỉ NAT để tránh xung đột địa chỉ khi kết nối 2 mạng.

Để thuận tiện cho công việc quản trị hệ thống, các thiết bị switch với khả năng hỗ trợ DHCP và cùng với việc thiết lập máy chủ DHCP, các máy tính trạm trong tòa nhà sẽ được cấp phát địa chỉ IP một cách tự động và tin cậy.

2.5.2 Xây dựng hệ thống tường lửa kết nối mạng với Internet

Tiếp theo, chúng ta mở rộng quy mô mạng LAN cho nhiều toà nhà trong khuôn viên của một tổ chức, một trường.

Mạng máy tính cục bộ sẽ được kết nối với phân mạng truy cập Internet thông qua Firewall. Firewall sẽ làm nhiệm vụ ngăn chặn và bảo mật các máy tính thuộc phân mạng nội bộ với mạng Internet phía bên ngoài. Như vậy một giao tiếp mạng của firewall sẽ kết nối với phân mạng bên trong và 1 giao tiếp mạng sẽ kết nối với phân mạng Internet công cộng.



Hình 2-32: Mô hình tường lửa kết nối mạng LAN với Internet

2.6 Tóm tắt chương 2

Chương này trình bày kiến thức về LAN bao gồm:

Kiến trúc mạng:

Cấu trúc tôpô

Phương pháp truy nhập

Phần hạ tầng LAN:

Các thiết bị kết nối mạng, hệ thống cáp nối.

Tập trung chủ yếu vào công nghệ mạng Ethernet, là công nghệ được dùng phổ biến hiện nay và trong tương lai gần.

Công nghệ Ethernet:

Nguyên lý hoạt động và các đặc tính quan trọng của Ethernet

Kỹ thuật chuyển mạch LAN

Phần cuối của chương trình bày phương pháp thiết kế mạng LAN sử dụng công nghệ Ethernet.

Thiết kế mạng LAN:

Mô hình thiết kế cơ bản

Các bước phân tích và thiết kế

Minh hoạ trong mô hình thực tế.

3 Chương III – Mạng WAN và thiết kế mạng WAN

3.1 Các kiến thức cơ bản về WAN.

3.1.1 Khái niệm về WAN

3.1.1.1 Mạng WAN là gì ?

Wide Area Networks – WAN, là mạng được thiết lập để liên kết các máy tính của hai hay nhiều khu vực khác nhau, ở khoảng cách xa về mặt địa lý, như giữa các quận trong một thành phố, hay giữa các thành phố hay các miền trong nước. Đặc tính này chỉ có tính chất ước lệ, nó càng trở nên khó xác định với việc phát triển mạnh của các công nghệ truyền dẫn không phụ thuộc vào khoảng cách. Tuy nhiên việc kết nối với khoảng cách địa lý xa buộc WAN phụ thuộc vào nhiều yếu tố như: giải thông và chi phí cho giải thông, chủ quản của mạng, đường đi của thông tin trên mạng.

WAN có thể kết nối thành mạng riêng của một tổ chức, hay có thể phải kết nối qua nhiều hạ tầng mạng công cộng và của các công ty viễn thông khác nhau.

WAN có thể dùng đường truyền có giải thông thay đổi trong khoảng rất lớn từ 56Kbps đến T1 với 1.544 Mbps hay E1 với 2.048 Mbps,....và đến Giga bít-Gbps là các đường trục nối các quốc gia hay châu lục. Ở đây bps (Bit Per Second) là một đơn vị trong truyền thông tương đương với 1 bit được truyền trong một giây, ví dụ như tốc độ đường truyền là 1 Mbps tức là có thể truyền tối đa 1 Megabit trong 1 giây trên đường truyền đó).

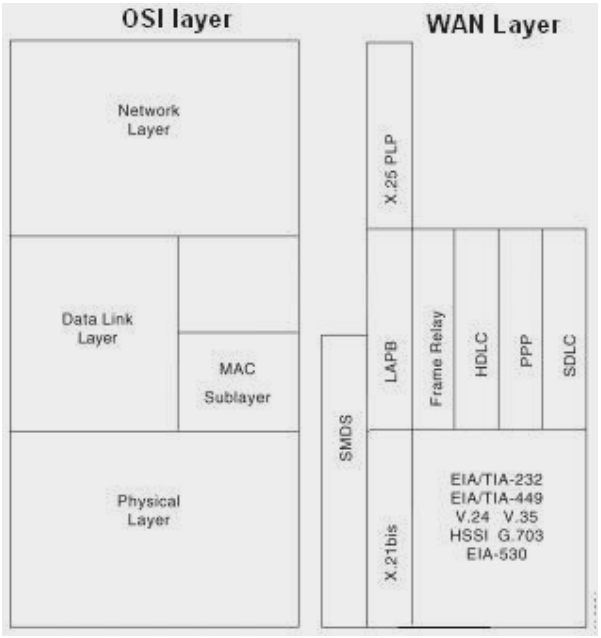
Do sự phức tạp trong việc xây dựng, quản lý, duy trì các đường truyền dẫn nên khi xây dựng mạng diện rộng WAN người ta thường sử dụng các đường truyền được thuê từ hạ tầng viễn thông công cộng, và từ các công ty viễn thông hay các nhà cung cấp dịch vụ truyền số liệu. Tùy theo cấu trúc của mạng những đường truyền đó thuộc cơ quan quản lý khác nhau như các nhà cung cấp đường truyền nội hạt, liên tỉnh, liên quốc gia, chẳng hạn ở Việt Nam là công ty Viễn thông liên tỉnh – VTN, công ty viễn thông quốc tế - VTI . Các đường truyền đó phải tuân thủ các quy định của chính phủ các khu vực có đường dây đi qua như: tốc độ, việc mã hóa.

Với WAN đường đi của thông tin có thể rất phức tạp do việc sử dụng các dịch vụ truyền dữ liệu khác nhau, của các nhà cung cấp dịch vụ khác nhau. Trong quá trình hoạt động các điểm nút có thể thay đổi đường đi của các thông tin khi phát hiện ra có trục trặc trên đường truyền hay khi phát hiện có quá nhiều thông tin cần truyền

giữa hai điểm nút nào đó. Trên WAN thông tin có thể có các con đường đi khác nhau, điều đó cho phép có thể sử dụng tối đa các năng lực của đường truyền và nâng cao điều kiện an toàn trong truyền dữ liệu.

Phần lớn các WAN hiện nay được phát triển cho việc truyền đồng thời trên đường truyền nhiều dạng thông tin khác nhau như: video, tiếng nói, dữ liệu...nhằm làm giảm chi phí dịch vụ.

Các công nghệ kết nối WAN thường liên quan đến 3 tầng đầu của mô hình ISO 7 tầng. Đó là tầng vật lý liên quan đến các chuẩn giao tiếp WAN, tầng data link liên quan đến các giao thức truyền thông của WAN, và một số giao thức WAN liên quan đến tầng mạng. Các quan hệ này được mô tả trong hình 3.1



Hình 3-1: Các chuẩn và giao thức WAN trong mô hình ISO 7 tầng

3.1.1.2 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 cập 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 viễn đàm, 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 cập từ xa dần trở thành một môi trường làm việc căn bản, 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 thuần 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 – Phục vụ(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-goverment) trong tương lai không xa.

3.1.1.3 Những điểm cần chú ý khi thiết kế WAN

Khi thiết kế WAN chúng ta cần chú ý đến ba yếu tố:

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 dải 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 hiên 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 công nghệ vệ tinh, vô tuyến,...

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

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

- Tính khả mở rộng thể hiện ở vấn đề có thể mở rộng, bổ sung thêm dịch vụ, tăng số lượng người dùng, tăng giải 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, khối hoá ở mức cao. Các khối, các mô đun của WAN độc lập một cách tương đối, quá trình triển khai có thể thực hiện theo từng khối, từng mô đun.
- Tính dễ phát hiện lỗi là một yêu cầu rất quan trọng, vì luồng thông tin vận chuyển trên WAN rất nhậy cảm cho các tổ chức dùng WAN. Vậy việc phát hiện và cô lập lỗi cần phải thực hiện dễ và nhanh đối 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 các 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.

An ninh-an toàn: việc đảm bảo an ninh, xây dựng chính sách an ninh,và thực hiện an ninh thế nào? ngay từ bước thiết kế.

3.1.2 Một số công nghệ kết nối cơ bản dùng cho WAN

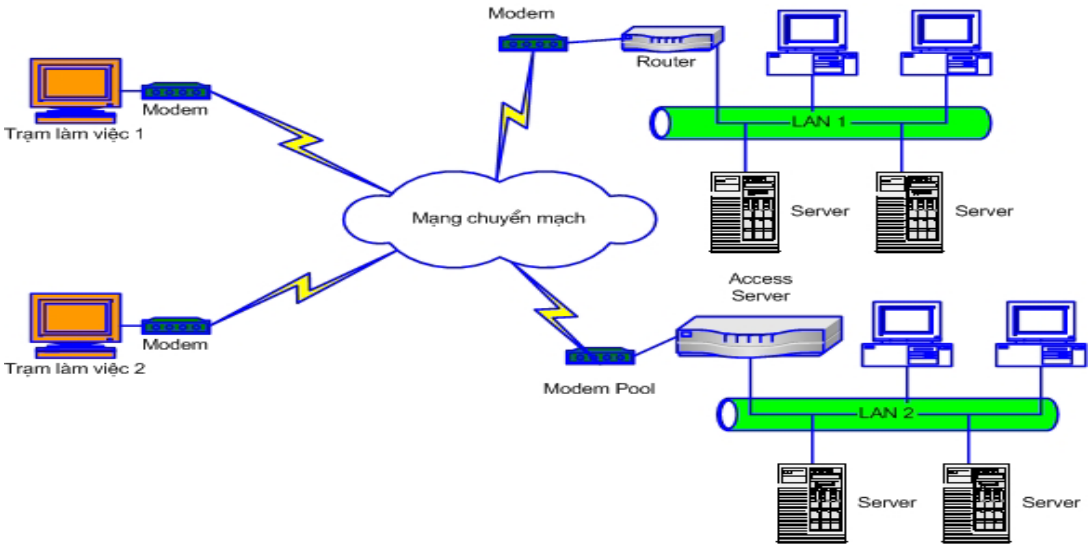
3.1.2.1 Mạng chuyển mạch (Circuit Swiching Network)

- **Giới thiệu**

Mạng chuyển mạch thực hiện việc liên kết giữa hai điểm nút qua một đường nối tạm thời hay giành riêng giữa điểm nút này và điêm 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 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 tao 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)

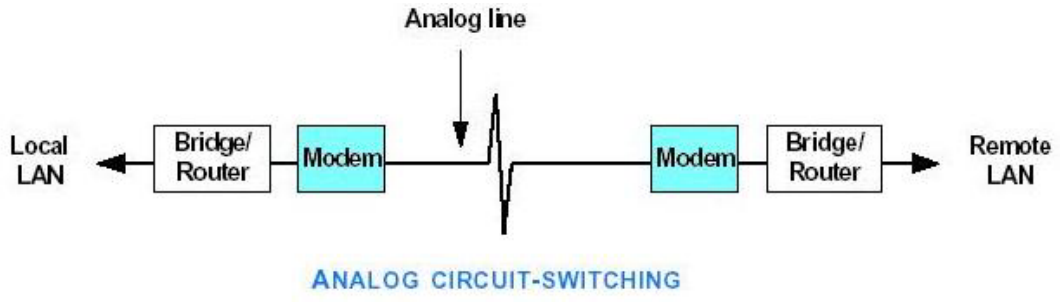


Hình 3-2: Mô hình kết nối WAN dùng mạng chuyển mạch

➢ Chuyển mạch tương tự (Analog)

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).



Hình 3-3: Mô hình kết nối WAN dùng mạng chuyển mạch tương tự

Kết nối PSTN

- Thiết bị:

  Dùng modem tương tự loại truyền không đồng bộ, hay truyền đồng bộ, để kết nối thiết bị mạng vào mạng điện thoại công cộng.
- Phương thức kết nối:

  Dùng kết nối PPP từ máy trạm hay từ thiết bị định tuyến qua modem, qua mạng điện thoại công cộng.

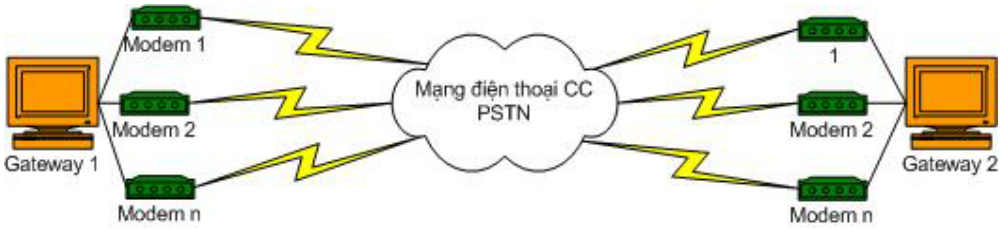
- Kết nối đơn tuyến- dùng 1 đường điện thoại.

Hình 3-4: Mô hình kết nối dùng một đường điện thoại

Các hạn chế khi dùng kết nối PSTN:

Các kết nối tương tự (analog) thực hiện trên mạng điện thoại công cộng và cước được tính theo phút. Đây là hình thức kết nối phổ biến nhất do tính đơn giản và tiện lợi của nó. Tuy nhiên chi phí cho nó tương đối cao cho các giao dịch liên tỉnh và chất lượng đường truyền không đảm bảo tính ổn định thấp, giải thông thấp, tốt đa 56Kbps cho 1 đường. Hình thức kết nối này chỉ phù hợp cho các chi nhánh nối tới Trung tâm mạng trong cùng một thành phố, đòi hỏi băng thông thấp và cho các người dùng di động, và cho các kết nối dùng không quá 4 giờ/ngày.

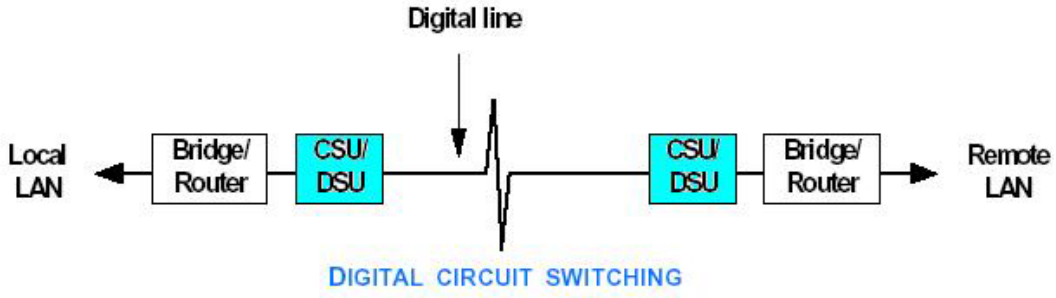
- Kết nối bó(multilink – đa tuyến)- dùng nhiều đường điện thoại.



Hình 3-5: Mô hình kết nối dùng nhiều đường điện thoại

Kết nối bó nhằm tăng dung lượng của đường truyền theo yêu cầu của dịch vụ (dial on demand)

- **Mạng chuyển mạch số (Digital)**



Hình 3-6: Mô hình kết nối WAN dùng mạng chuyển mạch số

Kết nối ISDN

- Giới thiệu

  Dịch vụ số ISDN - Intergrated Services Digital Network: ISDN là một loại mạng viễn thông số tích hợp đa dịch vụ cho phép sử dụng cùng một lúc nhiều dịch vụ trên cùng một đường dây điện thoại thông thường. Với cơ sở điện thoại cố định hạ tầng hiện có, ISDN là giải pháp cho phép truyền dẫn thoại, dữ liệu và hình ảnh tốc độ cao. Người dùng cùng một lúc có thể truy cập WAN và gọi điện thoại, fax mà chỉ cần một đường dây điện thoại duy nhất, thay vì 3 đường nếu dùng theo kiểu thông thường. Kết nối ISDN có tốc độ và chất lượng cao hơn hẳn dịch vụ kết nối theo kiểu quay số qua mạng điện thoại thường (PSTN). Tốc độ truy cập mạng WAN có thể lên đến 128 Kbps nếu sử dụng đường ISDN 2 kênh (2B+D) và tương đương 2.048 Mbps nếu sử dụng ISDN 30 kênh (30B+D).

- Các thiết bị dùng cho kết nối ISDN

  ISDN Adapter: Kết nối với máy tính thông qua các giao tiếp PCI, RS-232, USB, PCMCIA và cho phép máy tính kết nối với mạng WAN thông qua mạng đa dịch vụ tích hợp ISDN với tốc độ 128Kbps ổn định đa dịch vụ và

cao hơn hẳn so với các kết nối tương tự truyền thống mà tốc độ tối đa lý thuyết là 56Kbps.

ISDN Router: Thiết bị này cho phép kết nối LAN vào WAN cho một số lượng không giới hạn người dùng. Thông qua giao tiếp ISDN BRI, thiết bị này còn có thể đóng vai trò như một bộ chuyển đổi địa chỉ mạng (Network Address Translation) hoặc một máy chủ truy nhập từ xa. Khả năng thiết lập kết nối LAN-to-LAN qua dịch vụ ISDN cho phép nối mạng giữa Văn phòng chính và Chi nhánh hết sức thuận tiện. Cổng kết nối Ethernet tốc độ 10/100Mbps cho phép kết nối dễ dàng với mạng LAN. Các tính năng Quay số theo yêu cầu (Dial-on-Demand) và Dải thông theo yêu cầu (Bandwidth-on-Demand) tự động tối ưu hoá các kết nối theo yêu cầu của người dùng trên mạng.

- Các đặc tính của ISDN

  ISDN được chia làm hai loại kênh khác nhau:

  Kênh dữ liệu (Data Channel), tên kỹ thuật là B channel, hoạt động ở tốc độ 64 Kbps.

  Kênh kiểm soát (Control Channel), tên kỹ thuật là D Channel, hoạt động ở 16 Kbps (Basic rate) và 64 Kbps (Primary rate)

  Dữ liệu của người dùng sẽ được truyền trên các B channel, và dữ liệu tín hiệu (signaling data) được truyền qua D channel. Bất kể một kết nối ISDN có bao nhiêu B channel, nó chỉ có duy nhất một D channel. Đường ISDN truyền thống có hai tốc độ cơ bản là residential basic rate và commercial primary rate. Một vài công ty điện thoại không có đường truyền và thiết bị đầu cuối thích hợp cho dịch vụ tốc độ cơ bản nên họ cung cấp một tốc độ cơ bản cố định, có giá trị trong khoảng từ 64 Kbps đến 56 Kbps. Những biến thể này hoạt động như một B channel riêng biệt.

  Basic rate ISDN hoạt động với hai B channel 64 Kbps và một D channel 16 Kbps qua đường điện thoại thông thường, cung cấp băng thông dữ liệu là 128 Kbps. Tốc độ cơ bản được cung cấp phổ biến ở hầu hết các vùng ở Mỹ và châu Âu, với giá gần bằng với điện thoại thường ở một số vùng. (ở Đức, đường ISDN hoạt động với tốc độ cơ bản, với hai B channel 64 Kbps và một D channel 16 Kbps).

  Primary rate hoạt động với hai mươi ba B channel 64 Kbps và một D channel 64 Kbps qua một đường T1, cung cấp băng thông 1472 Kbps.

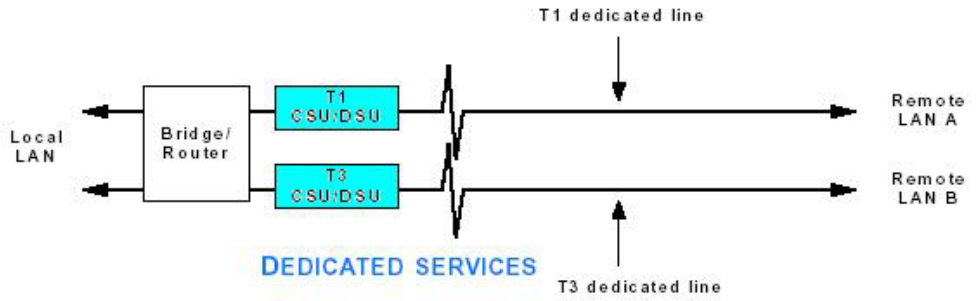
Primary rate đưa ra đường truyền quay số tốc độ cao, cần thiết cho các tổ chức lớn.

Đôi khi ISDN adaptor bị gọi là "ISDN modem" vì nó có chức năng quay số và trả lời cuộc gọi trên đường dây digital, như modem thực hiện trên đường dây analog. Tuy nhiên, ISDN adaptor không phải là modem vì không thực hiện chức năng modulation/demodulation và việc chuyển đổi tín hiệu giữa digital và analog (digital/analog conversion).

- Đánh giá khi dùng kết nối ISDN

  ISDN gồm hai kiểu BRI và PRI, đều đắt hơn điện thoại thông thường nhưng băng thông cao hơn. Hiện tại tốc độ cao nhất có thể cung cấp tại Việt Nam là 128 Kbps. Đây là hình thức kết nối mạng liên tỉnh tương đối rẻ so với các loại khác. Tuy nhiên nó đòi hỏi tổng đài điện thoại phải hỗ trợ kết nối ISDN (Cần phải khảo sát trước).

Mạng kênh thuê riêng (Leased lines Network)

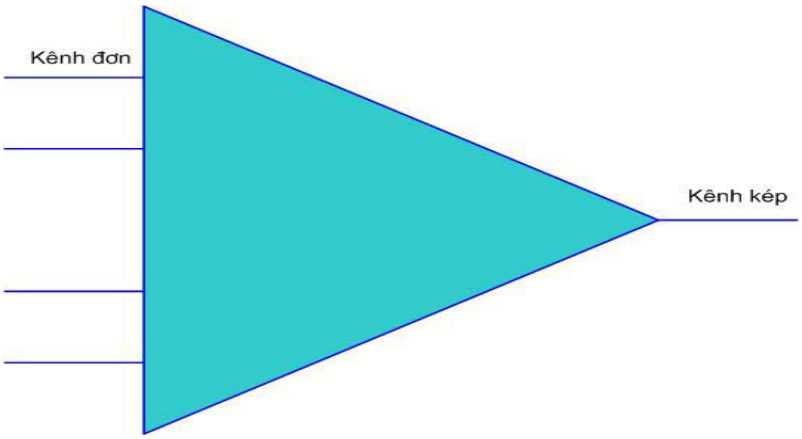


Hình 3-7: Mô hình kết nối WAN dùng các kênh thuê riêng

- Giới thiệu

  Cách kết nối phổ biến nhất hiện nay giữa hai điểm có khoảng cách lớn vẫn là Leased Line (tạm gọi là đường thuê bao).

  Với kỹ thuật chuyển mạch giữa các nút của mạng (tương tự hoặc số) có một số lượng lớn đường dây truyền dữ liệu, với mỗi đường dây trong một thời điểm chỉ có nhiều nhất một phiên giao dịch, khi số lượng các trạm sử dụng tăng cao người ta nhận thấy việc sử dụng mạng chuyển mạch trở nên không kinh tế. Để giảm bớt số lượng các đường dây kết nối giữa các nút mạng người ta đưa ra một kỹ thuật gọi là ghép kênh.



Hình 3-8: Mô hình ghép kênh

Mô hình đó được mô tả như sau: tại một nút người ta tập hợp các tín hiệu trên của nhiều người sử dụng ghép lại để truyền trên một kênh nối duy nhất đến các nút khác, tại nút cuối người ta phân kênh ghép ra thành các kênh riêng biệt và truyền tới các người nhận.

Có hai phương thức ghép kênh chính là ghép kênh theo tần số và ghép kênh theo thời gian, hai phương thức này tương ứng với mạng thuê bao tuần tự và mạng thuê bao kỹ thuật số. trong thời gian hiện nay mạng thuê bao kỹ thuật số sử dụng kỹ thuật ghép kênh theo thời gian với đường truyền T đang được sử dụng ngày một rộng rãi và dần dần thay thế mạng thuê bao tuần tự.

- Phương thức ghép kênh theo tần số:

  Để sử dụng phương thức ghép kênh theo tần số giữa các nút của mạng được liên kết bởi đường truyền băng tần rộng. Băng tần này được chia thành nhiều kênh con được phân biệt bởi tần số khác nhau. Khi truyền dử liệu, mỗi kênh truyền từ người sử dụng đến nút sẽ được chuyển thành một kênh con với tần số xác định và được truyền thông qua bộ ghép kênh đến nút cuối và tại đây nó được tách ra thành kênh riêng biệt để truyền tới người nhận. Theo các chuẩn của CCITT có các phương thức ghép kênh cho phép ghép 12, 60, 300 kênh đơn.

  Người ta có thể dùng đường thuê bao tuần tự (Analog) nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất. Khi máy của người sử dụng gửi dữ liệu thì kênh dữ liệu được ghép với các kênh khác và truyền trên đường truyền tới nút đích và được phân ra thành kênh riêng biệt trước khi gửi tới máy của người sử dụng. Đường nối giữa máy trạm của người sử dụng tới nút mạng thuê bao cũng giống như mạng chuyển mạch tuần tự sử

dụng đường dây điện thoại với các kỹ thuật chuyển đổi tín hiệu như V22, V22 bis, V32, V32 bis, các kỹ thuật nén V42 bis, MNP class 5.

- Phương thức ghép kênh theo thời gian:

  Khác với phương thức ghép kênh theo tần số, phương thức ghép kênh theo thời gian chia một chu kỳ thời gian hoạt động của đường truyền trục thành nhiều khoảng nhỏ và mỗi kênh tuyền dữ liệu được một khoảng. Sau khi ghép kênh lại thành một kênh chung dữ liệu được truyền đi tương tự như phương thức ghép kênh theo tần số. Người ta dùng đường thuê bao là đường truyền kỹ thuật số nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất.

  Hệ thống mang tín hiệu T-carrier được dùng ở Bắc mỹ từ 1962, dùng chế độ phân chia thời gian (Time Division Multiplexing - TDM) để cung cấp tín hiệu thoại qua các đường truyền số. Nó được thiết kế hoạt động trên hệ thống cáp đồng, các đường này cũng được dùng dể truyền số liệu hay các tín hiệu video. Tại mỗi đầu cuối trước khi nối vào thiết bị của khách hàng, phải sử dụng một thiết bị đầu cuối là CSU/DSU (Channel Service Unit/Data Service Unit - CSU/DSU) để mã hoá dữ liệu truyền. Thông thường thiết bị của khách hàng là các bộ chuyển kênh(multiplexer) hay một cầu(LAN bridge) dùng cho việc chuyển mạch với T-carrier. Nó có thể mang tín hiệu giọng nói dưới dạng mã số, khi đó băng thông sử dụng là 64 Kbps, giá trị này được xác định theo định luật Nyquist và điều biến theo mã xung Pulse Code Modulation - PCM.

  Theo định luật Nyquist tín hiệu giọng nói phải được lấy 8000 mẫu trên giây. Dùng điều biến PCM yêu cầu mỗi mẫu phải biểu diễn bằng giá trị 8-bit.

$$8000\ \frac{\text{mẫu}}{\text{giây}} \times 8\ \frac{\text{bit}}{\text{mẫu}} = 64000\ \frac{\text{bit}}{\text{giây}} = 64\ \text{Kbps}$$

  Tốc độ 64 Kbps được xác định như một kênh truyền ký hiệu là DS-0 (Digital Signal level 0) cho hệ thống T-carrier. Mỗi kênh DS-0 được dùng cho một kênh thoại.

  Khi dùng hệ thống T-carrier cho truyền số, mỗi khung dữ liệu là 193 bit, 8000 mẫu trên giây ta có:

$$193\ \frac{\text{bit}}{\text{khung}} \times 8000\ \frac{\text{khung}}{\text{giây}} = 1544000\ \frac{\text{bit}}{\text{giây}} = 1.544\ \text{Mbps}$$

Tốc độ 1.544 Mbps được gọi là kênh T-1, nó bằng 24 kênh DS-0, được ký hiệu là DS-1 (DigitalSignal level 1).

Hiện nay người ta có các đường truyền thuê bao như sau :

Leased Line được phân làm hai lớp chính là Tx (theo chuẩn của Mỹ và Canada) và Ex (theo chuẩn của châu Ấu, Nam Mỹ và Mehicô), 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.

Loại kênh	Thông lượng	Ghép kênh
T0	56 Kbps	1 đường thoại
T1	1.544 Mbps	24 đường T0
T2	6.312 Mbps	4 đường T1
T3	44.736 Mbps	28 đường T1
T4	274.176 Mbps	168 đường T1

T0/E0 là tương đương với một kênh truyền thoại đơn lẻ, T0 hoạt động ở tốc độ 56 Kbps và E0 hoạt động ở tốc độ 64 Kbps. Sở dĩ có sự khác biệt về tốc độ là vì các hệ thống viễn thông ở Bắc Mỹ dùng giao thức truyền tín hiệu cũ hơn, đảm bảo tạo ra chế độ sử dụng luân phiên 8 bit. Các máy biến đổi cảm ứng điện từ (Magnetic inductance transformer) trên công tắc chuyển mạch điện thoại (phone switch) cũ sẽ không khóa cứng (block) các công tắc chuyển mạch luân phiên (alternating switch) hiện nay. Còn chuẩn của châu Ấu sử dụng 8 bit để truyền tải thông tin do hệ thống chuyển mạch ở đây không dùng máy biến đổi cảm ứng. T0 và E0 tạo nền tảng cho các dịch vụ truyền số liệu tốc độ cao hơn vì các đường điện thoại tầm xa (Telephone trunk line - Thực ra trong ngành viễn thông, khái niệm mối kết nối được chia làm 3 loại tách biệt là trunk, channel và line, nhưng do phạm vi của bài viết và vấn đề thuật ngữ khi dịch ra tiếng Việt, chúng tôi không bàn sâu về sự khác biệt của 3 khái niệm này, và sẽ có đôi chỗ dùng chung các khái niệm) đều có thể truyền cuộc thoại được số hóa (digitized voice conversation). Tất cả các công ty điện thoại đều tối ưu hóa đường truyền của họ cho dịch vụ truyền thoại (voice service).

Bên cạnh việc phân chia trực tiếp các mức độ khác nhau của dịch vụ E/T, có nhiều đường truyền cung cấp dịch vụ phân chia nhỏ hơn, cho phép người dùng đặt thuê một số lượng bất kỳ các kênh (channel) T0 trong một đường

truyền T1 (tất nhiên số channel T0 đặt thuê phải nhỏ hơn hoặc bằng số channel T0 có trong một đường T1), hoặc đặt thuê các channel T1 trong một đường truyền T3 (số channel T1 đặt thuê phải nhỏ hơn hoặc bằng số channel T0 có trong một đường T3). Ví dụ nếu người dùng chỉ cần (hoặc chỉ đủ tiền để trả) một đường truyền khoảng 336 Kbps, họ có thể thuê 6 channel T0 của một đường truyền T1. Trong điều kiện đó, CSU/DSU (Channel Service Unit/Digital Service Unit) của người dùng phải có khả năng hỗ trợ các kênh phân chia (fractional channel). Khi đó công ty điện thoại sẽ tính tiền một phần của đường truyền T1 cho việc phân chia một phần thông lượng đường truyền mà người dùng sử dụng. Điều này thường được gọi là committed information rate. Các đường leased line được gắn vào cổng tuần tự (serial port) của máy tính hoặc router thông qua một CSU/DSU.

Các công nghệ xDSL

- Giới thiệu

  Việc kết nối WAN được thực hiện đầu tiên dùng modem tương tự qua mạng điện thoại, đến nay phương thức này chỉ dừng lại ở tốc độ truyền tải rất thấp, tối đa là 56kbps/line , điều này đã được cha đẻ của ngành lý thuyết thông tin Claude Shannon đã đưa ra giới hạn dung lượng cho kênh truyền có nhiễu là 35 kbps và thực tế đã đạt được 33.6kbps. Hạn chế của kênh truyền điện thoại với tốc tộ thông tin truyền số liệu do đôi dây cáp đồng như người ta nghĩ mà là khi qua mạch mã hóa PCM (Pulse Code Modulation) dãy tần truyền dẫn chỉ cho qua các tín hiệu từ 300hz đến 400hz. Sau này Modem X2 của hãng US Robotics và modem của hãng Rockwell được thống nhất bởi tiêu chuẩn V90 của ITU-T (liên minh viễn thông quốc tế) nhằm mục đích lách khỏi mạch lọc này trong chiều từ ISP về đến người sử dụng (downtream) đạt được tốc độ 56kbps nhưng tốc độ chiều từ người dùng lên ISP (uptream) vẫn là 33.6kbps và đây là tốc độ cao nhất có thể đạt được của modem. Đến nay cải tiến thành chuẩn V92 thực hiện kết nối nhanh hơn. Không đạt được tốc độ như đường T1: 1544kbps hay E1: 2048 kbps.

  Để vược qua ngưỡng tốc độ người ta chuyển sang dùng kỹ thuật số xDSL.

  Trên đường dây điện thoại thì thực tế chỉ dùng một khoảng tần số rất nhỏ từ 0KHz đến 20KHz để truyền dữ liệu âm thanh (điện thoại). Công nghệ DSL

tận dụng đặc điểm này để truyền dữ liệu trên cùng đường dây, nhưng ở tần số 25.875 KHz đến 1.104 MHz .

HDSL (High-speed DSL) là đường truyền thuê bao kỹ thuật số tốc độ cao, đạt 1,544-2,048 Mbps và cần dùng tới 2 hoặc 3 đường cáp đôi.

SDSL (Symmtric DSL) tương tự như HDSL, nhưng chỉ sử dụng một đường cáp và dung lượng truyền dữ liệu hai chiều bằng nhau, đạt khoảng 1,544-2,048 Mbps.

IDSL (Intergrated Service Digital Network DSL) là mạng tích hợp dịch vụ số, có tốc độ download và upload như nhau, đạt 128 Kbps.

RADSL (Rate Adaptive DSL) điều chỉnh tốc độ truyền theo chất lượng tín hiệu. Tốc độ download từ 640 Kbps tới 2,2 Mbps và upload từ 272 Kbps tới 1,088 Mbps.

CDSL (Consumer DSL) là một phiên bản của DSL, tốc độ download khoảng 1 Mbps và tốc độ upload thì thấp hơn.

UDSL (Unidirectional DSL) là một phiên bản dự kiến sắp đưa ra của một công ty ở châu Âu, tương tự như HDSL.

DSL Lite (còn gọi là G-Lite) có tốc độ đạt 1,544-6 Mbps.

ADSL (asymmetrical DSL) là đường truyền thuê bao kỹ thuật số không đối xứng, tốc độ download đạt 1,544-8 Mbps, upload đạt 16-640 Kbps.

VDSL (Very-high-bit-rate DSL) là đường truyền thuê bao kỹ thuật số tốc độ rất cao. Hiện nay, VDSL là hình thức DSL đạt tốc độ cao nhất với tốc độ download có thể đạt 12,9-52,8 Mbps và upload 1,5-2,3 Mbps.

G.SHDSL(Single pair High bit-rate DSL) là tiêu chuẩn quốc tế mới về truyền dẫn trên đôi cáp đơn, DSL tốc độ cao, được đưa ra trong tiêu chuẩn G.991.2 của ITU-T. Không giống như DSL không đối xứng, được thiết kế cho các ứng dụng ở khu vực mà băng tần đường xuống lớn hơn băng tần đường lên. G.SHDSL là chuẩn đối xứng cho phép truyền với tốc độ 2,3Mbit/s cho cả hai hướng. Do đó GSHDSL thích hợp hơn cho các ứng dụng thương mại đòi hỏi băng thông tốc độ cao cả hai hướng. G.SHDSL tích hợp được cả các tính năng tin cậy của cáp đồng hiện hành và truyền thông tốc độ cao mang lại hiệu quả: nâng cao tốc độ dữ liệu, cự ly dài hơn và ít tạp âm hơn.

Các dịch vụ kênh riêng, frame relay và Internet tại Bắc Mỹ ngày nay chủ yếu sử dụng tốc độ 1,544Mbit/s. Kỹ thuật mã hoá luồng T1 chuyển từ

phương pháp mã hoá AMI/B8ZS sang DSL tốc độ cao (HDSL) từ những năm 1990. Luồng T1 sử dụng mã AMI/B8ZS sử dụng hai đôi cáp (4 dây) với cự ly bị giới hạn, do đó đòi hỏi những bộ lặp trong phạm vi từ 3000-6000 feet (xấp xỉ 1-2km) tuỳ thuộc vào lưu lượng.

Trong khi đó để mua, lắp đặt và bảo dưỡng các bộ lặp T1 là khá đắt. HDSL đưa ra phương pháp điều chế mới mã cơ số 2 và mã cơ số 4 (2 binary 1 quaternary) cho đường truyền T1 do đó cự ly truyền dẫn được nâng lên tới 9000 feet (3km) mà không cần bộ lặp. Vì thế các công ty điện thoại Bắc Mỹ đã nhanh chóng chuyển sang HDSL để tiết kiệm chi phí.

Tại châu Âu và các nước khác, các ứng dụng thương mại chủ yếu tại tốc độ E1 2,048Mbit/s. Châu Âu cũng muốn nắm ưu thế của DSL mang lại, tiêu chuẩn đã được Liên minh Viễn thông quốc tế ITU công nhận, tính năng kỹ thuật của G.SHDSL cho phép mở rộng băng tần và giảm nhiễu.

Ngày nay, các đường dây DSL ở Mỹ chủ yếu là DSL không đối xứng (ADSL), kỹ thuật này chỉ truyền số liệu ở tốc độ 384kbit/s với các dịch vụ đối xứng. Các công ty điện thoại vừa và nhỏ ở Bắc Mỹ đang chuyển sang ứng dụng G.SHDSL cho các dịch vụ Internet, cho phép truyền số liệu với tốc độ là 786kbit/s, 1,544Mbit/s và 2,3Mbit/s, cho phép giảm cấp dịch vụ (service-level) ngang với các dịch vụ T1 hoặc E1 với mức cước hàng tháng thấp hơn.

Có 4 yếu tố cho làm cho G.SHDSL được quan tâm là:

Một là được tiêu chuẩn hoá: Nhu cầu của nền công nghiệp đòi hỏi tốc độ truyền dẫn số cao hơn cho ứng dụng thương mại. HDSL không bao giờ được chấp nhận như một tiêu chuẩn quốc tế. DSL đối xứng được đưa ra kinh doanh vào cuối những năm 1990 nhưng chưa bao giờ trở thành tiêu chuẩn và gây trở ngại cho dịch vụ ADSL vì nó không tương thích với phổ của ADSL (rất nhiễu). G.SHDSL được đưa ra để triển khai Internet và các ứng dụng cơ sở hạ tầng T1/E1 bởi vì nó là tiêu chuẩn được quốc tế hoá.

Hai là tốc độ dữ liệu được cải thiện: Chuẩn G.SHDSL cho phép tốc độ truyền dẫn lên tới 2,3Mbit/s (2 dây) và 4,6Mbit/s (4 dây) trong khi HDSL ban đầu chỉ cho phép tốc độ 1,544Mbit/s với 4 dây. G.SHDSL cung cấp tốc độ nhanh xấp xỉ 3 lần, và khi so sánh với các dịch vụ HDSL2 và HDSL4 (1,544Mbit/s qua hai dây hoặc 4 dây), và sử dụng băng tần hiệu quả hơn.

Ba là cự ly truyền dẫn được cải thiện: cự ly truyền dẫn của GSHDSL xa hơn HDSL từ 20% đến 30% tại cùng tốc độ truyền dẫn. Ngoài ra khi kỹ thuật đa liên kết được sử dụng, G.SHDSL cho phép truyền xa gấp hai lần HDSL

Bốn là băng phổ tương thích: GSHDSL có phổ tần tương thích với ADSL, do đó giảm can nhiễu và xuyên âm giữa các sợi cáp. Do đó các dịch vụ G.SHDSL có thể dùng chung với ADSL trên cùng một đôi cáp mà không có bất kỳ can nhiễu nào.

Vì những lý do trên mà G.SHDSL nhanh chóng trở nên phổ biến ở châu Âu và Bắc Mỹ.

- **ADSL(Asymmetric Digital Subscriber Line):** đường thuê bao kỹ thuật số không đối xứng là một công nghệ mới nhất cung cấp kết nối tới các thuê bao qua đường cáp điện thoại với tốc độ cao cho phép người sử dụng kết nối internet 24/24 mà không ảnh hưởng đến việc sử dụng điện thoại và fax. Công nghệ này tận dụng hạ tầng cáp đồng điện thoại hiện thời để cung cấp kết nối, truyền dữ liệu số tốc độ cao. ASDL là một chuẩn được Viện tiêu chuẩn quốc gia Hoa Kỳ thông qua năm 1993 và gần đây đã được Liên minh viễn thông quốc tế ITU công nhận và phát triển.

  ADSL hoạt động như thế nào?

  ADSL hoạt động trên đôi cáp đồng điện thoại truyền thống, tín hiệu được truyền bởi 2 modem chuyên dụng, một modem phía người dùng và 1 modem phía nhà cung cấp dịch vụ kết nối. Các modem này hoạt động trên dải tần số ngoài phạm vi sử dụng của các cuộc gọi thoại trên cáp đồng và có thể cho phép tốc độ truyền dữ liệu cao hơn nhiều so với các modem 56k hiện nay.

  Một thiết bị lọc (Spliter) đóng vai trò tách tín hiệu điện thoại và tín hiệu dữ liệu (data), thiết bị này được lắp đặt tại cả phía người sử dụng và phía nhà cung cấp kết nối. Tín hiệu điện thoại và tín hiệu DSL được lọc và tách riêng biệt cho phép người dùng cùng 1 lúc có thể nhận và gửi dữ liệu DSL mà không hề làm gián đoạn các cuộc gọi thoại. ADLS tận dụng tối đa khả năng của cáp đồng điện thoại nhưng vẫn không làm hạn chế dịch vụ điện thoại thông thường.

Spliter tạo nên 3 kênh thông tin: một kênh tải dữ liệu xuống tốc độ cao, một kênh đẩy ngược dữ liệu với tốc độ trung bình và 1 kênh cho dịch vụ điện thoại thông thường. Để đảm bảo dịch vụ điện thoại thông thường vẫn được duy trì khi tín hiệu ADSL bị gián đoạn, kênh tín hiệu thoại được tách riêng khỏi modem kỹ thuật số bởi các thiết bị lọc.

Những ưu điểm của ADSL:

- Tốc độ truy nhập cao: Tốc độ Download: 1,5 - 8 Mbps. Nhanh hơn Modem dial-up 56Kbps 140 lần. Nhanh hơn truy nhập ISDN 128Kbps 60 lần. Tốc độ Upload: 64-640 Kbps.
- Tối ưu cho truy nhập Internet. Tốc độ chiều xuống cao hơn nhiều lần so với tốc độ chiều lên. Vừa truy nhập Internet, vừa sử dụng điện thoại. Tín hiệu truyền độc lập so với tín hiệu thoại/Fax đo đó cho phép vừa truy nhập Internet, vừa sử dụng điện thoại.
- Kết nối liên tục: Liên tục giữ kết nối (Always on) Không tín hiệu bận, không thời gian chờ.
- Không phải quay số truy nhập: Không phải thực hiện vào mạng/ra mạng. Không phải trả cước điện thoại nội hạt.
- Cước phí tuỳ vào chính sách của ISP: Thông thường cấu trúc cước theo lưu lượng sử dụng, dùng bao nhiêu, trả tiền bấy nhiêu.
- Thiết bị đầu cuối rẻ. 100 - 150 USD cho một máy đơn lẻ. 400- 500 USD cho một mạng LAN (10-15 máy).

Nhược điểm:

- Sự phụ thuộc của tốc độ vào khoảng cách từ nhà thuê bao đến nơi đặt tổng đài ADSL (DSLAM). Khoảng cách càng dài thì tốc độ đạt được càng thấp. Nếu khoảng cách trên 5Km thì tốc độ sẽ xuống dưới 1Mbps. Tuy nhiên, hiện tại hầu hết các tổng đài vệ tinh của nhà cung cấp (nơi sẽ đặt các DSLAM) chỉ cách các thuê bao trong phạm vi dưới 2km. Như vậy, sự ảnh hưởng của khoảng cách tới tốc độ sẽ không còn là vấn đề lớn.
- Trong thời gian đầu cung cấp dịch vụ, nhà cung cấp dịch vụ sẽ không thể đầu tư các DSLAM tại tất cả các tổng đài điện thoại vệ tinh (chi phí rất lớn) vì vậy một số khách hàng có nhu cầu không

được đáp ứng do chưa đặt được DSLAM tới tổng đài điện thoại vệ tinh gần nhà thuê bao. Như vậy, trong thời gian đầu cung cấp dịch vụ, dịch vụ sẽ chỉ được triển khai tại các thành phố lớn, các khu vực tập trung nhiều khách hàng tiềm năng. Tuy nhiên, khi số lượng khách hàng tăng thì sẽ tăng cường số lượng DSLAM để phục vụ khách hàng.

- ADSL dùng kỹ thuật ghép kênh phân tầng rời rạc DMT, tận dụng cả 3: tần số, biên độ, pha của tín hiệu sóng mang để truyền tải dữ liệu.

Quá trình điều chế:

Input Data --> Serial to Parallel Input Data Buffer --> DMT Symbol Encoder --> Invert Fast Fourier Transform (IFFT) --> A/D Tranceiver(Analog to Digital) --> Line Filter --> Output Data.

Dữ liệu vào sẽ qua bộ đệm dữ liệu, tại đây sẽ tiến hành lấy N mẫu và đưa ra N đường song song, chuyển đến bộ mã hoá DMT.

Bộ mã hóa DMT tiến hành ghép N mẫu với tần số sóng mang fi, tín hiệu đã điều chế này theo N kênh song song đến bộ biến đổi fourier ngược IFFT. Bộ IFFT thực hiện ghép các sóng đã điều chế f1,f2,..fN thành f0 sao cho f1,f2,..fN là các hài của f0. f0 lúc này là tín hiệu thực sự và duy nhất đi vào bộ biến đổi analog-->digital(A/D).

Bộ A/D thực hiện biến đổi tín hiệu tương tự sang tín hiệu số để phù hợp với đường truyền.

Tín hiệu ra đến bộ lọc đường truyền để giới hạn băng thông(bandwidth), loại bỏ nhiễu(noise) --> output data.

Quá trình giải điều chế: ngược lại:

Input Data --> Line Filter --> D/A (Digital to Analog) --> Fast Fourier Transform (FFT) --> DMT Symbol Encoder --> Parallel to Serial Data Buffer --> Output Data

Căn bản về công nghệ ADSL

ADSL là một thành viên của họ công nghệ kết nối modem tốc độ cao hay còn gọi là DSL, viết tắt của Digital Subscriber Line.

DSL tận dụng hệ thống cáp điện thoại bằng đồng có sẵn để truyền tải dữ liệu ở tốc độ cao, tiết kiệm kinh phí lắp đặt cáp quang (fibre-optic) đắt tiền

hơn. Tất cả các dạng DSL hoạt động dựa trên thực tế là truyền âm thanh qua đường cáp điện thoại đồng chỉ chiếm một phần băng thông rất nhỏ. DSL tách băng thông trên đường cáp điện thoại thành hai: một phần nhỏ dành cho truyền âm, phần lớn dành cho truyền tải dữ liệu ở tốc độ cao.

- Đánh giá các công nghệ xDSL

Loại DSL	Tên đầy đủ	Download	Upload	Khoảng cách *	Số đường điện thoại cần	Hỗ trợ điện thoại **
ADSL	Asymetric DSL	8Mbps	800Kbps	5500m	1	Có
HDSL	High bit-rate DSL	1.54Mbps	1.54Mbps	3650m	2	Không
IDSL	Intergrated Service Digital Network DSL	144Kbps	144Kbps	10700m	1	Không
MSDSL	Multirate Symetric DSL	2Mbps	2Mbps	8800m	1	Không
RADSL	Rate Adaptive DSL	7Mbps	1Mbps	5500m	1	Có
SDSL	Symetric DSL	2.3Mbps	2.3Mbps	6700m	1	Không
VDSL	Veryhigh bit-rate DSL	52Mbps	16Mbps	1200m	1	Có

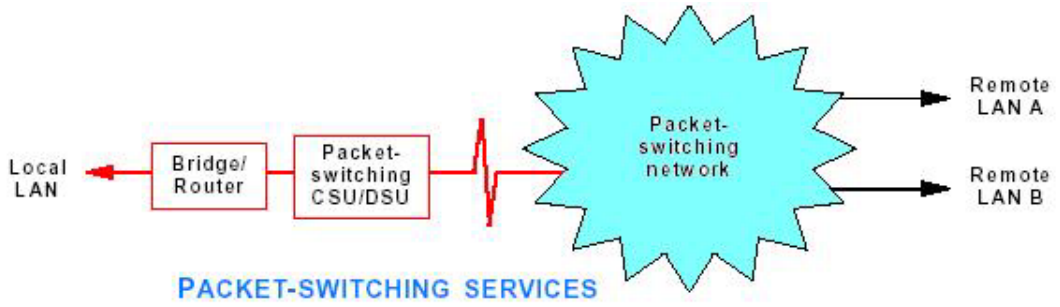
* Khoảng cách cáp từ thuê bao đến tổng đài, nếu nằm trong khoảng cách này thì có thể dùng công nghệ xDSL.

** Khả năng dùng điện thoại bình thường khi xDSL đang hoạt động trên đường cáp.

Phần này chúng tôi đề cập chủ yếu về công nghệ ADSL, là công nghệ mới đang được dùng phổ biến . Đặc biệt là đối với các doanh nghiệp thương mại điện tử và nền công nghiệp thông tin là nền tảng tương lai của mọi nền kinh tế. ADSL nói riêng và broadband Internet nói chung khiến thương mại điện tử trở nên khả thi. Các cửa hàng trên mạng có thể được thiết kế với tính tương tác cao hơn, cách trình bày sản phẩm hấp dẫn hơn với người dùng.

Loại cửa hàng này dễ thiết kế, dễ bảo quản, giá thành rẻ, kết hợp với khả năng tương tác trực tiếp với người dùng sẽ giúp cho doanh nghiệp nhỏ có thể cạnh tranh với các cơ sở lớn hơn trên quy mô toàn cầu. Nền công nghệ phần mềm của Việtnam sẽ đạt tính cạnh tranh cao hơn với Internet băng thông rộng. Việc phát triển, thăm dò và xâm nhập thị trường cũng như nhận đơn đặt hàng và giao sản phẩm sẽ trở nên dễ dàng hơn và kinh tế hơn rất nhiều.

3.1.2.2 Mạng chuyển gói (Packet Switching Network)



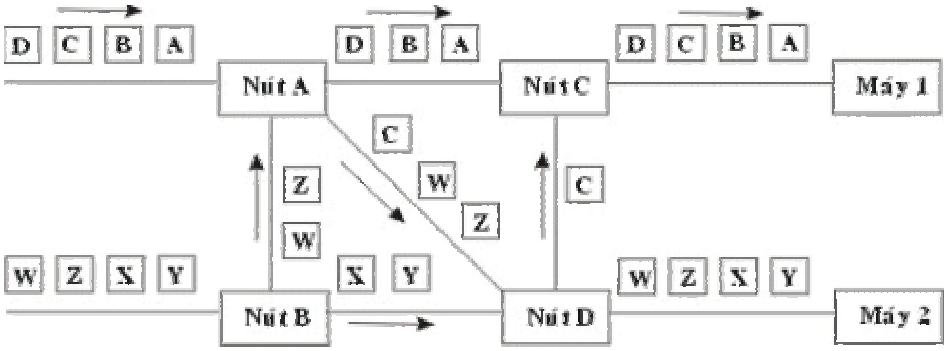
Hình 3-9: Mô hình kết nối WAN dùng chuyển mạch gói

Mạng chuyển mạch gói 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.

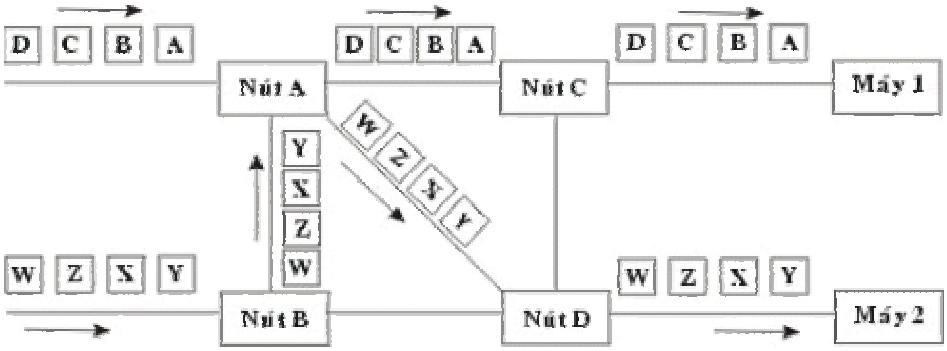
Với phương thức chuyển mạch gói theo sơ đồ rời rạc các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ nơi gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xem đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin 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 3-10: Ví dụ phương thức sơ đồ rời rạc

- **Phương thức chuyển mạch gói theo đường đi xác định:**

Trước khi truyền dữ liệu một đường đi (hay còn gọi là đường đi ảo) được thiết lập giữa trạm gửi và trạm nhận thông qua các nút của mạng. Đường đi trên mang số hiệu phân biệt với các đường đi khác, sau đó các gói tin được gửi đi theo đường đã thiết lập để tới đích, các gói tin mang số hiệu củ 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 3-11: Ví dụ phương thức đường đi xác định

- **Kết nối dùng ATM**

  - 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 Mbps. 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 chanell) khác

nhau, mỗi kênh ảo được sử dụng bởi một ứng dụng nào đó tại một thời điểm.

ATM đã kết hợp những đặc tính tốt nhất của dạng chuyển mạch liên tục và dạng chuyển mạch gói, nó có thể kết hợp dải thông linh hoạt và khả năng chuyển tiếp cao tốc và có khả năng quản lý đồng thời dữ liệu số, tiếng nói, hình ành 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 dáp 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 tắt nghẽn thấp, hổ 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 tố 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, bằng con đường của chính nó đi qua bộ chuyển mạch bằng cách cho mỗi trạm cuối băng thông chỉ định. Băng thông rộng được chỉ định của ATM với đặc tính có thể xác nhận khiến nó trở thành một kỹ thuật tuyệt hảo dùng cho bất kỳ nơi nào trong mạng cục bộ của doanh nghiệp.

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

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

một số sản phẩm đó như DEC 900 Multiwitch, IBM 8250 hub, Cisco 7000 rounter, Cablectron, ATM module for MMAC hub.

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

- 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.

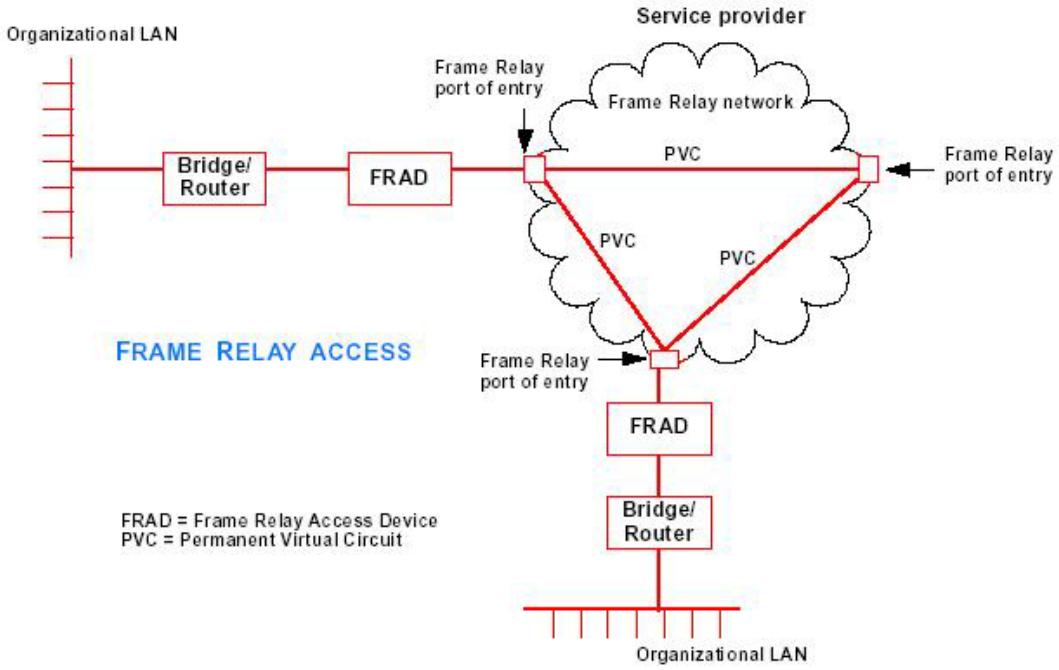
- Đánh giá khi dùng kế nối ATM

  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 hoá, 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.

➢ **Kết nối dùng mạng Frame Relay**



Hình 3-12: Mô hình kết nối WAN dùng mạng Frame relay

- Giới thiệu về mạng Frame Relay

  Frame relay - mạng chuyển mạch khung:

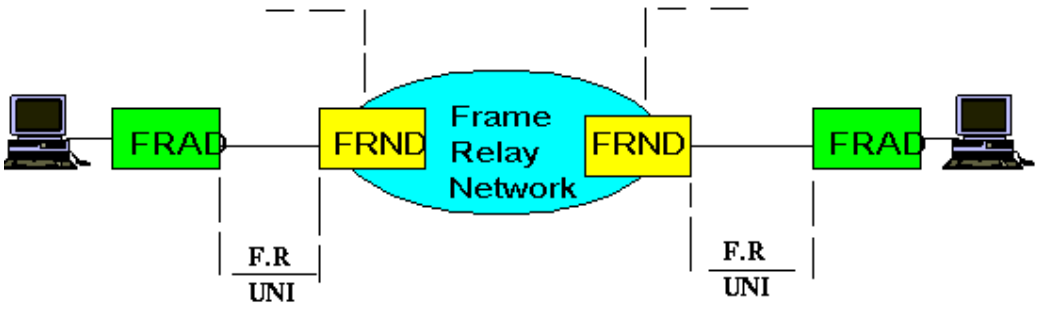
  Bước sang thập kỷ 80 và đầu thập kỷ 90, công nghệ truyền thông có những bước tiến nhảy vọt đặc biệt là chế tạo và sử dụng cáp quang vào mạng truyền dẫn tạo nên chất lượng thông tin rất cao. Việc xử dụng thủ tục hỏi đáp X25 để thực hiện truyền số liệu trên mạng cáp quang luôn đạt được chất lượng rất cao, 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 chuyển 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

  Cơ sở để tạo được mạng Frame relay là:

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

Đường nối giữa các thiết bị và mạng trục Frame Relay, mô tả trong hình vẽ dưới đây.



Hình 3-13: 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 trục 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 network, Frame Relay không dùng thủ tục gì cả (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 (Bandwith) cho từng cuộc gọi một mà phân phối bandwith 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 kb, khi họ chuyển đi một lượng thông tin quá lớn, Frame Relay cho phép truyền chúng ở tốc độ cao hơn 64 kb. 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 data.

Cũng như X25, 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.

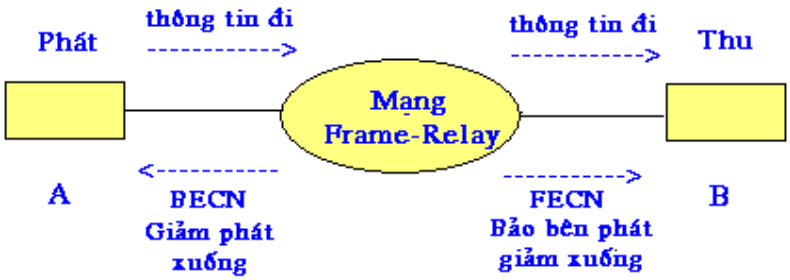
Về lý mà nói nếu chuyển các Frame vượt quá tốc độ cam kết, thì những Frame đó sẽ bị loại bỏ và bit DE được sử dụng. Tuy nhiên có thể chuyển các frame đi với tốc độ lớn hơn CIR hay thậm chí hơn cả CBIR tuỳ thuộc vào trạng thái của mạng Frame relay lúc đó có độ nghẽn ít hay nhiều (Thực chất của khả năng 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.



Hình 3-14: Nguyên lý sử dụng FECN và BECN

Sử dụng LMI (Local Manegment 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 kế 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 Communacation 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, kênh 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 (Integrated Service Digital Network) 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 chuyển khung (Frame-Relay) rồi mạng truyền dẫn không đồng bộ ATM (Asynchronous Transfer Mode) 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%
- Hội thảo video: 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 (trafic bursty) mà ở các công nghệ cũ hơn như chuyển mạch kênh hay chuyển mạch gói không thể tạo ra.

- **Kết nối dùng dịch vụ chuyển mạch tốc độ cao (SMDS)**

- Giới thiệu

  SMDS (Switched Multimegabit Data Service) mạng chuyển mạch tốc độ cực cao. Giống như mạng frame relay, nó cung cấp các kênh ảo(virtual channels) với tốc độ thấp nhất là T1(gần 1.5 Mbps) đến tốc độ T3(gần 45 Mbps).

  SMDS dùng phương pháp truy nhập mạng và giao diện theo chuẩn IEEE 802.6. khoảng cách kết nối tối đa là 160 kilô mét(100 dặm Anh).

  SMDS dùng công nghệ tế bào kích thước cố định gần như ATM, nó thường cung cấp dịch vụ dùng tốc độ cao trên T-1, hay T-3 thường là 4, 10, 16, 25 and 34 Mbps.

  Mạng trục SMDS có tốc độ DS-3 (45 Mbps), OC-3 (155 Mbps) hỗ trợ tốc độ truyền SONET, và OC-12 (622 Mbps).

  Dùng SMDS rất có lợi cho các ứng dụng đòi hỏi tốc độ cao như truyền ảnh, thiết kế trợ giúp bằng máy tính(computer-aided design -CAD),xuất bản, và cácứng dụng về tài chính .

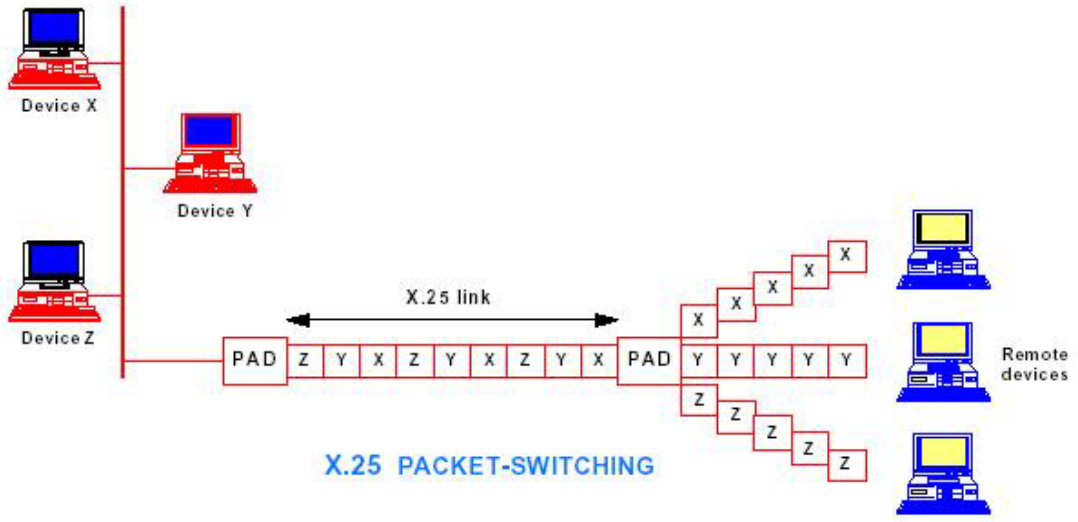
  SMDS phù hợp với các tổ chức có các đặc trưng sau:

  - Có nhiều địa điểm phân tán về mặt địa lý, tại mỗi địa địa điểm đều có LAN
  - Cần trao đổi thông tin ở tốc độ cực cao.
  - Chấp nhận dùng truyền số liệu qua mạng dịch vụ công cộng.

- Đánh giá khi dùng kế nối SMDS

  Việc dùng mạng SMDS để kết nối WAN chỉ giành cho các IXP lớn.

➢ Kết nối dùng chuẩn X.25



Hình 3-15: hình kết nối WAN dùng mạng X25

- Giới thiệu

  Mạng X25 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:

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

  Trong X25 có chức năng dồn kênh (multiplexing) đối với liên kết logic (virtual circuits) chỉ làm nhiệm vụ kiểm soát lỗi cho các frame đi qua. Điều này làm tăng độ phức tạp trong việc phối hợp các thủ tục giữa hai tầng kề nhau, dẫn đến thông lượng bị hạn chế do tổng phí xử lý mỗi gói tin tăng lên. X25 kiểm tra lỗi tại mỗi nút trước khi truyền tiếp, điều này làm 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 X25 nhanh chóng trở thành lạc hậu.

- Đánh giá khi dùng kế nối X.25

  Hiện nay không còn phù hợp với công nghệ truyền số liệu.

3.1.2.3 Kết nối WAN dùng VPN

➢ **Giới thiệu tổng quan về VPN**

VPN (Virtual Private Network) là một mạng riêng được xây dựng trên nền tảng hạ tầng mạng công cộng (như là mạng Internet). Mạng IP riêng (VPN) là một dịch vụ mạng có thể dùng cho các ứng dụng khác nhau, cho phép việc trao đổi thông tin một cách an toàn với nhiều lựa chọn kết nối. Dịch vụ này cho phép các tổ chức xây dựng hệ thống mạng WAN riêng có quy mô lớn tại Việt Nam.

Giải pháp VPN cho phép người sử dụng làm việc tại nhà hoặc đang đi công tác ở xa có thể thực hiện một kết nối tới trụ sở chính của mình, bằng việc sử dụng hạ tầng mạng thông qua việc tạo lập một kết nối nội hạt tới một ISP. Khi đó, một kết nối VPN sẽ được thiết lập giữa người dùng với mạng trung tâm của họ.

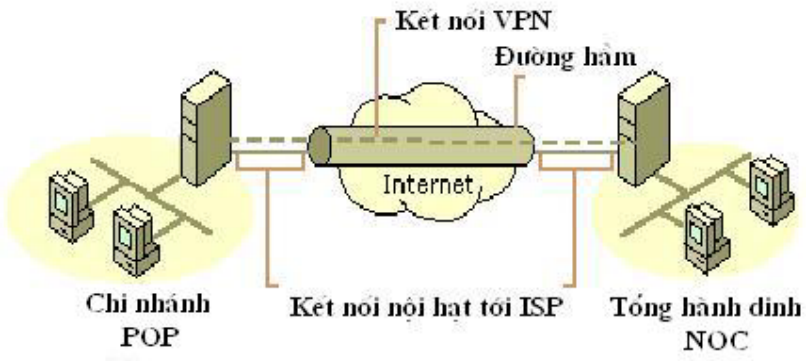
Kết nối VPN cũng cho phép các tổ chức kết nối liên mạng giữa các NOC của họ đặt tại các địa điểm khác nhau thông qua các kết nối trực tiếp (Leased line) từ các địa điểm đó tới một ISP. Điều đó giúp giảm chi phí gọi đường dài qua dial-up và chi phí thuê đường Leased line cho khoảng cách xa. Dữ liệu chuyển đi được đảm bảo an toàn vì các gói dữ liệu truyền thông trên mạng đã được mã hoá.

➢ **Một số giải pháp kỹ thuật hay dùng trong kết nối VPN**

- IPSec
- PPTP
- L2TP

➢ **Một số mô hình WAN dùng VPN**

- DùngVPN kết nối POP về NOC



Hình 3-16: Mô hình WAN dùng VPN nối POP với NOC

- Dùng VPN truy nhập về POP hay NOC

➢ **Một vài nhận xét khi sử dụng VPN trong kết nối WAN.**

Hạn chế khi VPN dùng công nghệ IPSec là làm giảm hiệu năng của mạng vì trước khi gửi gói tin đi. đầu tiên, gói tin được mã hóa, sau đó đóng gói vào các gói IP, hoạt động này tiêu tốn thời gian và gây trễ cho gói tin. Tiếp theo gói tin mới được đưa vào trong mạng của nhà cung cấp dịch vụ.

Các VPN gateway phải tương thích khi chúng kết nối với nhau.

Đường hầm VPN được tạo ra trong không gian mạng không đồng nhất do đó rất khó đảm bảo chất lượng dịch vụ.

3.1.3 Giao thức kết nối WAN cơ bản trong mạng TCP/IP.

3.1.3.1 Giao thức PPP

Giao thức PPP(*Point-to-Point Protocol) là giao thức dùng để đóng gói dữ liệu cho truyền thông điểm điểm*. PPP là một chuẩn để gán và quản lý địa chỉ IP, đóng gói dị bộ(asynchronous start/stop), đồng bộ định hướng bít(bit-oriented synchronous), giao thức mạng phân kênh(network protocol multiplexing), cấu hình kết nối(link configuration), kiểm tra chất lượng kết nối(link quality testing),phát hiện lỗi(error detection), bao gồm cả giao thức kiểm soát tầng kết nối LCP(Link Control Protocol) và giao thức kiểm soát tầng mạng NCP(Network Control Protocols) phục vụ cho việc lựa chọn địa chỉ tầng liên kết, việc nén dữ liệu truyền, cũng như xác định các cấu hình tham số cho tầng liên kết. PPP hỗ trợ trong nhiều bộ giao thức khác nhau như: bộ giao thức Intranet/Internet IP, bộ giao thức IPX - Novell's Internetwork Packet Exchange, bộ giao thức DECnet,...

➢ **Các thành phần của PPP**

PPP cung cấp phương pháp để truyền các khung dữ liệu(datagrams) trên các liên kết tuần tự điểm - điểm(serial point-to-point links). PPP có 3 thành phần chính:

- HDLC - Phương pháp đóng gói các khung dữ liệu trên các liên kết điểm - điểm.. PPP dùng giao thức HDLC(High-Level Data Link Control protocol) là cơ sở cho việc đóng gói này
- LCP - để lập cấu hình và kiểm tra kết nối - data link connection.
- NCP - để lập cấu hình các giao thức tầng mạng(network layer protocols). PPP được thiết kế dùng cho nhiều bộ giao thức mạng khác nhau.

➢ **Nguyên tắc làm việc của PPP**

- Giới thiệu

Để lập kết nối qua liên kết PPP, đầu tiên PPP gửi khung LCP để cấu hình và kiểm tra liên kết dữ liệu(data link). Sau đó liên kết được lập, PPP gửi khung NCP để chọn và cấu hình các giao thức tầng mạng(network layer).

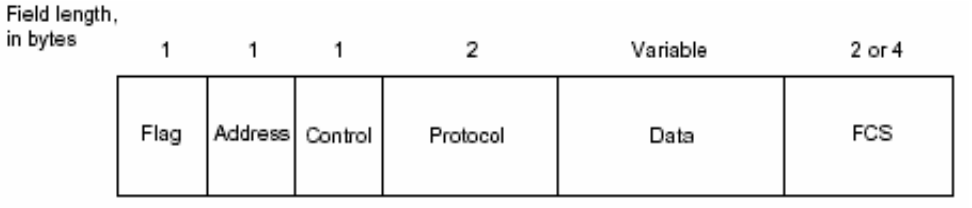
- Yêu cầu của tầng vật lý

  PPP có khả năng làm việc với nhiều loại giao diện DTE/DCE,chẳng hạn như EIA/TIA-232-C (RS-232-C cũ), EIA/TIA-422 (RS-422 cũ), EIA/TIA-423 (RS-423 cũ), V.35. Yên cầu tuyệt đối của PPP là mạch song công (duplex circuit), hoặc mạch chuyên dụng(dedicated), hay chuyển mạch (switched), Các mạch này có thể làm việc ở chế độ tuần tự bit dị bộ (asynchronous) hay đồng bộ (synchronous bit-serial mode), trong suốt với các khung PPP tầng liên kết (link layer). PPP không bắt buộc một hạn chế gì về tốc độ truyền trên DTE/DCE interface.

- Yêu cầu của tầng PPP link

  PPP dùng các nguyên tắc, thuật ngữ, cấu trúc khung của ISO(the International Organization for Standardization) HDLC thủ tục (ISO 3309-1979), được thay bằng ISO 3309:1984/PDAD1

  "Addendum 1: Start/Stop Transmission." ISO 3309-1979 xác định cấu trúc khung HDLC dùng cho môi trường đồng bộ. ISO 3309:1984/PDAD1 thay cho ISO 3309-1979 dùng cho môi trường dị bộ. Thủ tục điều khiển PPP dùng để xác định mã hoá trường điều khiển được chuẩn hoá trong ISO 4335-1979 and ISO 4335-1979/ Addendum 1-1979. Qui cách khung dữ liệu PPP gồm 6 trường được mô tả dưới đây:



Các trường trong khung PPP gồm:

- **Flag** - Trường cờ 1 byte xác định bắt đầu hay kết thúc của 1 khung, gồm một chuỗi nhị phân 01111110.
- **Address** - Trường địa chỉ 1 byte gồm một chuỗi nhị phân 11111111, địa chỉ broadcast chuẩn, PPP không gán địa chỉ trạm riêng.
- **Control** - Trường điều khiển 1 byte gồm một chuỗi nhị phân 00000011, mà nó điều khiển việc truyền các khung dữ liệu không tuần tự.

- **Protocol** - Trường giao thức 2 byte xác định giao thức đóng gói của khung.
- **Data** - có thể là 0 hoặc nhiều byte, giá trị mặc định là 1500 byte.
- **Frame check sequence (FCS)** - Chuỗi kiểm tra khung 16 bit (2 byte). Cho phép PPP phát hiện lỗi

- Giao thức điều khiển PPP link LCP

  PPP LCP cung cấp phương pháp lập, cấu hình, duy trì và kết thúc kết nối điểm-điểm(point-to-point).

  LCP trải qua 4 pha khác nhau:

  Pha đầu lập và cấu hình kết nối, trước khi truyền dữ liệu LCP mở kết nối để cấu hình, xác lập các tham số kết nối . Khi pha này kết thúc khung xác lập cấu hình đã được gửi và nhận, do đó cũng xác định luôn được chất lượng kết nối .

  Pha xác định chất lượng kết nối.

  Pha cấu hình tầng mạng NCP làm việc khi chất lượng kết nối xác nhận là đảm bảo

  Pha cuối là kết thúc, khi chất lượng kết nối không đảm bảo hay kết thúc truyền.

- PPP trong kết nối WAN

  Các kết nối WAN trong mạng IP, IPX hay DECnet đều dùng PPP.

3.1.4 Các thiết bị dùng cho kết nối WAN

3.1.4.1 Router (Bộ định tuyến)

Đã được trình bày trong mục 2.1.2.

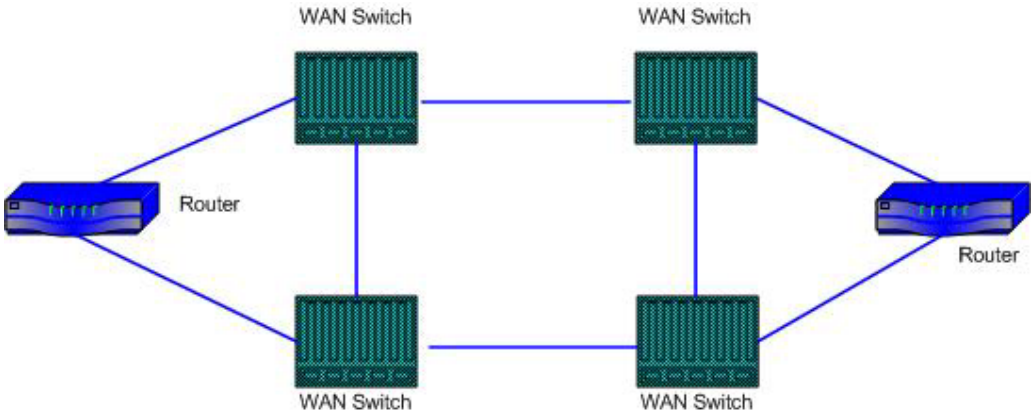
3.1.4.2 Chuyển mạch WAN

➢ **Khái niệm**

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 hoạ cho chuyển mạch WAN là mạng chuyển mạch số đa dịch vụ ISDN(Integrated Services Digital Network).

Thiết bị chuyển mạch WAN(WAN switch) là thiết bị nhiều cổng liên mạng (multiport internetworking device) dùng trong các mạng viễn thông như Frame Relay, X.25, và SMDS, nó hoạt động ở tầng data link. Chẳng hạn chuyển mạch WAN 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 3-17: Bộ chuyển mạch WAN

- **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.

3.1.4.3 Access Server

- **Khái niệm**

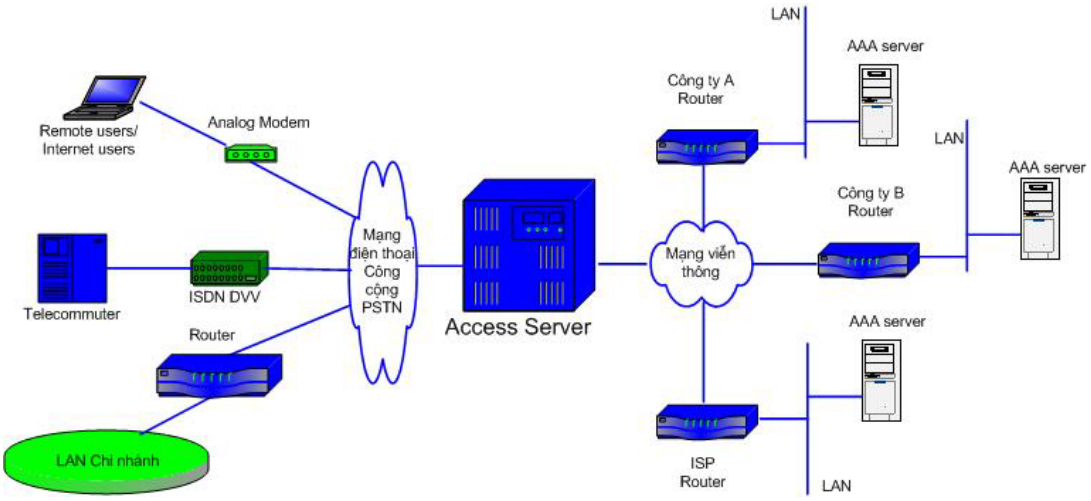
Access server là điểm tập trung cho phép kết nối WAN qua các mạng điện thoại công công cộng(PSTN), mạng đa dịch vụ số(ISDN), hay mạng dữ liệu công cộng (PDN).

Người dùng từ xa, hay mạng LAN xa qua modem nối vào một trong các mạng trên đều có thể truy nhập vào mạng của mình qua access server.

Access server có nhiều loại, và có thể phân nhiều cấp như có khả năng tích hợp nhiều modem trong cùng một thiết bị, có khả năng tích hợp nhiều trung kế, có khả năng ghép nhiều kênh truyền dẫn,...

Chẳng hạn thiết bị CVX 1800 của hãng Nortel có thể cung cấp 2688 modem trên một thiết bị do vậy có thể cùng lúc kết nối 2688 đường. Có giao tiếp WAN để làm nhiệm vụ chuyển mạch WAN khi kết nối với các mạng dữ liệu công cộng PDN. Kết nối với mạng điện thoại công cộng PSTN nó dùng giao tiếp DS1, DS3 hay E1. Kết nối với các tổng đài TANDEM nó có bộ chuyển mạch ghép kênh theo thời gian (TDMS - time division multiplexing switch).

Dùng linux box và 1 vỉ multiport cũng có thể tạo ra 1 access server dùng cho truy nhập qua mạng điện thoại công cộng.



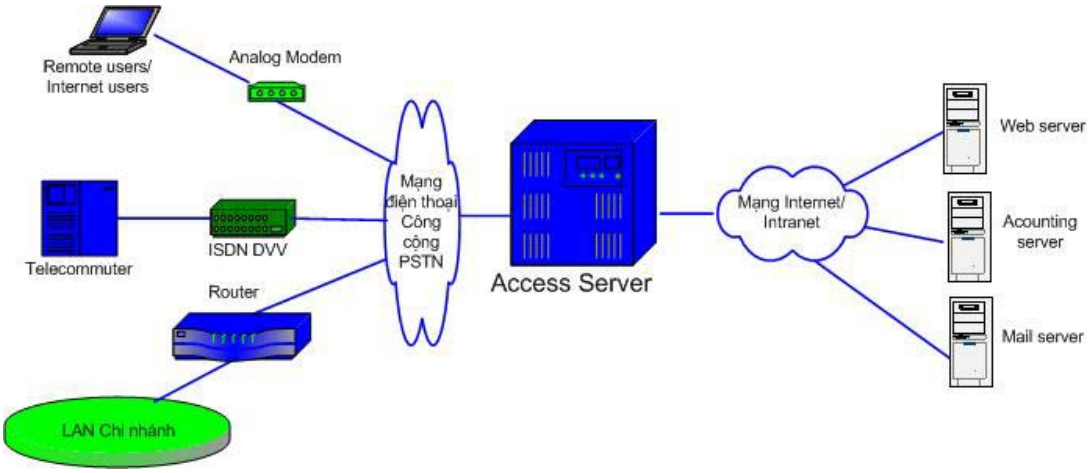
Hình 3-18: Access server hỗ trợ truy nhập tổng hợp

- **Hoạt động của Access Server**

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 có thể dùng các tài nguyên mạng đang kết nối với access server này, hay access server nay là một trạm chuyển tiếp để kết nối đi tiếp.

- **Lý do phải dùng Access Server:**

Kết nối WAN, truy nhập từ xa dùng access server là giải pháp đơn giản, tiết kiệm chi phí nhất.



Hình 3-19: Access server hỗ trợ truy nhập vào internet/intranet

3.1.4.4 Modem

Modem là từ ghép của MOdulator/DEModulator (Điều chế/giải điều chế), chuyển tín hiệu digital từ máy tính thành tín hiệu analog để có thể truyền qua, đường điện thoại. Còn modem ở đầu nhận thì chuyển tín hiệu analog trở lại thành tín hiệu digital cho máy tính tiếp nhận có thể hiểu được.

Modem truyền số liệu theo tốc độ chuẩn, biểu hiện bằng đơn vị bit truyền trong một giây (bits per second - bps) hoặc đo bằng bốt (baud rate). Về mặt kỹ thuật thì bps và baud khác nhau, nhưng việc dùng baud thay cho bps đã quá phổ biến nên hai đơn vị này có thể thay thế cho nhau.

Nếu xét về tốc độ thì càng nhanh càng tốt. Ví dụ truyền một file 300K qua modem có tốc độ là 2400 bps thì mất khoảng 22 phút, còn với modem 9600 bps chỉ mất 5,5 phút. Ưu thế về tốc độ càng thể hiện rõ khi truyền hoặc nhận thông tin khoảng cách xa. Tại Việt Nam, nhất là ở các thành phố lớn chất lượng đường truyền rất tốt nên thường đạt được tốc độ cao nhất upload là 33.6 Kbps, download là 56 Kbps.

Vào thời điểm hiện nay, modem có khá nhiều thương hiệu như Origo, Pine, Intel, Acorp, Vern, GVC, Creative, Prolink, Creative và US Robotics, phổ biến nhất là hai chuẩn V90 và V92.

Modem loại gắn trong (Internal) là một vỉ dùng để cắm vào một khe(slot) trong máy PC.

Loại dùng cho modem tích hợp trên mainboard, là bản mạch được thiết kế tích hợp luôn trên PC, do đó PC có cổng cắm line điện thoại vào.

Loại modem gắn ngoài (External) thông qua cổng COM hoặc USB khá phong phú về chủng loại, các thương hiệu có tiếng như US Robotics (56K, V90,Voice, dùng chip 3COM), Creative (USB, V90/92), Hayes Accura 56Kbps V92 - External (Com Port).

Modem loại PCMCIA (3COM, CNET, XIRCOM) dùng cho máy tính xách tay cắm qua cổng PCMCIA.

Theo kinh nghiệm sử dụng chất lượng các loại modem trong(internal) không đảm bảo, chỉ dùng được trong khoảng thời gian bảo hành (12 tháng), sau khi hết bảo hành vài tuần hay thậm chí sớm hơn là bắt đầu có trục trặc. Loại modem ngoài (Ext) chất lượng đảm bảo hơn, có khả năng kết nối với tốc độ cao, nhất là những loại modem của các hãng nổi tiếng như US Robotics, Creative (USB, V90/92), Hayes Accura 56Kbps V92.

- **Giới thiệu một số chuẩn phổ biến mà các modem đang dùng: V42, X2, K56Flex,V90 và chuẩn V92**
  - Chuẩn V90:

    Trước khi công nghệ V90 ra đời thì công nghệ K56Flex và x2 là hai công nghệ mà hai nhà sản xuất modem hàng đầu đưa ra. Công nghệ K56Flex là do công ty Lucent Technologies và Rockwell Semiconductor Systems phối

hợp. x2 là công nghệ do 3Com Coporation/US Robotics. Ngoài hai công nghệ K56Flex và x2 thì loại modem nào có hai chuẩn này thì có thể đạt được tốc độ kết nối nhanh hơn tốc độ 33.6Kbps. Modem sử dụng công nghệ K56Flex hoặc x2 không thể đạt được tốc độ tải nhanh từ những nhà cung cấp dịch vụ khi modem ta đang sử dụng một công nghệ khác ngoài K56Flex và x2. Điều này có nghĩa là nhà cung cấp dịch vụ mà ta kết nối vào cũng phải hỗ trợ chuẩn K56Flex và x2. V90 trước đây được biết dưới dạng V.pcm, nó là kỹ thuật điều chế xung. Sau này hai chuẩn này được thiết lập lại thành một chuẩn mà tất cả các modem khác có thể hiểu được và tương thích trên toàn cầu.

- Chuẩn V92:

  Sau khi cho ra đời chuẩn V90 được hai năm, tổ chức ITU-T cho ra đời chuẩn V92. Đây là thế hệ tiếp theo của modem tương tự. Chuẩn này sẽ được thông qua một chính thức từ năm 2000.

  Chuẩn V92 có thêm 3 chức năng so với chuẩn V90 như: kết nối nhanh, chúng ta chỉ cần một nửa thời gian so với trước để dial-up; nhớ được những cuộc điện thoại gọi đến, chức năng này cho phép nhận một cuộc điện thoại gọi đến trong khi modem đang sử dụng; khả năng điều chế xung ngược có thể đẩy mạnh liên kết ngược chiều lên tới 48kbit/s.

  Kết nối nhanh là một ưu điểm đặc biệt với người dùng, thời gian kết nối rút ngắn xuống còn 10 giây, điều này rất có ý nghĩa khi chuẩn V90cần tới 20 giây. Tính năng kết nối nhanh, duy trì các tham số đường truyền cho những điểm truy nhập chung, như là tỷ lệ tín hiệu và nhiễu, tần số xuất hiện câu trả lời để mà giảm đi được những thời gian thăm dò vì vậy tiết kiệm được thời gian. Công ty Conexant nói rằng sẽ nghiên cứu để giảm thời gian kết nối xuống còn 5 giây. Nhớ được những cuộc điện thoại gọi đến. Chức năng này có thể bảo vệ sự kết nối modem lên tới 16 phút, trong khoảng thời gian đó một cuộc điện thoại gọi đến sẽ được phát hiện khi modem đang được sử dụng. Chức năng này được dựa trên một phiên bản modem của hãng NTT với chức năng "Bắt cuộc gọi". Chức năng này được người dùng quan tâm nhiều, đặc biệt là ở Mỹ, ở đó trong toàn bộ thời gian kết nối thì có thể xảy ra những cuộc gọi với một tỷ lệ cố định, ở Nhật thì vấn đề này còn phụ thuộc vào các nhà cung cấp dịch vụ, và phần mềm chuyển đổi kỹ thuật số

đặc biệt phải được cài đặt bởi một hãng truyền thông. Liên kết ngược chiều lên tới 48kbit/s

Các cải tiến đã làm cho dữ liệu được truyền với tốc độ cao trên liên kết ngược chiều từ nhà tới tổng đài. Người ta sử dụng kỹ thuật giống như sự điều chế mã hoá xung (PCM) để cho tăng tốc độ từ 33.6 kbit/s trong modem 56k lên 48 kbit/s.

- Chuẩn V42:

  Giao thức V42 có thêm LAPM (Link Access Protocol) và MNP 1-4. Khi hai modem bắt tay ở chế độ V42 thì nó sử dụng giao thức LAPM để điều khiển những dữ liệu bị lỗi và sẽ yêu cầu modem phát truyền lại những khối dữ liệu bị lỗi. Nếu một trong hai modem hỗ trợ chuẩn V42 và modem còn lại chỉ hỗ trợ MNP thì modem kia sẽ thương lượng để sử dụng MNP. Cả hai trường hợp trên thì quá trình sửa lỗi trên đường truyền hoàn toàn tự động và không yêu cầu bất cứ phần mềm nào hay chuyên gia mới sử dụng được.

- Chuẩn V42BIS:

  Giao thức này sẽ sử dụng MNP Level 5 để tương xứng dữ liệu, điểm khác biệt là khối lượng dữ liệu được nén bao nhiêu. Giao thức V42 thường nén dữ liệu ở tỉ lệ 4:1 phụ thuộc vào loại tập tin được gửi. Những tập tin hay dữ liệu đã được nén sẵn như là PKZIP, GIF hay JPG thì tỉ lệ nén không biết sẽ được modem nén nữa hay không, nó sẽ phụ thuộc vào hệ thống nén của modem.

  NTU - Thiết bị kết cuối mạng (Network Terminal Unit) là thiết bị đặt tại các điểm kết cuối mạng, thực hiện chức năng kết nối tín hiệu và chuyển đổi giao diện giữa kênh truyền dẫn truy nhập mạng với thiết bị đầu cuối thuê bao.

3.1.4.5 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 thông 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

3.1.4.6 ISDN terminal Adaptor

Là thiết bị đầu cuối để kết nối PC hay LAN vào WAN qua mạng ISDN.

3.1.5 Đánh giá và so sánh một số công nghệ dùng cho kết nối WAN.

Với nhu cầu đòi hỏi ngày càng cao của xã hội nên vấn đề xem xét đánh giá kỹ thuật trong mạng là mối quan tâm hàng đầu của các nhà phân tích và thiết kế mạng. Chẳng hạn một yêu cầu phổ biến như làm thế nào để truy xuất thông tin một cách nhanh chóng và tối ưu nhất, trong khi việc xử lý thông tin trên mạng quá nhiều đôi khi có thể làm tắc nghẽn trên mạng và gây ra gián đoạn thông tin một cách đáng tiếc.

Hiện nay việc làm sao có được một hệ thống mạng chạy thật tốt, thật an toàn với chi phí hợp lý, và mang lại lợi ích kinh tế cao, đang rất được quan tâm. Một vấn đề đặt ra có rất nhiều giải pháp về công nghệ, mỗi giải pháp có rất nhiều yếu tố cấu thành, trong mỗi yếu tố có nhiều cách lựa chọn. Như vậy để đưa ra một giải pháp hoàn chỉnh, phù hợp thì phải trải qua một quá trình chọn lọc dựa trên những ưu điểm của từng yếu tố, từng chi tiết rất nhỏ. Trong thiết kế WAN thì công nghệ kết nối là vấn đề cơ bản nhất cần được xem xét, đánh giá và lựa chọn hợp lý.

Để giải quyết một vấn đề phải dựa trên những yêu cầu đặt ra và dựa trên công nghệ để giải quyết. Nhưng công nghệ cao nhất chưa chắc là công nghệ tốt nhất, mà công nghệ tốt nhất là công nghệ phù hợp nhất với yêu cầu đặt ra và điều kiện thực tế.

- **Kết nối PSTN(mạng điện thoại công cộng)**

Kết nối WAN qua mạng điện thoại công cộng có ưu điểm là đơn giản, dễ thực hiện, nhưng nhược điểm lớn nhất là hạn chế về tốc độ, và độ tin cậy thấp. Chỉ dùng hiệu quả cho các thuê bao có thời gian kết nối dưới 4 giờ/ngày.

- **Kết nối ISDN(mạng dịch vụ tổng hợp)**

Kết nối WAN qua mạng đa dịch vụ số ISDN có ưu điểm là ổn định hơn qua mạng điện thoại công cộng, nhưng lại chịu chi phí cao hơn, và là loại kết nối không phổ biến. Chi thực hiện được tại các địa phương mà tổng đài hỗ trợ dịch vụ ISDN.

- **Kết nối FRAME RELAY**

Hiện nay ở Việt nam, với một mạng lưới truyền dẫn chưa tốt đồng đều, các trục chính dùng cáp quang, còn lại nhiều phần vẫn dùng viba với các kênh dùng cho thoại là chính, ít có các kênh dùng cho truyền số liệu, chất lượng truyền dẫn chưa hoàn toàn tốt. Do vậy bưu điện chưa triển khai công nghệ Frame Relay trên toàn quốc, như trên đã trình bầy điều kiện tiên quyết để sử dụng Frame Relay là chất lượng mạng truyền dẫn phải cao. Tuy nhiên, ở nhữ nơi mà bưu điện đã triển khai

công nghệ Frame Relay thì việc xem xét chọn giải pháp kết nối WAN dùng Frame relay là hoàn toàn chấp nhận được, cần được xem xét và triển khai.

- **Kết nối sử dụng công nghệ xDSL**

Như phần lớn công nghệ khác, tiềm năng trên lý thuyết của công nghệ DSL có sự khác biệt đáng kể đối với tốc độ kết nối WAN cho các tổ chức và giới doanh nghiệp hiện nay. Đặc biệt, công nghệ VDSL có thể cung cấp tốc độ truy cập lên đến 52 Mbps tuy nhiên phần lớn các kết nối vẫn dùng tốc độ đường truyền thấp hơn nhiều ở 128 Kbps.

Các chuyên gia công nghệ cho biết đã có những hoàn thiện đáng kể trong chất lượng đường truyền theo công nghệ xDSL. Vì thế lượng khách hàng thuê bao sử dụng dịch vụ xDSL vẫn không ngừng tăng lên.

Việc kết nối sử dụng xDSL ở những doanh nghiệp từ khoảng 1999 là bước hậu thuẫn cho việc sử dụng công nghệ ADSL hiện nay (công nghệ DSL không đối xứng) với tốc độ truy cập từ 512 Kbps đến 8 Mbps.

Chuyên gia phân tích cấp cao của Gartner Dataquest ông Charles Carr nói tốc độ của công nghệ xDSL có khả năng thay đổi cao vì nhiều lý do kỹ thuật khác nhau như chất lượng đường truyền và khoảng cách giữa các văn phòng trung tâm. Dù công nghệ với tốc độ truy cập nhanh hơn bình thường có thể được triển khai tại một số khu vực nhưng phần lớn các doanh nghiệp và khách hàng sử dụng dịch vụ kết nối DSL là những người làm việc từ xa và cảm thấy hài lòng với tốc độ hiện hành.

Trong những năm tới công nghệ như VDSL có thể phân phối tốc độ kết nối hoàn thiện đáng kể từ 26 Mbps đến 52 Mbps. Ông Carr cũng chỉ ra rằng chỉ có Qwest là công ty duy nhất hiện nay có thể cung cấp công nghệ này. Ông cho biết so với tốc độ đạt được trên lý thuyết, công nghệ VDSL thực sẽ có tốc độ kết nối trung bình ở mức thấp gồm hai chữ số megabit.

Ngày nay công nghệ kết nối xDSL được xem là công nghệ có tốc độ truy cập nhanh hơn, rẻ hơn, và tin cậy, nó sẽ là lựa chọn đầu tiên của các nhà thiết kế WAN.

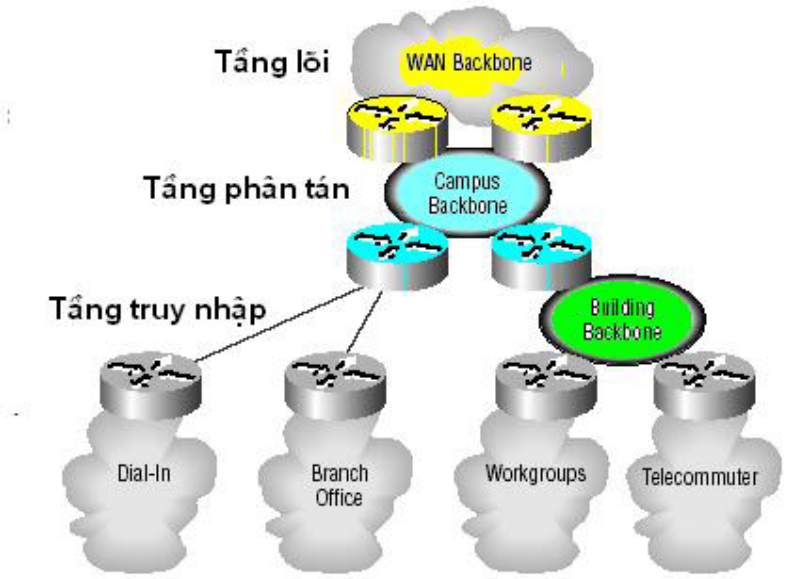
3.2 Thiết kế mạng WAN.

3.2.1 Các mô hình WAN

3.2.1.1 Mô hình phân cấp

- **Khái niệm mô hình phân cấp**

Mô hình phân cấp để hỗ trợ thiết kế WAN thường là mô hình phân cấp ba tầng: Tầng 1 là tầng lõi(xương sống của WAN – backbone), tầng 2 phân tán, tầng 3 là tầng truy nhập, gọi tắt là mô hình phân cấp phục vụ cho việc khảo sát và thiết kế WAN.



Hình 3-20: Mô hình phân cấp để hỗ trợ thiết kế WAN

Tầng lõi là phần kết nối mạng trục(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 nưa 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 kết 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.

- **Các tầng trong mô hình phân cấp**
  - Tầng lõi
  - Tầng phân tán
  - Tầng truy nhập

3.2.1.2 Các mô hình tôpô.

Mô hình tôpô (Topology) của WAN gọi tắt là mô hình tôpô thực chất là 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, và PC , Laptop,...

Các NOC, hay POP có thể là cac campus LAN, hay là một WAN.

Mô hình tôpô giúp các nhà thiết kế WAN thực hiện việc tổ chức khảo sát, phân tích và quản lý trong quá trình thiết kế, cũng như thi công hiệu quả.

Cấu trúc, địa phương hoá 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.

3.2.2 Các mô hình an ninh mạng.

3.2.2.1 An ninh-an toàn mạng là gì ?

Khái niệm: Theo một nghĩa rộng thì an ninh-an toàn mạng dùng riêng, hay mạng nội bộ là giữ không cho ai làm cái mà mạng nội bộ đó không muốn cho làm.

Vậy khi kết nối WAN phải triển khai cơ chế nào để thực hiện yêu cầu an ninh-an toàn, chúng ta gọi đó là cơ chế an ninh-an toàn mạng.

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 có, để cung ứng cho những người dùng mà nó cho phép, ...

Nhìn từ một phía khác thì vấn đề an ninh - an toàn 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 còn thể hiên 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). Chúng ta sẽ xem xét chi tiết:

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-an toàn.

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 3-21: 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.

Tin tặc tấn công mạng khi kết nối WAN thế nào?

Ở đây chúng ta cũng phải đề cập đến các hành động tin tặc khác nhau có thể gặp phải khi kết nối WAN, thử liệt kê một số loại hành động tin tặc sau:

Hành động thăm dò (probe), hành động quét (scan), hành động thử vào một tài khoản (account compromise), hành động thử vào làm quản trị hệ thống (root compromise), hành động thu lượm các gói tin (packet sniffer), hành động tấn công từ chối dịch vụ (denial of service), hành động khai thác quyền (exploitation of trust), hành động làm mã giả (malicious code),...

Hành động thăm dò (Probe).

Hành động thăm dò được đặc trưng bằng việc thử truy nhập từ xa vào một hệ thống hay sau khi vào được hệ thống thử tìm các thông tin của một hệ thống mà không được phép. Thăm dò thường là kết quả của sự tò mò hay sự nhầm lẫn khi truy nhập mạng. Hậu quả của sự thăm dò có khi rất lớn, nhất là khi truy nhập được vào mạng với quyền lớn, hay mò ra các thông tin quan trọng.

Hành động quét (Scan).

Hành động quét là việc dùng một công cụ tự động để thực hiện thăm dò tìm lỗ hổng an ninh của hệ thống với một số lượng lớn. Hành động quét đôi khi là kết quả của một lỗi hệ thống như hỏng hay mất cấu hình của một dịch vụ. Nhưng cũng có thể là giai đoạn đầu mà tin tặc dùng để tìm các lỗ hổng an ninh mạng chuẩn bị cho một cuộc tấn công. Quản trị hệ thống cũng có thể dùng phương pháp quét để phát hiện các điểm yếu về an ninh - an toàn trong hệ thống mạng của mình.

Hành động vào một tài khoản (Account Compromise).

Hành động vào một tài khoản là hành động dùng một tài khoản không được phép. Hành động này có thể gây mất dữ liệu quan trọng, hay là hành động dùng trộm dịch vụ, lấy cắp dữ liệu. Người dùng mạng bị tin tặc lấy cắp mật khẩu. Cách vào một máy tính dễ nhất là có được mật khẩu và vào máy bằng lệnh login; rào cản tin tặc đầu tiên là mật khẩu. Nếu mật khẩu bị mất, thì tin tặc có thể làm mọi thứ mà người dùng đó được phép.

Hành động vào quyền quản trị (Root Compromise).

Hành động vào quyền quản trị là hành động vào một tài khoản có quyền lớn nhất của hệ thống, do vậy có thể gây ra những hậu quả rất nghiêm trọng cho hệ thống. Từ việc thay đổi toàn bộ cấu hình của hệ thống, đến việc cài đặt các công cụ phá hoại, lấy cắp thông tin, cho đến việc tổ chức các cuộc tấn công lớn.

Hành động thu lượm các gói tin (Packet Sniffer).

Hành động thu lượm các gói tin là việc thực hiện chương trình bắt các gói dữ liệu đang truyền trên mạng do vậy bắt được cả thông tin người dùng, mật khẩu và cả các thông tin riêng tư ở dạng văn bản. Dựa vào các thông tin thu lượm được tin tặc có thể thực hiện tấn công hệ thống.

Hành động tấn công từ chối dịch vụ (Denial of Service).

Mục đích của hành động tấn công từ chối dịch vụ là ngăn cản không cho người dùng hợp pháp sử dụng dịch vụ. Tấn công từ chối dịch vụ có thể thực hiện bằng nhiều cách, như tạo tìm cách sử dụng bất hợp pháp tất cả các tài nguyên mạng như treo các kết nối, tạo luồng dữ liệu lớn, gây tắc nghẽn tại các cổng kết nối,...

Làm thế nào để đảm bảo an toàn-an ninh khi kết nối WAN?

Các vấn đề về an ninh-an toàn 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.

3.2.2.2 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 có thể ?
  - Xác định các công cụ để bảo đảm an ninh ?
  - Xây dựng mô hình an ninh-an toàn

Thường xuyên kiểm tra các bước trên, nâng cấp, cập nhật và vá hệ thống khi có một lỗ hổng an ninh - an toàn 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 khi kết nối và đưa WAN vào hoạt động.

Đầu tiên, mục đích và yêu cầu về an ninh-an toàn hệ thống ứng dụng phải được vạch ra rõ ràng. Chẳng hạn mục tiêu và yêu cầu an ninh-an toàn 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 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 một cách toàn cục. Có nghĩa là phải đảm bảo cả về phương tiện kỹ thuật và con người triển khai.

3.2.2.3 Một số công cụ triển khai mô hình an toàn-an ninh

➢ **Hệ thống tường lửa 3 phần(Three-Part Firewall System)**

- Tường lửa là gì?

  Tường lửa là một công cụ phục vụ cho việc thực hiện an ninh - an toàn mạng từ vòng ngoài, nhiệm vụ của nó như là hệ thống hàng rào vòng ngoài của cơ sở cần bảo vệ. Khi kết nối hai hay nhiều phần tử của WAN, chẳng hạn kết nối một NOC với với nhiều POP, khi đó nguy cơ mất an ninh tại các điển kết nối là rất lớn, tường lửa là công cụ được chọn đặt tại các điểm kết nối đó.

  Tường lửa trong tiếng Anh là Firewall, là ghép của 2 từ fireproof và wall nghĩa là ngăn không cho lửa cháy lan. Trong xây dựng, tường lửa được thiết kế để giữ không cho lửa lan từ phần này của toà nhà sang phần khác của toà nhà khi có hoả hoạn. Trong công nghệ mạng, tường lửa được xây dựng với mục đích tương tự, nó ngăn ngừa các hiểm hoạ từ phía cộng đồng các mạng công cộng hay mạng INTERNET, hay tấn công vào một mạng nội bộ (internal network) của một công ty, hay một tổ chức khi mạng này kết nối qua mạng công cộng, hay INTERNET.

- Chức năng của hệ thống tường lửa:

  Tường lửa đặt ở cổng vào/ra của mạng, kiểm soát việc truy nhập vào/ra mạng nội bộ để ngăn ngừa tấn công từ phía ngoài vào mạng nội bộ.

  Tường lửa phải kiểm tra, phát hiện, dò tìm dấu vết tất cả các dữ liệu đi qua nó để làm cơ sở cho các quyết định (cho phép, loại bỏ, xác thực, mã hoá, ghi nhật ký,..) kiểm soát các dịch vụ của mạng nó bảo vệ.

  Để đảm bảo mức độ an ninh - an toàn cao, tường lửa phải có khả năng truy nhập, phân tích và sử dụng các thông tin về truyền thông trong cả 7 tầng và các trạng thái của các phiên truyền thông và các ứng dụng. Tường lửa cũng phải có khả năng thao tác các các dữ liệu bằng các phép toán logic, số học nhằm thực hiện các yêu cầu về an ninh - an toàn. Tường lửa bao gồm các thành phần: các bộ lọc hay sàng lọc.

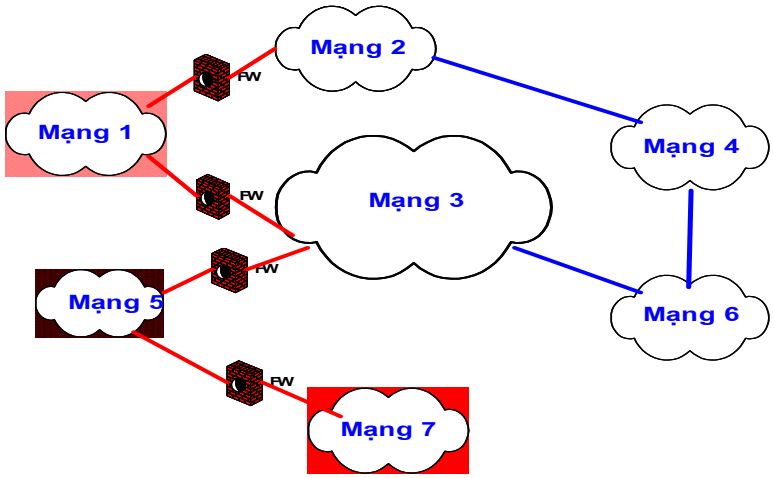
Hình 3-22: Mô hình logic của tường lửa

Tường lửa chính là cổng (gateway) vào/ra của một mạng nội bộ (mạng trong), trên đó có đặt 2 bộ lọc vào/ra để kiểm soát dữ liệu vào/ra mạng nội bộ.

Xác định vị trí đặt tường lửa trong hệ thống mạng hiện đại.

Theo truyền thống thì tường lửa được đặt tại vị trí vào/ra mạng nội bộ (mạng được bảo vệ) với mạng công cộng(mạng ngoài), hay mạng internet (internet, khi kết nối với internet).

Ngày nay trong một tổ chức khi kết nối WAN có thể kết nối đoạn mạng khác nhau, và do yêu cầu về an ninh - an toàn của các đoạn mạng đó khác nhau. Khi đó tường lửa sẽ được đặt ở vị trí vào/ra của các đoạn mạng cần bảo vệ. Dưới đây các đoạn mạng 1, 5, 7 cần bảo vệ.



Hình 3-23: Vị trí đặt tường lửa trên mạng

Dữ liệu vào/ra mạng nội bộ với mạng ngoài đều đi qua tường lửa, do đó tường lửa có thể kiểm soát và đảm bảo dữ liệu nào là có thể được chấp nhận (acceptable) cho phép vào/ra mạng nội bộ.

Về mặt logic thì tường lửa là bộ tách, bộ hạn chế và bộ phân tích. Tường lửa là điểm thắt(choke point). Cơ chế này bắt buộc những kẻ tấn công từ phía ngoài chỉ có thể thâm nhập vào hệ thống qua một kênh rất hẹp (nơi này thể giám sát và điều khiển được). Cơ chế này hoạt động cũng tương tự như các trạm thu phí giao thông đặt tại các đầu cầu, hay các điểm kiểm soát vé vào cổng ở một sân vận động. Tuy nhiên cơ chế này có một yếu điểm là nó không thể ngăn chặn được những kẻ tấn công xâm nhập vào hệ thống bằng cách đi vòng qua nó, hay tấn công từ bên trong.

Các mối đe dọa mà tường lửa có thể chống lại được là:

Chống lại các cuộc thâm nhập từ xa đến các nguồn thông tin khi không được phép.

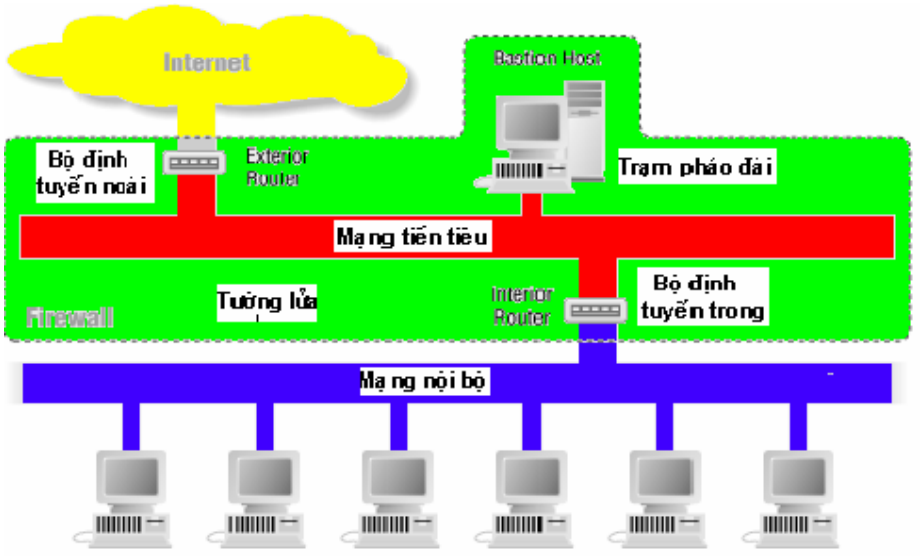
Từ chối các dịch vụ đưa thông tin từ mạng ngoài vào mạng nội bộ với mục đích làm rối loạn hệ thống.

Quản lý được truy nhập ra mạng ngoài, do đó cấm được truy nhập từ mạng nội bộ ra ngoài khi cần thiết.

Bằng cơ chế xác thực chống lại sự giả danh để truy nhập mạng từ mạng ngoài vào.

Ngoài ra tường lửa còn có khả năng trợ giúp cho người quan trị hệ thống như ghi nhật ký, điều khiển truy nhập, phát hiện các thâm nhập đáng ngờ, có phản ứng khi có các trạng thái khả nghi, ...

Ngoài những ưu điểm đã liệt kê ở trên, thì tường lửa cũng có nhược điểm như tường lửa không chống được virút, không chống lại được tin tặc tấn cống từ cổng sau (backdoor)



Hình 3-24: Mô hình hệ thống tường lửa 3 phần

- **Hệ thống phát hiện đột nhập mạng**

Giới thiệu

Như đã trình bầy ở phần trên công nghệ tường lửa không thể bảo vệ an ninh - an toàn mạng đầy đủ, nó chỉ là một phần trong mô hình an ninh-an toàn khi kết nối WAN. Tường lửa không tự nhận ra được các cuộc tấn công và cũng không tự ngăn chặn được các cuộc tấn công đó. Có thể xem hệ thống tường lửa như hàng rào và hệ thống gác cổng vào/ra, không có khả năng phát hiện tin tặc tấn công, cũng không tự phản ứng được với các cuộc tấn công mà nó chưa biết trước .

Trong phần này chúng ta trình bầy một công cụ phục vụ an ninh - an toàn mạng thứ hai, đó là công nghệ phát hiện đột nhập, nó là công cụ bổ sung cho công cụ tường lửa. Nếu tường lửa là các trạm gác, thì hệ thống phát hiện đột nhập được xem như hệ thống các camera/video theo dõi, giám sát và là hệ thống báo động. Nó thường được đặt ở ngay trong trạm gác "tường lửa", hay đặt ở các vị trí quan trọng bên trong của mạng, nhằm chủ động phát hiện ra dấu hiệu mất an ninh-an toàn, hay phát hiện ra các cuộc tấn công không biết trước.

Hệ phát hiện đột nhập mạng là gì?

Là hệ thống nhằm phát hiện ra việc sử dụng không hợp pháp tài nguyên hệ thống, phát hiện những hoạt động lạm dụng, tấn công vào hệ thống máy tính hoặc mạng máy tính. Hệ phát hiện đột nhập IDS (intrusion detection system) là hệ thống bao gồm phần mềm và phần cứng thực hiện việc theo dõi, giám sát, thu nhận thông tin từ các nguồn khác nhau, sau đó phân tích để phát hiện ra dấu hiệu ("signature") của sự đột nhập (dấu hiệu của các hoạt động tấn công hay lạm dụng hệ thống), cảnh báo cho quản trị hệ thống, hay ra các quyết định phản ứng để phòng vệ. Nói một cách tổng quát IDS là hệ thống cho phép phát hiện các dấu hiệu làm hại đến tính bảo mật, tính toàn vẹn, và tính sẵn dùng của hệ thống máy tính hay hệ thống mạng máy tính làm cơ sở cho việc phản ứng lại, bảo đảm an ninh - an toàn hệ thống.

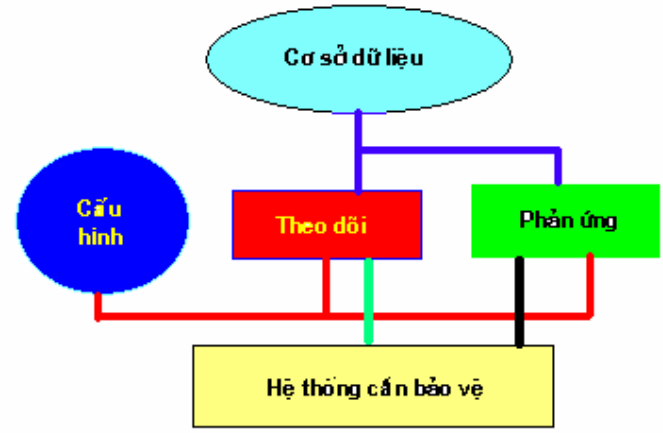
Để phát hiện ra những dấu hiệu của sự đột nhập, IDS cần phân tích các hoạt động của hệ thống, đồng thời nó phải có khả năng chỉ ra hoạt động nào là hoạt động tấn công hoặc lạm dụng hệ thống. Đôi khi để phát hiện sự đột nhập cần phải kết hợp nhiều phương pháp phân tích và quá trình phân tích cũng chia ra làm nhiều bước để phát hiện việc đột nhập đã vào chưa và ở mức độ nào (trước khi, trong khi, hay sau khi đã đột nhập thành công vào hệ thống?). Chẳng hạn một cuộc đột nhập bị phát hiện trước khi xảy ra thì người quản trị hệ thống sẽ dễ dàng ngăn chặn hoặc là cơ sở để giăng bẫy để bắt kẻ đột nhập khi chúng đột nhập và tấn công vào hệ thống (thu thập chứng cứ cho việc truy tố sau này). Nếu việc đột nhập được phát hiện trong khi đang xảy ra, hay thậm chí sau khi nó đã hoàn thành, thì điều phải làm đầu tiên của người quản trị hệ thống là đánh giá mức độ gây hại và cô lập đoạn mạng bị tấn công.

Cơ sở để thực hiện phản ứng lại với những hoạt động gây hại thường là ghi các sự kiện ra một hay nhiều nhật ký hệ thống thuận tiện cho việc phân tích sau này. Hệ thống phát hiện đột nhập cũng có thể được cấu hình để báo động khi có dấu hiệu

tấn công được phát hiện (dấu hiệu này được lưu trong cơ sở dữ liệu các dấu hiệu về các cuộc tấn công đã được biết). Phản ứng lại với các hoạt động gây hại cũng có thể là ngăn chặn tin tặc truy nhập vào hệ thống hoặc cho phép truy nhập kèm theo giám sát chặt, hoặc kích hoạt hệ thống tường lửa ngăn chặn các tác nhân gây hại.

Những hoạt động đột nhập là những hoạt động xâm nhập vào hệ thống một cách có ý thức mà không được phép của chủ hệ thống, nhằm mục đích:

- Truy cập các thông tin không được phép.
- Phá hoại thông tin.
- Phá hoại an ninh- an toàn hệ thống, làm cho hệ thống trở nên không tin cậy hoặc không hoạt động được,....



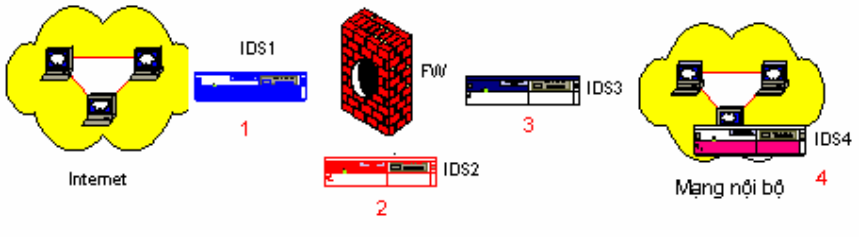
Hình 3-25: đồ cấu trúc của một hệ thống phát hiện đột nhập

Người đột nhập trong cuộc xâm nhập vào một hệ thống một cách có ý thức được phân làm hai dạng: từ bên trong và từ bên ngoài. Những kẻ đột nhập từ bên ngoài là những người không có quyền truy nhập vào máy hay mạng. Những kẻ xâm nhập từ bên trong là những người dùng hợp pháp nhưng chỉ được cấp quyền hạn chế trong hệ thống. Họ hoạt động bằng cách cố gắng truy cập tới những phần mà họ không được phép truy nhập của hệ thống. Họ truy nhập vì tò mò hoặc để lấy trộm thông tin không được phép.

Hệ phát hiện đột nhập là một hệ thống có các chức năng sau:

- Theo dõi, giám sát toàn mạng, thu nhận thông tin từ nhiều nguồn khác nhau của hệ thống.
- Phân tích những thông tin đã nhận được, để phát hiện những dấu hiệu phản ánh sự lạm dụng hệ thống hoặc những dấu hiệu phản ánh những hoạt động bất thường xảy ra trong hệ thống.

- Quản lý, phân tích hoạt động của người sử dụng hệ thống.
- Kiểm tra cấu hình hệ thống và phát hiện khả năng hệ thống có thể bị tấn công.
- Phân tích bằng thống kê để phát hiện những dấu hiệu thể hiện hoạt động bất thường của hệ thống.
- Quản lý nhật ký của hệ điều hành để phát hiện các hoạt đông vi phạm quyền của các người dùng.
- Tổ chức tự động phản ứng lại những hành động đột nhập hay gây hại mà nó phát hiện ra, ghi nhận những kết quả của nó.



Hình 3-26: Các vị trí đặt hệ phát hiện đột nhập

➢ **Hệ thống phát hiện lỗ hổng an ninh**

Hệ thống phát hiện lỗ hổ an ninh 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 an toàn trước khi đưa mạng vào hoạt động, và thường xuyên theo dõi để nâng cấp, vá các lỗ hỏng an ninh.

3.2.2.4 Bảo mật thông tin trên mạng

Công nghệ mã mật (cryptography)

Một trong những nguyên nhân sơ đẳng mà tin tặc có thể thành công là hầu hết các thông tin chúng ta truyền trên mạng đều ở dạng dễ đọc, dễ hiểu. Khi chúng ta kết nối WAN bằng công nghệ IP thì tin tặc dễ dàng thấy có thể bắt các gói tin bằng công cụ bắt gói (network sniffer), có thể khai thác các thông tin này để thực hiện tấn công mạng. Một giải pháp để giải quyết vấn đề này là dùng mật mã để ngăn tin tặc có thể khai thác các thông tin chúng bắt được khi nó đang được truyền trên mạng.

Mã hoá (Encryption) là quá trình dịch thông tin từ dạng nguồn dễ đọc sang dạng mã khó hiểu.Giải mã (Decryption) là quá trình ngược lại. Việc dùng mật mã sẽ đảm bảo tính bảo mật của thông tin truyền trên mạng, cũng như bảo vệ tính toàn vẹn, tính xác thực của thông tin khi lưu trữ.

Mã mật được xây dựng để đảm bảo tính bảo mật (confidentiality), khi dữ liệu lưu chuyển trên mạng. Khi dữ liệu đã được mã hóa thì chỉ khi biết cách giải mã mới có khả năng sử dụng dữ liệu đó. Hiện nay các kỹ thuật mã hóa đã phát triển rất mạnh với rất nhiều thuật toán mã hóa khác nhau. Các hệ mã khoá được chia làm hai lớp chính: Mã khoá đối xứng hay còn gọi là mã khoá bí mật. Mã khoá bất đối xứng hay còn gọi là mã khoá công khai.

Hệ mã đối xứng – Khoá mã bí mật.

Hệ mã đối xứng là hệ sử dụng một khoá bí mật cho các tác vụ mã hoá và giải mã. Có nhiều thuật toán khoá bí mật khác nhau nhưng giải thuật được dùng nhiều nhất trong loại này là:

DES (Data Encryption Standard). DES mã hoá khối dữ liệu 64 bit dùng khoá 56 bit. Hiện nay trong một số hệ thống sử dụng DES3 (sử dụng 168bit khoá thực chất là 3 khoá 56 bit)

IDEA (International Data Encryption Standard).IDEA trái với DES, nó được thiết kế để sử dụng hiệu quả hơn bằng phần mềm. Thay vì biến đổi dữ liệu trên các khối có độ dài 64 bit, IDEA sử dụng khóa 128 bit để chuyển đổi khối dữ liệu có độ dài 64 bit tạo ra khối mã cũng có dài 64 bit. Thuật toán này đã được chứng minh là khá an toàn và rõ ràng là hơn hẳn DES.

Các hệ mã hoá đối xứng thường được sử dụng trong quân đội, nội vụ, ngân hàng,... và một số hệ thống yêu cầu an toàn cao.

Vấn đề khó khăn khi sử dụng khoá bí mật là vấn đề trao đổi khoá. Trao đổi khoá bí mật luôn phải truyền trên một kênh truyền riêng đặc biệt an toàn, tuyệt đối không sử dụng kênh truyền là kênh truyền dữ liệu.

Hệ mã bất đối xứng – Khoá mã công khai.

Mã khoá công khai đã được tạo ra để giải quyết hai vấn đề khó khăn nhất trong khoá quy ước đó là sự phân bố khoá và chữ ký số.

Hoạt động của hệ thống mạng sử dụng mã khoá công khai như sau:

Khởi tạo hệ thống đầu cuối:

Mỗi hệ thống đầu cuối trong mạng tạo ra một cặp khoá để dùng mã hoá và giải mã thông tin sẽ nhận. Khoá thứ nhất K1 là khoá bí mật; Khoá thứ hai K2 là khóa công khai.

Các hệ thống công bố rộng rãi khoá K2 của mình trên mạng. Khoá K1 được giữ bí mật.

Mã hoá và giải mã thông tin:

Khi một người dùng A muốn gửi thông tin cho người dùng B

Người dùng A sẽ mã hoá thông tin bằng khoá công khai của người dùng B (K2B).

Khi người dùng B nhận được thông tin nó sẽ giải mã thông tin bằng khoá bí mật của mình (K1B).

Chữ ký số

Khi người dùng A gửi chữ ký cho người dùng B

Người dùng A mã hoá chữ ký của mình bằng khoá bí mật của chính mình (K1A).

Người dùng B nhận được chữ ký của người dùng A, người dùng B sẽ giải mã chữ ký của người dùng A bằng khoá công khai của người dùng A (K2A).

Chuyển đổi khoá

Khi người dùng A gửi thông tin khoá cho người dùng B.

Người dùng A mã hoá thông tin khoá 2 lần. Lần đầu bằng khoá bí mật của bản thân (K1A); Lần hai bằng mã công khai của người nhận (K2B).

Người dùng B nhận được thông tin khoá sẽ giải mã thông tin khoá hai lần. Lần đầu bằng khoá bí mật của bản thân (K1B). Lần 2 bằng khoá công khai của người gửi (K2A).

Một số giải thuật cho mã khoá công khai được sử dụng như: Diffie_Hellman, RSA, ECC, LUC, DSS,...

- **Mô hình ứng dụng**

Mô hình ứng dụng là mô hình xây dựng trên các ứng dụng yêu cầu kết nối WAN

Phân tích kết nối dựa trên các yêu cầu ứng dụng

Tách, gộp các ứng dụng, đánh giá yêu cầu giải thông, đánh giá yêu cầu chất kượng dịch vụ, đánh giá yêu cầu độ tin cậy của các kết nối,...

Trên cơ sở các mô hình phân cấp, mô hình tôpô, 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 tôpô chúng ta có thể tính khoảng cách kết nối, mô hình ứng dụng để dự tính giải 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 nầy cần được tối ưu chọn giải pháp hợp lý thoả 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 quả lý mạng:
  Từ mô hình tôpô, 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 , giải thông cần thiết cho từng ứng dụng, các giao thức mạng triên khai ngay, và các giao thức sẽ dùng trong tương lai gần, tương lai xa,... tính toán phân bố 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.

Từ các yêu cầu chúng ta tiến hành bước lựa chọn công nghệ kết nối:

- 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 dải thông của các ứng dụng.
  - Chi phí cho kết nối bao gồm chi phí thiết bị, chi phí cài đặt ban đầu, và đặc biệt phải xem xét là chi phí hàng tháng, và 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
- 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.

3.3 Phân tích một số mạng WAN mẫu

Phần này đưa ra một số WAN minh hoạ:

Xây dựng WAN cho trung tâm thông tin của một bộ ngành.

➢ **Phân tích yêu cầu:**

Mục tiêu của hệ thống: hệ thống WAN và truy cập từ xa, cho trung tâm thông tin của một bộ được thiết kế nhằm đảm bảo các mục tiêu sau đây:

- Hệ thống này được xây dựng trên các thành phố Hà Nội, Hồ Chí Minh, Đà Nẵng và Cần Thơ;
- Tại mỗi thành phố, các chi nhánh được kết nối tới trụ sở chính;
- Trụ sở chính 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 và trụ sở khác qua nhiều cách thức kết nối mạng diện rộng khác nhau hiện có tại Việt Nam như Leased line, vô tuyến trải phổ, 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 Khách hàng.

Các yêu cầu của hệ thống:

- Kết nối được với Internet;
- Có thể truy cập vào trung tâm mạng (NOC) qua mạng điện thoại công cộng PSTN
- Hệ thống được được thiết kế như một ISP cỡ nhỏ;
- Hệ thống kết nối và truy cập 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;
- Hệ thống mạng phục vụ công tác nghiệp vụ và khai thác Internet cho khoảng 100 nút mạng trong Trung tâm mạng;
- Hỗ trợ các cách thức kết nối mạng diện 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, hội nghị viễn đàm,...mà không bị phá vỡ cấu trúc thiết kế ban đầu;
- Phân mạng truy cập 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 của Khách hàng. 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. Hiện tại, Trung tâm được thiết kế cho khoảng 100 thành viên. 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.

Hệ thống mạng tại Hà Nội và thành phố Hồ Chí Minh được thiết kế là trung tâm mạng, cho phép các chi nhánh có thể truy nhập bằng nhiều phương thức và có thể kết nối với Internet.

Do kinh phí hạn chế nên chúng ta có thể thực hiện thành nhiều pha. Pha 1 triển khai tại tổng hành dinh (head office).

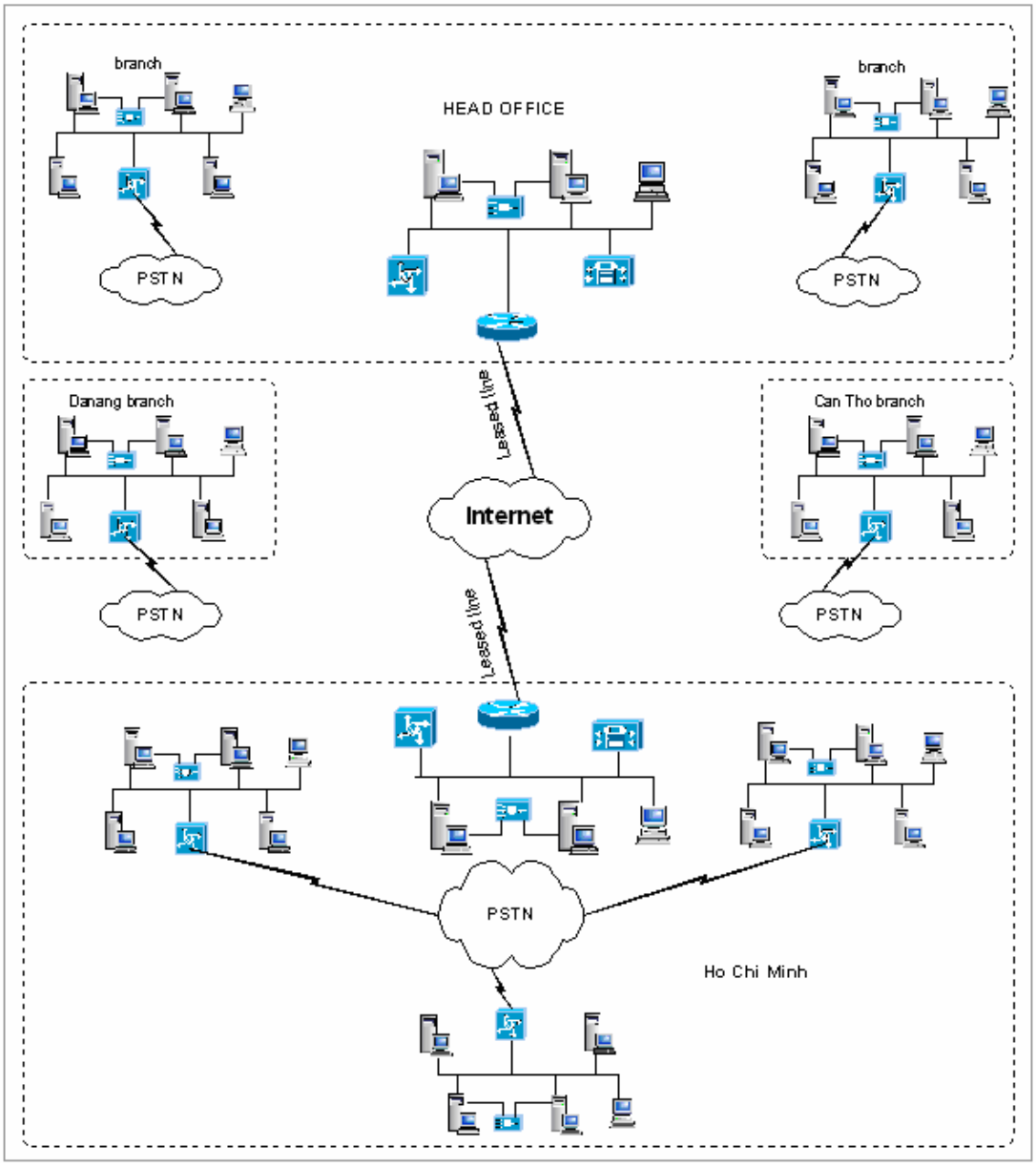
Nhìn từ góc độ tổ chức hệ thống mạng,và các yêu cầu kỹ thuật, cũng như các yêu cầu ứng dụng, trung tâm thông tin của một bộ vừa là một nơi chứa và cung cấp thông tin, tương tự như một nhà cấp nội dung (ICP), vừa là nơi cung cấp dịch vụ truy nhập từ xa, và kết nối các chi nhánh tương tự như một nhà cung cấp dịch vụ Internet (ISP). Do đó thiết kế sẽ có thể tham khảo hệ thống mạng của một nhà cung cấp dịch vụ Internet vớicác hoạt động lõi là kho thông tin và hệ thống biên tập tin.

Cấu hình cơ bản bao gồm một số phân mạng (Subnet) với các mức độ an ninh - bảo vệ khác nhau tùy theo chức năng và được tách biệt bởi hệ tường lửa.

Phân lớp mạng cung cấp truy nhập (Access Network): Cung cấp truy nhập từ xa vào trung tâm mạng(NOC) bằng nhiều phương thức như từ Internet và từ người dùng quay số (Dialup) qua mạng điện thoại công cộng (PSTN).

Thiết bị trung tâm của phân mạng cung cấp truy nhập bao gồm: Bộ định tuyến – Router, đây là thiết bị thực hiện các kết nối WAN trung tâm mạng với các chi nhánh, và từ mạng trong ra Internet trên các kênh thuê riêng (leased line), VPN, hay vô tuyến trải phổ tuỳ theo yêu cầu chất lượng, và chi phí kết nối phải trả.

Hệ thống kết nối này cũng phải được thiết kế có khả năng mở rộng cao, dễ dàng nâng cấp đường khi có yêu cầu.



Hình 3-27: Mô hình topo WAN kết nối tổng hành dinh với các chi nhánh

Dịch vụ cung cấp truy nhập từ xa qua mạng điện thoại công cộng PSTN được thực hiện thông qua Access Server, chủ yếu cấp cho các thành viên của trung tâm truy cập từ xa. Access Server cần phải lựa chọn để đảm bảo tốc độ kết nối và có thể được mở rộng được.

Các kết nối qua đường Leased line chủ yếu phục vụ trao đổi thông tin giữa các chi nhánh và trung tâm. Dung lượng leased line phhổ biến bắt đầu từ 64 Kbps và có thể nâng cấp từng bước đến E1 (2,048 Mpbs) do vậy cũng phải chọn thiết bị kết nối(NTU,...) có thể nâng cấp được tốc độ. Trong trường hợp yêu cầu kết nối có tốc độ cao hơn thì phải khảo sát khả năng dùng hệ thống cáp quang cùng các thiết

bị kết nối SONET, hay các nhà cung cấp dịch vụ viễn thông có thể cung cấp được không.Hệ thống kết nối kênh tốc đọ cao này cũng cần có giải pháp dự phòng cho trường hợp có sự cố sẽ không làm gián đoạn kết nối. Giải pháp dự phòng có thể dùng nối bó qua đường điện thoại công cộng.

Phân lớp mạng cung cấp dịch vụ (Service Network): Cung cấp các dịch vụ chạy trên bộ giao thức IP như thư điện tử, diễn đàn, truy cập Web và các dịch vụ trên Internet khác. Dịch vụ tên miền(DNS),... ;

Phụ thuộc vào số lượng người sử dụng của toàn bộ hệ thống mạng, phần mạng cung cấp dịch vụ này sẽ được thiết kế cho phù hợp. Khả năng có thể mở rộng là điều được quan tâm hàng đầu trong phần mạng này, một hoặc nhiều máy chủ sẽ được thêm vào hệ thống cho phép các dịch vụ Web, điện thư hay dịch vụ khác được phục vụ dựa trên các máy chủ riêng rẽ.

Trong giai đoạn ban đầu với số lượng người dùng hạn chế, số lượng máy chủ chưa cần tối đa với cấu hình mạnh. Tuy nhiên, đối với hệ thống cần độ sẵn sàng cao, việc có ít nhất mỗi dịch vụ một máy chủ với cấu hình đủ mạnh, có khả năng thay thế dịch vụ cho nhau là cần thiết để đảm bảo tính liên tục của dịch vụ.

Các máy chủ ứng dụng là các thiết bị quan trọng nhất cho việc xử lý thông tin, cũng là trung tâm của toàn bộ hệ thống thông tin. Chúng chịu trách nhiệm lưu trữ, tính toán, xử lý các thông tin vào/ra của toàn bộ hệ thống. Chúng ta có thể sử dụng giải pháp của nhiều hãng chẳng hạn như :

- Borland Insprise;
- Oracle;
- Microsoft;
- IBM;
- Bộ phần mềm WebSphere;
- Các hãng khác.

Phân lớp mạng nội bộ (Internal Network): Cung cấp các dịch vụ xác thực người dùng (Authentication), tính cước (Billing) và quản lý mạng. Đây là lớp cần được quan tâm bảo vệ nhất trong thiết kế của các hệ thống mạng cung cấp dịch vụ;

Để đảm bảo độ an toàn an ninh cao cho người dùng trong mạng nội bộ, ta có thể đặt thêm máy chủ xác thực bên ngoài mạng nội bộ.

Dịch vụ xác thực và tính cước được xây dựng dựa trên độ lớn của hệ thống mạng, số lượng người sử dụng và các yêu cầu tính cước.

Các dịch vụ hỗ trợ cung cấp dịch vụ và quản lý mạng khác cũng được thực hiện trong phân mạng này, trong đó các chức năng quản lý mạng, sao lưu dữ liệu, dịch vụ khách hàng. Các công cụ chuyên nghiệp có thể được dùng như SyMON đối với hệ SUN Microsystem hay HP OpenView có thể chạy trên hệ Windows,...

Phân mạng Cơ sở dữ liệu, biên tập (Information Editing): Nơi chứa kho dữ liệu, đồng thời là nơi làm việc của ban biên tập. Từ đây các thông tin, dữ liệu được biên tập để cập nhật vào hệ CSDL và Web server. Phân mạng này cũng cần được bảo vệ chống mọi hình thức xâm nhập trái phép từ bên ngoài với mục đích lấy thông tin hay phá hoại hệ thống.

Các máy tính trong phân mạng này chỉ được phép truy nhập trong nội bộ và tới một số máy chủ nhất định như máy chủ Web hay CSDL. Bên ngoài tường lửa không thể truy nhập tới các máy tính trong phân mạng này.

- **Lựa chọn phương án kết nối:**

<u>Lựa chọn số 1 là dùng cáp đồng trực tiếp nối Leased line</u>

Leased line dùng trực tiếp cáp đồng là cách kết nối phổ biến nhất hiện nay giữa hai điểm có khoảng cách xa, từ Trung tâm Thông tin tới đầu cuối của nhà cung cấp IXP/ISP gần nhất.

Tại Việt Nam, để tiết kiệm chi phí thuê băng thông, chúng ta thường thuê một số kênh cơ sở n x 64K rồi ghép kênh rồi mở rộng dần đạt được băng thông theo yêu cầu.

Với nhu cầu trước ban đầu của Trung tâm Thông tin , kênh thuê riêng là 128 Kbps. Với hệ thống này ta dễ dàng nâng cấp từng bước tới E1(2,048 Mbps) bằng cách thuê và ghép thêm các kênh cơ sở .

Để thực hiện được các yêu cầu và nhiệm vụ ở trên, qua mô hình topo phương án kết nối được thực hiện như sau:

- Kết nối truyền số liệu (TSL) bằng cáp đồng từ Trung tâm mạng tới Nhà cung cấp kết nối Internet (IXP). Trong thời điểm hiện tại, Việt Nam đang có 3 nhà cung cấp IXP là công ty VDC trực thuộc Tổng công ty Bưu chính Viễn thông, công ty truyền thông FPT và công ty điện tử Viễn thông quân đội Vietel. Đường truyền này tốc độ khởi điểm được đặt là 128 Kbps, có khả năng nâng cấp lên tốc độ E1 (2,048 Mbps);
- 01 kênh dự phòng được nối tới một IXP hoặc ISP khác để đảm bảo độ ổn định cao của hệ thống;

Kênh thuê bao kết nối riêng đi Internet tới một IXP hoặc ISP gần nhất:

- Cáp đồng điện thoại thông thường của hạ tầng viễn thông Việt Nam (đường kính cáp 0,5 mm);
- Sử dụng các tuyến cáp riêng trực tiếp (thông thường là cáp đồng đường kính cáp 0,9 mm hoặc cáp quang), có thể dùng cho nâng cấp kết nối tới tốc độ 2,048 Mbps (E1).

Dùng kết nối mạng riêng ảo VPN là lựa chon thứ 2, sau khi so sánh chi phí kết nối với phương án 1.

Mạng riêng ảo VPN có các ưu điểm:

- Kết nối trực tiếp giữa các điểm bất kỳ (Any-to-Any Connectivity)
  Tất cả các địa điểm trong mạng có thể liên hệ trực tiếp với nhau chỉ với một kết nối vật lý duy nhất tại mỗi địa điểm, không cần dùng leased line hay PVC. Điều này làm cấu trúc mạng trở nên đơn giản và cho phép mở rộng mạng một cách nhanh chóng không cần thiết kế lại mạng hay làm gián đoạn hoạt động của mạng.
- Dùng các công nghệ kết nối khác nhau
  VPN cho phép lựa chọn các công nghệ kết nối khác nhau (leased line, frame relay, ADSL, Ethernet, PSTN, ...) tuỳ thuộc vào yêu cầu về băng thông và phương thức kết nối tại mỗi điểm của người dùng.
  Có thể tích hợp dữ liệu, thoại và video (Data, Voice and Video Convergence)
  Với các công nghệ quản lý chất lượng dịch vụ (QoS) chuẩn, tất cả các ứng dụng dữ liệu, thoại và video có thể chạy trên một Mạng IP riêng, không cần có các mạng riêng rẽ hay thiết bị chuyên dùng.
- Độ bảo mật cao (High Network Privacy)
  Hệ thống bảo mật có sẵn trong mạng sử dụng công nghệ Chuyển mạch nhãn đa giao thức (Multi-Protocol Label Switching - MPLS) cho phép phân tách luồng dữ liệu của mỗi khách hàng ra khỏi Internet cũng như các khách hàng khác. Mức độ bảo mật tương đương như các dịch vụ lớp 2 như X.25, frame relay và ATM.
- Dễ sử dụng (Ease of Operation)
  VPN hạn chế yêu cầu đối với người dùng trong việc thực hiện các công việc phức tạp như thiết kế mạng, cầu hình bộ định tuyến. Do vậy giảm rất nhiều chi phí vận hành
- Một điểm liên hệ cho mọi yêu cầu (One Stop Shopping)

Các ISP cung cấp dịch vụ trọn gói với một điểm liên hệ duy nhất trên phạm vi toàn Việt Nam. điều đó giúp đơn giản hoá việc triển khai các mạng quy mô lớn.

- Đáp ứng nhiều dịch vụ

  Ứng dụng trao đổi dữ liệu như truyền file, dịch vụ thư tín điện tử, chia sẻ tài nguyên mạng (file hoặc máy in), cơ sở dữ liệu, Web nội bộ, Truyền ảnh, Các ứng dụng ERP, các ứng dụng thiết kế kỹ thuật.

  Truy nhập Internet và sử dụng các dịch vụ trên nền mạng này như một khách hàng Internet trực tiếp bình thường.

  Các ứng dụng về âm thanh, hình ảnh trong mạng riêng của khách hàng (Khách hàng có khả năng thiết lập một tổng đài PBX sử dụng công nghệ IP và có thể gọi trong phạm vi mạng nội bộ của mình).

  Một số ứng dụng cao hơn như: hội thảo qua mạng MPLS VPN, hosting...

  Mạng riêng ảo trên Internet cho phép tận dụng được những ưu thế của Internet, đặc biệt khi phải thực hiện kết nối tới các điểm có khoảng cách xa. Do một kết nối Internet có thể được dùng để nối tới nhiều điểm khác nhau, nên Mạng riêng ảo có những ưu thế tổng hợp của các kết nối PPP, dialup, và các dịch vụ mạng lưới. Đồng thời, VPN cho phép dễ dàng tích hợp nhiều giao thức WAN khác nhau.

Tiết kiệm chi phí với mạng riêng ảo VPN:

Nếu dùng Internet cho các giao dịch LAN-to-LAN, theo đánh giá của một số tổ chức nghiên cứu về mạng, có thể làm giảm tới 80% chi phí so với cách thức kết nối WAN truyền thống. Hiện nay, nhiều công ty và tổ chức nhận thức được điều này nhưng chưa thực hiện vì còn một vấn đề lớn cần quan tâm: an ninh. Mạng riêng ảo (VPN) cung cấp một giải pháp hiệu quả cho vấn đề an ninh. VPN đưa ra một cách thức – công nghệ kết nối các mạng LAN với nhau và với người dùng di động an toàn và hiệu quả.

Nhưng phương thức này hiện chưa được dùng nhiều vì chưa đực đánh giá đầy đủ về chi phí cũng như an ninh-an toàn.

<u>Dùng kết nối ADSL là lựa chọn thứ 3:</u>

ADSL (Asymetric Digital Subcriber Line) là công nghệ băng thông rộng cho phép truy cập về trung tâm mạng hay vào internet với tốc độ cao.

ADSL tận dụng hệ thống cáp điện thoại bằng đồng có sẵn để truyền tải dữ liệu ở tốc độ cao mà không cần phải lắp đặt thêm cáp quang (fibre-optic) hoặc cáp đồng,

tiết kiệm chi phí hơn. Tất cả các dạng ADSL hoạt động dựa trên nguyên tắc tách băng thông trên đường cáp điện thoại thành hai: một phần nhỏ dành cho truyền âm, phần lớn dành cho truyền tải dữ liệu ở tốc độ cao. Trên đường dây điện thoại thì thực tế chỉ dùng một khoảng tần số rất nhỏ từ 0KHz đến 20KHz để truyền dữ liệu âm thanh (điện thoại). Công nghệ ADSL tận dụng đặc điểm này để truyền dữ liệu trên cùng đường dây, nhưng ở tần số 25.875 KHz đến 1.104 MHz. Do vậy ta vừa có thể kết nối truyền số liệu vừa dùng điện thoại.

Đây là công nghệ rất mới cần được đánh giá.

So sánh đánh giá các phương thức kết nối WAN hiện có tại Việt Nam:

Dịch vụ WAN	Một cổng WAN có thể nối tới:	Số lượng kết nối	Đặc điểm chính
Dial-Up Analog	Nhiều nơi	Một	• Nối một điểm tới một điểm • Tốc độ hạn chế
ISDN Dial-Up (BRI)	Nhiều nơi	1 đường (128K) hoặc 2 đường (mỗi đường 64K)	• Nối một điểm tới một điểm • Chưa phổ biến ở Việt Nam, Chỉ có ở Hà nội, Tp HCMC
ISDN Dial-Up (PRI)	Nhiều nơi	30 đường (tới 64K mỗi đường)	• Mô hình tập trung • Nhiều kết nối đồng thời • Chưa phổ biến ở Việt Nam
Leased Line	Một nơi	Một	• Cố định điểm tới điểm • Băng thông đảm bảo • Độ tin cậy cao
Frame Relay	Nhiều nơi	Nhiều điểm	• Một điểm tới nhiều điểm • Băng thông đảm bảo • Đang được khuyến khích phát triển bởi Tổng CT BCVT VN
X.25	Nhiều nơi	Nhiều điểm	• Một điểm tới nhiều điểm • Thường được dùng với các hạ tầng viễn thông lạc hậu
mạng riêng ảoVPN, qua	Nhiều nơi	Nhiều điểm	• Một điểm tới nhiều điểm • Chi phí hấp dẫn đối với các

hạ tầng Internet			mạng WAN khoảng cách xa • Băng thông linh hoạt • Độc lập với các dịch vụ diện rộng nội bộ
ADSL	Một nơi	Một	• Cố định điểm tới điểm • Băng thông rất cao • Chi phí hứa hẹn • Hiện đang là dịch vụ thử nghiệm
Dịch vụ WAN	Băng thông	Giá	Độ sẵn có về địa lý
Analog	• Tốc độ tới 56K	• Nội hạt thì rẻ, đường dài và quốc tế còn đắt	Có ở khắp mọi nơi
ISDN Dial-Up (BRI)	• Lên tới 64K mỗi kênh • được đảm bảo tới 128K	• Cước tính theo thời lượng sử dụng	Châu Âu rất thông dụng, tuy nhiên chỉ một phần châu Á phát triển loại hình này. Đang được thử nghiệm ở Việt Nam.
ISDN Dial-Up (PRI)	• 64K mỗi kênh	• Cước tính theo thời lượng sử dụng	Cũng như trên
Leased Line	• 56K-1.5Mb (T1) • 64K-2Mb (E1) • 45Mb (T3)	• Phụ thuộc khoảng cách và băng thông	Có ở khắp mọi nơi; có nhiều lựa chọn.
Frame Relay	• 56K-1.5Mb (T1) • 64K-2Mb (E1) • 45Mb (T3)	• Cước có thể tính theo khoảng cách và băng thông, cũng như có thể tính theo dung lượng truyền	Được phát triển chủ yếu ở Bắc Mỹ và Tây Âu, Việt Nam đang cố gắng đẩy loại hình này phát triển.
X.25	• Tới 64K	• Tính cước theo băng thông hoặc theo thông lượng	Chủ yếu ở các thị trường châu Á, Mỹ La tinh và Đông Âu. Việt Nam đang dùng ít.

Mạng riêng ảo VPN trên hạ tầng internet	• 56K-1.5Mb (T1) • 64K-2Mb (for E1) • 45Mb (T3)	• Phụ thuộc vào giá cước viễn thông nội hạt để nối tới ISP và giá quy định bởi ISP	Ở đâu có Internet thì có nó!
ADSL	• 8Mb (download) • 800Kb (upload) • Càng gần tổng đài tốc độ càng cao	Chưa có giá chính thức	Đang phổ biến ở nhiều nước châu Á, đã có ở Hà nội , Hải phòng, và TP HCMC

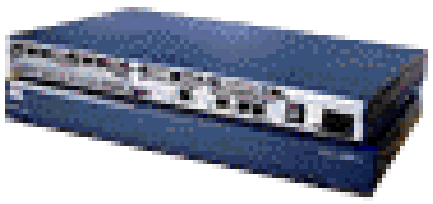
➢ **Lựa chọn thiết bị:**

Thiết bị, vật tư tối thiểu để xây dựng kết nối WAN trung tâm Trung tâm Thông tin tới ISP, và tới các chi nhánh gồm có:

- Bộ định tuyến - Router

  Thiết bị Router được lựa chọn phải đảm bảo:

  - Có số lượng cổng WAN nhiều hơn các điểm cần kết nối. Có các cổng LAN đủ nối với các phân đoạn mạng cần thiết. Có năng lực xử lý đảm bảo không quá 60% yêu cầu, có số RAM đủ.
  - Có Router dự phòng cho Router chính .
  - Router phải được sản xuất bởi hãng có uy tín trên Thế giới, như Cisco, Nortel,... để đảm bảo độ ổn định, tin cậy cao.
  - Hỗ trợ các giao thức định tuyến động như RIP-1, OSPF, EIGRP,...
  - Có các bộ giao tiếp cho phép thiết bị tương thích với nhiều loại kết nối trong điều kiện hạ tầng Viễn thông hiện tại ở Việt Nam như Ethernet/Fast Ethernet, T1/E1, ISDN PRI, ISDN BRI, OC-3, ATM,...

    
  - Đảm bảo tương thích để bảo toàn được chi phí đầu tư ban đầu cho phía Khách hàng, .

Với yêu cầu ban đầu là 3 cổng WAN Router được chọn là Cisco Router 2621. Đây là thiết bị thỏa mãn mọi yêu cầu đặt ra của Dự án. Nó cho phép đạt tốc độ xử lý 25 Kpps.Ngoài ra, nó còn hỗ trợ VLAN, IP VPN,... và các bộ giao tiếp cắm thêm theo yêu cầu cho phép ta dễ dàng nâng cấp nếu cần.

- Modem số (xDSL Modem)

  Là thiết bị nối giữa thiết bị truyền và đầu nối viễn thông, hay còn gọi là thiết bị đầu cuối mạch dữ liệu DCE, thực hiện nhiệm vụ chuyển số liệu. Modem số được lựa chọn cho Dự án Khách hàng phải thoả mãn các yêu cầu sau đây:

  - Được sản xuất bởi các hãng có danh tiếng trên Thế giới như Patton, RAD, Pandatel, v.v...
  - Thiết bị hỗ trợ tốc độ cao hơn trong trường hợp nâng cấp đường kết nối mạng diện rộng. Pha đầu của Dự án Khách hàng, kênh thuê riêng có tốc độ 128 Kbps;
  - Đảm bảo độ chính xác cao, dữ liệu lưu thông qua phương thức đồng bộ bằng nhau bằng cách cung cấp nguồn định thời;
  - Đảm bảo điện áp luôn thích hợp;
  - An toàn dữ liệu cao, tìm và hiệu chỉnh lỗi trong quá trình truyền/nhận dòng thông tin;
  - Hỗ trợ nén thông tin;
  - Định hình tín hiệu số;
  - Có khả năng chẩn đoán lỗi từ xa.
  - Hỗ trợ quản trị từ xa qua các module ghép thêm tại tổng đài kết nối;

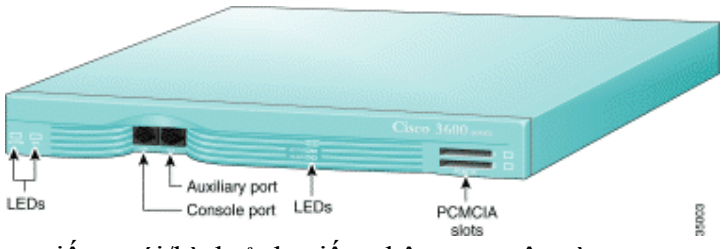
  Modem được lựa chọn cho Dự án Trung tâm Thông tin là ASMi-50.

  Đây là sản phẩm nổi tiếng của hãng RAD, hiện đang rất thông dụng tại Việt Nam.

  Dòng modem này cho phép truyền với khoảng cách xa tới 8,2 Km và tốc độ cao nhất đạt 1152 Kbps.

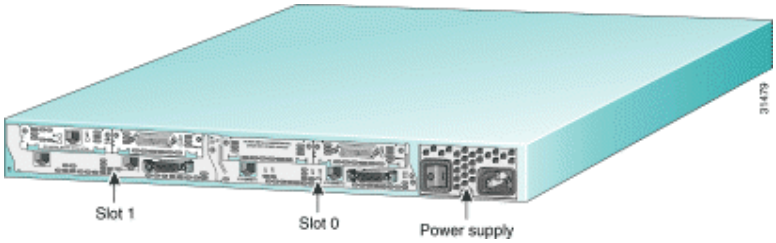
- Access Server

Thiết bị Access Server đặt tại Trung tâm được thiết kế để đáp ứng nhu cầu kết nối qua mạng PSTN cho khoảng 200÷300 tài khoản người dùng. Như vậy hệ thống phải đáp ứng được nhiều cuộc gọi cùng lúc. Ngoài ra hệ thống cũng cho phép lắp thêm đường truy cập trong trường hợp nâng cấp hệ thống.
Tại Trung tâm cấp truy cập qua mạng điện thoại của hệ thống mạng, ta đăng ký số trượt cho các đường điện thoại truy cập của Dự án. Thiết bị Access Server được đặt chế độ tự động trượt số trong trường hợp có nhiều yêu cầu kết nối cùng lúc tới Trung tâm.
Các tài khoản người dùng được quản lý thông qua một phần mềm quản trị tài khoản truy cập từ xa.
Phần mềm quản lý tài khoản truy nhập phải tương thích hoàn toàn với thiết bị Access Server. Đồng thời nó cũng hỗ trợ sử dụng các giao thức bảo mật tài khoản người dùng như CHAP/PAP, TACACS+, DES,...
Công tác quản trị người dùng truy cập được thông qua giao diện Web thân thiện. Nhân viên quản trị mạng có thể dễ dàng chỉnh sửa, tạo/xoá các tài khoản truy nhập.
Trong trường hợp nâng cấp hệ thống, các Access Server thế hệ mới được lựa chọn cũng hỗ trợ kết nối tới mạng điện thoại công cộng thông qua các kênh thuê riêng như T1/E1.
Sử dụng các Access Server thế hệ mới, ngoài việc nâng tốc độ kết nối ngược dòng qua modem là 56K, nhờ vậy, tốc độ và độ ổn định của kết nối dialup tới Trung tâm mạng cũng được cải thiện đáng kể.
Access Server có thể lựa chọn là loại Cisco Access Router 3620.
Đây là thiết bị đa chức năng được thiết kế cho một ISP cỡ nhỏ. Với hơn 20 module tuỳ chọn trên một thiết bị, nó cho phép tích hợp nhiều giải pháp trên cùng một thiết bị: đa giao thức định tuyến, tích hợp tiếng nói/hình ảnh, tiếp nhận truy cập từ xa qua Dialup, ...

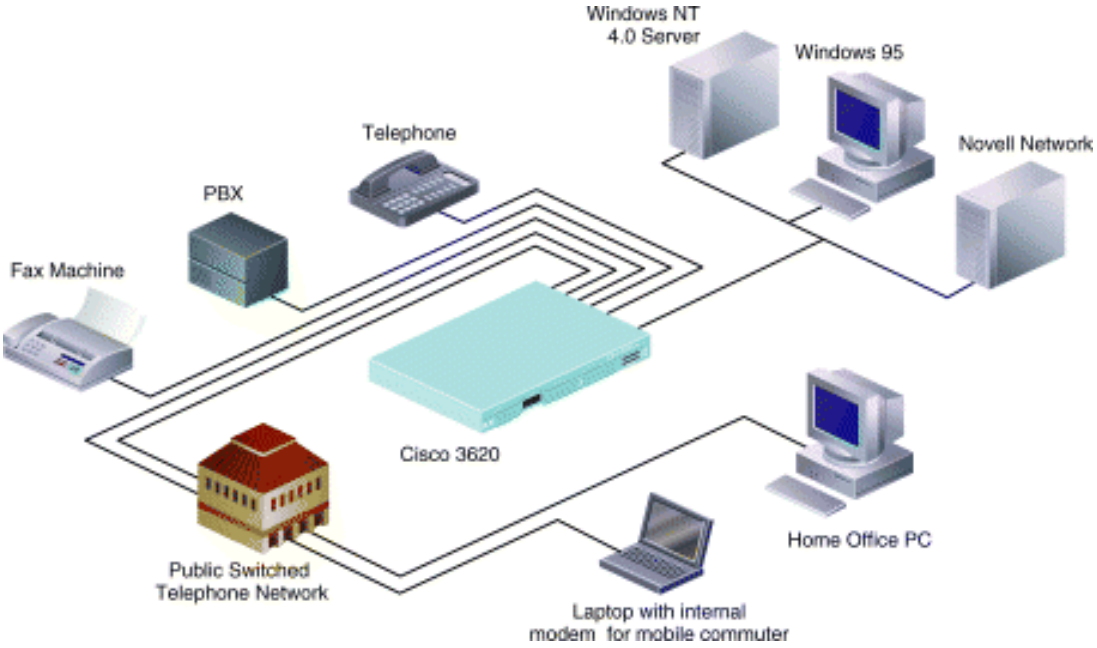


Thiết bị thuộc họ 3600, có tính tương thích cao với nhiều loại kết nối Viễn thông khác nhau như Ethernet/Fast Ethernet, T1/E1, ISDN PRI, ISDN BRI, OC-3, ATM,....và các module tuỳ chọn thêm.

Tập hợp các module trên người ta gọi là 1 Slot. Mỗi Slot cho phép đặt nhiều nhất 16 đường kết nối không đồng bộ qua modem. Dòng 3620 có 02 Slot. Tuỳ theo yêu cầu sử dụng mà ta đặt hàng trong Slot gồm những module nào?



Cisco 3620 sử dụng bộ xử lý R4700 80Mhz, cho phép đạt hiệu suất 20÷40 Kpps.



Hình 3-28: Access Server Cisco 3620

Kiến trúc Module:

Mỗi chức năng của hệ thống được bóc tách thành các module riêng. Đây là loại kiến trúc có hiệu năng cao, cho phép bảo vệ đầu tư cho dự án của Khách hàng và tích hợp nhiều chức năng trên cùng một thiết bị. Khi nhu cầu của dự án ban đầu là dùng 3620 làm thiết bị phục vụ truy cập từ xa thì ta chỉ cần đặt hàng cổng modem không đồng bộ trong tùy chọn.

Trong trường hợp dự án Khách hàng xây dựng hệ thống tiếp nhận các kết nối Dialup của người dùng từ xa, thiết bị Cisco 3620 có thể phục vụ tối đa 32 người dùng cùng lúc kết nối vào hệ thống. Thực tế cho thấy hệ thống tiếp nhận truy cập này có thể cung cấp cho khoảng xấp xỉ 500 người dùng truy cập từ xa.

Ngoài ra, 3620 cũng cho phép ta lắp đặt thêm các module modem kỹ thuật số trong trrường hợp hệ thống kết nối nâng cấp lên E1.

Chi tiết về thiết bị được mô tả bởi bảng dưới đây:

Các tính năng kỹ thuật	Chi tiết
Các tính năng chung	24 ÷32 cổng modem analog dựng sẵn; 10/100 Ethernet LAN Cho phép kết nối qua đường T1/E1 WAN qua các cổng modem dựng sẵn; Hỗ trợ các dòng modem analog 56K theo chuẩn V90; Cho phép cập nhật các phần mềm nâng cấp của modem; Hiệu suất cao, đạt 20÷40 (Kpps); Hỗ trợ các kết nối an toàn bảo mật qua VPN, bao gồm các tuỳ chọn như firewall, mã hoá dữ liệu và các giao thức đường hầm.
Bộ vi xử lý	80-MHz IDT R4700 RISC
DRAM	4 ÷ 64 MB
NVRAM	32 KB
Flash memory (SIMM)	4 ÷ 32 MB
Flash memory (PCMCIA)	2 ÷ 32 MB
Boot ROM	512 KB
Dimensions (H x W x D)	1.75 x 17.5 x 13.5 inches (4.4 x 44.5 x 34.3 cm)
Weight	23 lb (10.45 kg) maximum, including chassis and two network modules
Input voltage, AC power supply Current Frequency Input surge current (AC)	100 to 240 VAC, autoranging 1.0A 47 to 63 Hz 50A, one cycle

Input rating, DC power supply Operational between Current Input surge current (DC)	-48 to -60 VDC -36 to -72 VDC 3.0A 65A, 250mS
Power dissipation	60W (maximum)
Console and Auxiliary ports	RJ-45 connector
Operating humidity	5 to 95%, noncondensing
Operating temperature	32 to 104\xb0 F (0 to 40\xb0 C)
Nonoperating temperature	-40 to 185\xb0 F (-40 to 85\xb0 C)
Noise level	45 dBA (maximum)

Tóm lại, đây là thiết bị thoả mãn mọi yêu cầu đặt ra cho các thiết bị kết nối và truy nhập mạng.

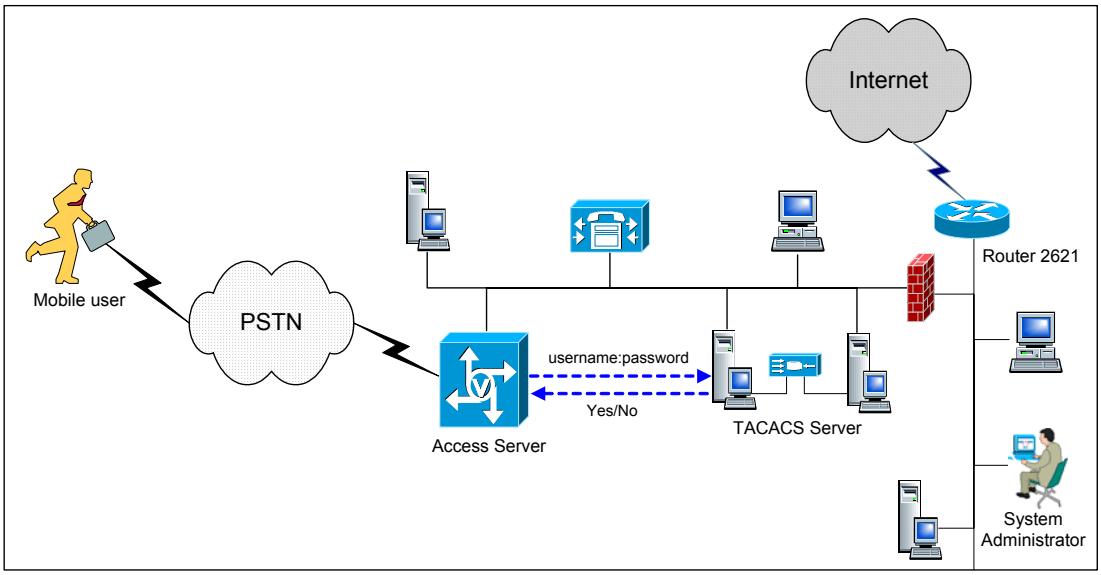
- Modem

  Các modem được cấu hình để tự động trả lời cuộc gọi. Thông thường, cuộc gọi được ấn định sau hai hồi chuông. Trong pha đầu của Dự án, kết nối Dialup được thực hiện qua mạng điện thoại công cộng nên tốc độ ngược dòng hạn chế là 33.6 Kbps. Do đó ta nên đặt cấu hình cho modem chạy với tốc độ 38.400 bps để hiện tượng ngắt kết nối đột ngột.

  Ta nên ghi cứng chuỗi khởi tạo cho modem để đề phòng trường hợp mất điện hoặc sự cố. Khi Access Server phải khởi động lại, từ chuỗi khởi tạo chung, nó sẽ nhận lại cấu hình đã được ghi cứng cho modem.

  Giá đặt modem cần phải được thiết kế khoa học, vừa đủ không gian để thoát nhiệt vừa đảm bảo mỹ quan cho phòng mạng.

  Modem cho dự án – Khách hàng được lựa chọn là Fax modem US Robotic 56K.



Hình 3-29: Người dùng xa kết nối về tổng hành dinh qua mạng điện thoại công

➢ Tổ chức triển khai

Công tác cấu hình hệ thống WAN sẽ được triển khai sau khi hoàn thành lắp đặt hệ thống LAN tại tòa nhà Trung tâm Thông tin.

Toàn bộ hệ thống WAN đã được chia thành các phân lớp mạng trong quá trình thiết kế. Do đó, triển khai hệ thống theo từng phân lớp mạng.

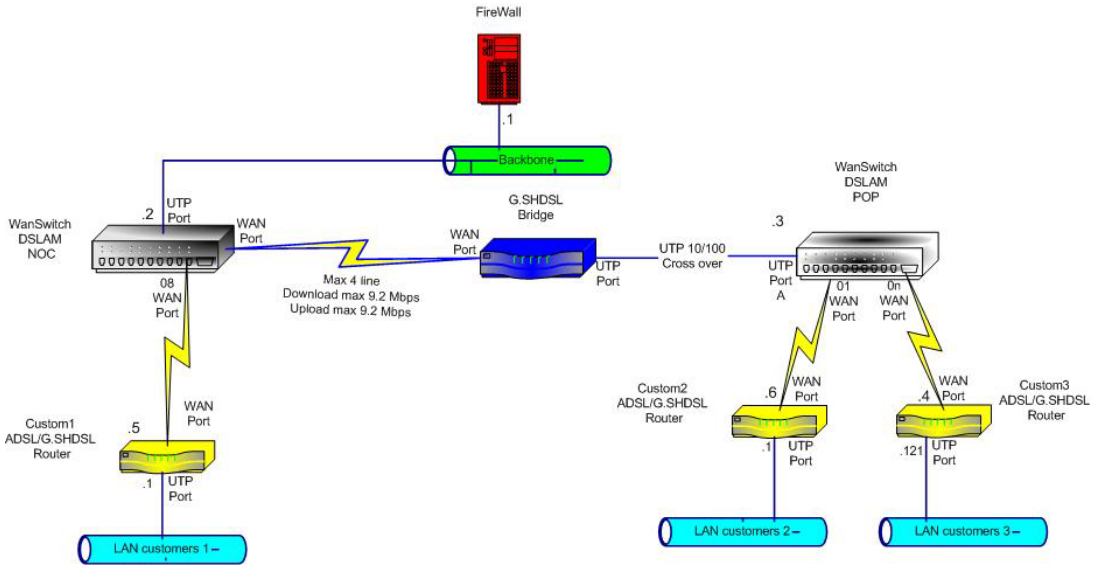
Để đảm bảo đúng chất lượng và tiến độ thi công, công tác kiểm tra và giám sát sẽ được tiến hành ngay sau khi hoàn thành từng phân đoạn mạng. Việc khiểm tra từng phân hệ cho phép chúng ta bỏ qua giai đoạn triển khai thử nghiệm mà vẫn rút ra được kinh nghiệm cô những phân đoạn tiếp theo.

Sau khi công trình hoàn thành hồ sơ thiết kế kỹ thuật, hồ sơ hoàn công của toàn bộ mạng lưới cũng như hồ sơ cấu hình của tất cả thiết bị đã triển khai phải có đầy đủ, và được bài giao cho nhóm quản trị mạng.

Kế hoạch triển khai.

Lịch triển khai được dự tính ngay trong thiết kế như sau:

Chi tiết	Ngày									
	1	2	3	4	5	6	7	8	9	10
Cấu hình thiết bị										
Kiểm tra và hoàn thiện hệ thống										
Bàn giao kỹ thuật										



Hình 3-30: Minh hoạ Wan backbone dùng chuẩn G.SHDSL/ADSL đã triển khai tại công ty NetNam

3.4 Tóm tắt chương 3

Phần đầu trình bày các kiến thức cơ bản về WAN, các yêu cầu khi thiết kế WAN, các công nghệ và các thiết bị dùng cho kết nối WAN. Đồng thời đưa ra so sánh và đánh giá các công nghệ này.

Phần hai trình bày phương pháp thiết kế WAN bao gồm các mô hình phục vụ cho thiết kế và đi sâu vào mô hình an toàn an ninh, là một vấn đề đặc biệt quan trọng khi thiết kế WAN. Trong phần này chúng tôi cũng đưa ra các bước phân tích và thiết kế WAN.

Phần cuối trình bày chi tiết mẫu thiết kế hệ thống WAN đơn giản nhưng khá phổ biến cho các cơ quan và tổ chức chính phủ ở Việt Nam hiện nay, đó là thiết kế WAN cho Trung tâm Thông tin của một Bộ, ngành mà chúng tôi đã triển khai trong thực tế.

4 Kết luận.

Là một đơn vị nghiên cứu, đồng thời là một ISP, chúng tôi đã trực tiếp thiết kế và triển khai nhiều hệ thống mạng trong nhiều năm qua, chúng tôi cố gắng đưa vào giáo trình những hiểu biết của mình nhằm giúp học viên các kiến thức cơ bản và thực tế khi thiết kế và xây dựng hệ thống mạng LAN, WAN.

Do phải viết giáo trình trong thời gian quá ngắn nên không tránh khỏi nhiều thiếu sót mong các đồng nghiệp chân thành góp ý.

5 Tài liệu tham khảo

[1] **Internetworking Design Basics**, Copyright Cisco Press 2003.

[2] **Internetwork Design Guide**, Copyright Cisco Press 2003.

[3] **Ethernet Networks: Design, Implementation, Operation, Management**. Gilbert Held .Copyright 2003 John Wiley & Sons, Ltd.

[4] **Internetworking Technologies Handbook.** Copyright Cisco Press 2003.

[5] **CCDA Exam Certification Guide**. Anthony Bruno, Jacqueline Kim, Copyright Cisco Press 2002.

[6] **TCP/IP Network Administration**. Craig Hunt, O'Reilly & Associates.

[7] **ISP Network Design**. IBM.

[8] **LAN Design Manual**. BICSI.

[9] **Mạng máy tính.** Nguyễn Gia Hiểu.

[10] **Mạng căn bản**. Nhà Xuất bản Thống kê.